SPLUNK_LOGS

Time	Event
2023-12-07T10:17:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:17:30.387721700Z'/><EventRecordID>1044</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:17:30.378</Data><Data Name='ProcessGuid'>{3CBB8FBE-8DAA-6571-B60B-000000001200}</Data><Data Name='ProcessId'>1908</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:17:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:17:28.372288900Z'/><EventRecordID>1043</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:17:28.362</Data><Data Name='ProcessGuid'>{3CBB8FBE-8DA8-6571-B50B-000000001200}</Data><Data Name='ProcessId'>8356</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:17:24+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:17:24.338452400Z'/><EventRecordID>1042</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:17:24.330</Data><Data Name='ProcessGuid'>{3CBB8FBE-8DA4-6571-B40B-000000001200}</Data><Data Name='ProcessId'>7876</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:17:22+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:17:22.310755100Z'/><EventRecordID>1041</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:17:22.301</Data><Data Name='ProcessGuid'>{3CBB8FBE-8DA2-6571-B30B-000000001200}</Data><Data Name='ProcessId'>10684</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:17:21+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:17:21.311241700Z'/><EventRecordID>1040</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:17:21.300</Data><Data Name='ProcessGuid'>{3CBB8FBE-8DA1-6571-B20B-000000001200}</Data><Data Name='ProcessId'>10304</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:17:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:17:19.279399500Z'/><EventRecordID>1039</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:17:19.269</Data><Data Name='ProcessGuid'>{3CBB8FBE-8D9F-6571-B10B-000000001200}</Data><Data Name='ProcessId'>9564</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:16:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:16:30.811708200Z'/><EventRecordID>1038</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:16:30.801</Data><Data Name='ProcessGuid'>{3CBB8FBE-8D6E-6571-AD0B-000000001200}</Data><Data Name='ProcessId'>10060</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:16:27+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:16:27.779769500Z'/><EventRecordID>1037</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:16:27.770</Data><Data Name='ProcessGuid'>{3CBB8FBE-8D6B-6571-AC0B-000000001200}</Data><Data Name='ProcessId'>5080</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:16:22+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:16:22.716494300Z'/><EventRecordID>1036</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:16:22.708</Data><Data Name='ProcessGuid'>{3CBB8FBE-8D66-6571-AB0B-000000001200}</Data><Data Name='ProcessId'>5460</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:16:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:16:20.700832200Z'/><EventRecordID>1035</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:16:20.692</Data><Data Name='ProcessGuid'>{3CBB8FBE-8D64-6571-AA0B-000000001200}</Data><Data Name='ProcessId'>8828</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:16:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:16:18.674129400Z'/><EventRecordID>1034</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:16:18.664</Data><Data Name='ProcessGuid'>{3CBB8FBE-8D62-6571-A90B-000000001200}</Data><Data Name='ProcessId'>10824</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:16:17+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:16:17.655476100Z'/><EventRecordID>1033</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:16:17.645</Data><Data Name='ProcessGuid'>{3CBB8FBE-8D61-6571-A80B-000000001200}</Data><Data Name='ProcessId'>8248</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:15:51+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:15:51.363798200Z'/><EventRecordID>1032</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:15:50.364</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>drive.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:216.58.206.46;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:15:48+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:15:48.988788300Z'/><EventRecordID>1031</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:15:47.835</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1500-000000001200}</Data><Data Name='ProcessId'>1096</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.137;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\NETWORK SERVICE</Data></EventData></Event>
2023-12-07T10:15:24+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:15:24.155560300Z'/><EventRecordID>1030</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:15:24.147</Data><Data Name='ProcessGuid'>{3CBB8FBE-8D2C-6571-A70B-000000001200}</Data><Data Name='ProcessId'>8348</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:15:23+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:15:23.156936700Z'/><EventRecordID>1029</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:15:23.147</Data><Data Name='ProcessGuid'>{3CBB8FBE-8D2B-6571-A60B-000000001200}</Data><Data Name='ProcessId'>6360</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:15:21+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:15:21.141185600Z'/><EventRecordID>1028</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:15:21.131</Data><Data Name='ProcessGuid'>{3CBB8FBE-8D29-6571-A50B-000000001200}</Data><Data Name='ProcessId'>8520</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-8A7E-6571-150B-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:15:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:15:19.127091400Z'/><EventRecordID>1027</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:15:19.115</Data><Data Name='ProcessGuid'>{3CBB8FBE-8D27-6571-A40B-000000001200}</Data><Data Name='ProcessId'>10448</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:15:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:15:18.125905200Z'/><EventRecordID>1026</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:15:18.115</Data><Data Name='ProcessGuid'>{3CBB8FBE-8D26-6571-A30B-000000001200}</Data><Data Name='ProcessId'>7268</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:15:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:15:16.110791900Z'/><EventRecordID>1025</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:15:16.100</Data><Data Name='ProcessGuid'>{3CBB8FBE-8D24-6571-A20B-000000001200}</Data><Data Name='ProcessId'>10924</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:14:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:14:29.704849000Z'/><EventRecordID>1024</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:14:29.694</Data><Data Name='ProcessGuid'>{3CBB8FBE-8CF5-6571-A10B-000000001200}</Data><Data Name='ProcessId'>6628</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:14:26+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:14:26.676849000Z'/><EventRecordID>1023</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:14:26.663</Data><Data Name='ProcessGuid'>{3CBB8FBE-8CF2-6571-A00B-000000001200}</Data><Data Name='ProcessId'>10456</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:14:22+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:14:22.614961900Z'/><EventRecordID>1022</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:14:22.601</Data><Data Name='ProcessGuid'>{3CBB8FBE-8CEE-6571-9F0B-000000001200}</Data><Data Name='ProcessId'>10892</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:14:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:14:20.596552900Z'/><EventRecordID>1021</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:14:20.585</Data><Data Name='ProcessGuid'>{3CBB8FBE-8CEC-6571-9E0B-000000001200}</Data><Data Name='ProcessId'>6232</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:14:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:14:19.580518300Z'/><EventRecordID>1020</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:14:19.569</Data><Data Name='ProcessGuid'>{3CBB8FBE-8CEB-6571-9D0B-000000001200}</Data><Data Name='ProcessId'>10296</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:14:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:14:16.547896500Z'/><EventRecordID>1019</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:14:16.538</Data><Data Name='ProcessGuid'>{3CBB8FBE-8CE8-6571-9C0B-000000001200}</Data><Data Name='ProcessId'>9128</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:13:57+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:13:57.944923800Z'/><EventRecordID>1018</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:13:56.967</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>aa.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 5 www3.l.google.com;::ffff:142.250.186.142;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:13:48+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:13:48.241590200Z'/><EventRecordID>1017</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:13:46.351</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>signaler-pa.clients6.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:216.58.212.106;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:13:23+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:13:23.082394500Z'/><EventRecordID>1016</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:13:23.070</Data><Data Name='ProcessGuid'>{3CBB8FBE-8CB3-6571-9B0B-000000001200}</Data><Data Name='ProcessId'>4964</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:13:22+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:13:22.069236300Z'/><EventRecordID>1015</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:13:22.055</Data><Data Name='ProcessGuid'>{3CBB8FBE-8CB2-6571-9A0B-000000001200}</Data><Data Name='ProcessId'>9332</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:13:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:13:20.050042900Z'/><EventRecordID>1014</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:13:20.040</Data><Data Name='ProcessGuid'>{3CBB8FBE-8CB0-6571-990B-000000001200}</Data><Data Name='ProcessId'>5488</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:13:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:13:18.036592300Z'/><EventRecordID>1013</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:13:18.026</Data><Data Name='ProcessGuid'>{3CBB8FBE-8CAE-6571-980B-000000001200}</Data><Data Name='ProcessId'>6780</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:13:17+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:13:17.002967800Z'/><EventRecordID>1012</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:13:16.994</Data><Data Name='ProcessGuid'>{3CBB8FBE-8CAC-6571-970B-000000001200}</Data><Data Name='ProcessId'>10096</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:13:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:13:16.003414000Z'/><EventRecordID>1011</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:13:15.993</Data><Data Name='ProcessGuid'>{3CBB8FBE-8CAB-6571-960B-000000001200}</Data><Data Name='ProcessId'>10920</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:12:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:12:32.789448200Z'/><EventRecordID>1010</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:12:30.762</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1200-000000001200}</Data><Data Name='ProcessId'>392</Data><Data Name='QueryName'>MEEREEN</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.137;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\LOCAL SERVICE</Data></EventData></Event>
2023-12-07T10:12:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:12:28.289583900Z'/><EventRecordID>1009</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:12:27.446</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>history.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 5 history.l.google.com;::ffff:172.253.122.100;::ffff:172.253.122.113;::ffff:172.253.122.138;::ffff:172.253.122.101;::ffff:172.253.122.139;::ffff:172.253.122.102;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T10:12:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:12:28.289563000Z'/><EventRecordID>1008</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:12:27.310</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>www.googleapis.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:216.58.212.170;::ffff:172.217.18.10;::ffff:142.250.185.106;::ffff:142.250.74.202;::ffff:172.217.23.106;::ffff:142.250.186.170;::ffff:142.250.185.74;::ffff:142.250.184.202;::ffff:172.217.16.202;::ffff:142.250.185.170;::ffff:142.250.186.138;::ffff:142.250.186.42;::ffff:172.217.18.106;::ffff:216.58.206.42;::ffff:142.250.185.138;::ffff:142.250.184.234;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:12:25+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:12:25.628452100Z'/><EventRecordID>1007</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:12:25.618</Data><Data Name='ProcessGuid'>{3CBB8FBE-8C79-6571-950B-000000001200}</Data><Data Name='ProcessId'>4128</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:12:24+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:12:24.612811200Z'/><EventRecordID>1006</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:12:24.603</Data><Data Name='ProcessGuid'>{3CBB8FBE-8C78-6571-940B-000000001200}</Data><Data Name='ProcessId'>11056</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:12:21+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:12:21.595788600Z'/><EventRecordID>1005</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:12:21.587</Data><Data Name='ProcessGuid'>{3CBB8FBE-8C75-6571-930B-000000001200}</Data><Data Name='ProcessId'>2836</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:12:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:12:20.582031200Z'/><EventRecordID>1004</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:12:20.572</Data><Data Name='ProcessGuid'>{3CBB8FBE-8C74-6571-920B-000000001200}</Data><Data Name='ProcessId'>7952</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:12:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:12:19.581506300Z'/><EventRecordID>1003</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:12:19.571</Data><Data Name='ProcessGuid'>{3CBB8FBE-8C73-6571-910B-000000001200}</Data><Data Name='ProcessId'>10396</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:12:17+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:12:17.534005000Z'/><EventRecordID>1002</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:12:17.526</Data><Data Name='ProcessGuid'>{3CBB8FBE-8C71-6571-900B-000000001200}</Data><Data Name='ProcessId'>2460</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:11:21+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:11:21.052340300Z'/><EventRecordID>1001</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:11:21.041</Data><Data Name='ProcessGuid'>{3CBB8FBE-8C39-6571-8F0B-000000001200}</Data><Data Name='ProcessId'>7820</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:11:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:11:20.051579400Z'/><EventRecordID>1000</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:11:20.041</Data><Data Name='ProcessGuid'>{3CBB8FBE-8C38-6571-8E0B-000000001200}</Data><Data Name='ProcessId'>6316</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:11:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:11:18.025350500Z'/><EventRecordID>999</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:11:18.013</Data><Data Name='ProcessGuid'>{3CBB8FBE-8C36-6571-8D0B-000000001200}</Data><Data Name='ProcessId'>10352</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:11:17+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:11:17.005862500Z'/><EventRecordID>998</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:11:16.995</Data><Data Name='ProcessGuid'>{3CBB8FBE-8C34-6571-8C0B-000000001200}</Data><Data Name='ProcessId'>8844</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:11:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:11:16.005420700Z'/><EventRecordID>997</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:11:15.995</Data><Data Name='ProcessGuid'>{3CBB8FBE-8C33-6571-8B0B-000000001200}</Data><Data Name='ProcessId'>4092</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:11:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:11:15.004729600Z'/><EventRecordID>996</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:11:14.994</Data><Data Name='ProcessGuid'>{3CBB8FBE-8C32-6571-8A0B-000000001200}</Data><Data Name='ProcessId'>8164</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:10:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:10:20.535147600Z'/><EventRecordID>995</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:10:20.526</Data><Data Name='ProcessGuid'>{3CBB8FBE-8BFC-6571-890B-000000001200}</Data><Data Name='ProcessId'>9464</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:10:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:10:19.506377800Z'/><EventRecordID>994</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:10:19.495</Data><Data Name='ProcessGuid'>{3CBB8FBE-8BFB-6571-880B-000000001200}</Data><Data Name='ProcessId'>7268</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:10:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:10:16.474349000Z'/><EventRecordID>993</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:10:16.465</Data><Data Name='ProcessGuid'>{3CBB8FBE-8BF8-6571-870B-000000001200}</Data><Data Name='ProcessId'>6152</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:10:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:10:15.476005800Z'/><EventRecordID>992</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:10:15.458</Data><Data Name='ProcessGuid'>{3CBB8FBE-8BF7-6571-860B-000000001200}</Data><Data Name='ProcessId'>3616</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:10:14+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:10:14.383532400Z'/><EventRecordID>991</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:10:14.371</Data><Data Name='ProcessGuid'>{3CBB8FBE-8BF6-6571-850B-000000001200}</Data><Data Name='ProcessId'>7556</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:10:13+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:10:13.380979600Z'/><EventRecordID>990</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:10:13.370</Data><Data Name='ProcessGuid'>{3CBB8FBE-8BF5-6571-840B-000000001200}</Data><Data Name='ProcessId'>8884</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:10:01+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:10:01.917233500Z'/><EventRecordID>989</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:10:00.913</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:142.250.186.174;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:09:36+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:09:36.813754400Z'/><EventRecordID>988</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 09:09:36.807</Data><Data Name='ProcessGuid'>{3CBB8FBE-0240-656E-5100-000000001200}</Data><Data Name='ProcessId'>4984</Data><Data Name='Image'>C:\Windows\Explorer.EXE</Data><Data Name='TargetObject'>HKU\S-1-5-21-2479543311-1709999589-3761869525-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{FFE2A43C-56B9-4BF5-9A79-CC6D4285608A} {000214E4-0000-0000-C000-000000000046} 0xFFFF</Data><Data Name='Details'>Binary Data</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:09:36+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:09:36.772686800Z'/><EventRecordID>987</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 09:09:36.760</Data><Data Name='ProcessGuid'>{3CBB8FBE-0240-656E-5100-000000001200}</Data><Data Name='ProcessId'>4984</Data><Data Name='Image'>C:\Windows\Explorer.EXE</Data><Data Name='TargetObject'>HKU\S-1-5-21-2479543311-1709999589-3761869525-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{7AD84985-87B4-4A16-BE58-8B72A5B390F7} {000214E4-0000-0000-C000-000000000046} 0xFFFF</Data><Data Name='Details'>Binary Data</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:09:23+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:09:23.073104300Z'/><EventRecordID>986</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:09:21.932</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>passwordsleakcheck-pa.googleapis.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:142.250.185.106;::ffff:216.58.212.138;::ffff:142.250.181.234;::ffff:142.250.186.138;::ffff:172.217.16.202;::ffff:142.250.186.106;::ffff:142.250.184.202;::ffff:216.58.206.42;::ffff:142.250.186.74;::ffff:142.250.186.42;::ffff:142.250.185.234;::ffff:142.250.186.170;::ffff:172.217.18.10;::ffff:172.217.23.106;::ffff:142.250.185.74;::ffff:142.250.184.234;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T10:09:22+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:09:22.074242100Z'/><EventRecordID>985</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:09:21.093</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>ogs.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 5 www3.l.google.com;::ffff:142.250.181.238;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:09:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:09:20.868491300Z'/><EventRecordID>984</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:09:20.858</Data><Data Name='ProcessGuid'>{3CBB8FBE-8BC0-6571-820B-000000001200}</Data><Data Name='ProcessId'>5384</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:09:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:09:19.856469100Z'/><EventRecordID>983</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:09:19.840</Data><Data Name='ProcessGuid'>{3CBB8FBE-8BBF-6571-810B-000000001200}</Data><Data Name='ProcessId'>8216</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:09:17+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:09:17.839259700Z'/><EventRecordID>982</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:09:17.828</Data><Data Name='ProcessGuid'>{3CBB8FBE-8BBD-6571-800B-000000001200}</Data><Data Name='ProcessId'>2228</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:09:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:09:16.824166000Z'/><EventRecordID>981</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:09:16.813</Data><Data Name='ProcessGuid'>{3CBB8FBE-8BBC-6571-7F0B-000000001200}</Data><Data Name='ProcessId'>8764</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:09:14+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:09:14.808909100Z'/><EventRecordID>980</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:09:14.797</Data><Data Name='ProcessGuid'>{3CBB8FBE-8BBA-6571-7E0B-000000001200}</Data><Data Name='ProcessId'>836</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:09:13+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:09:13.790180600Z'/><EventRecordID>979</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:09:13.780</Data><Data Name='ProcessGuid'>{3CBB8FBE-8BB9-6571-7D0B-000000001200}</Data><Data Name='ProcessId'>10540</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:09:08+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:09:08.212783900Z'/><EventRecordID>978</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:09:07.410</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>signaler-pa.clients6.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:142.250.186.170;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:09:08+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:09:08.212763500Z'/><EventRecordID>977</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:09:07.232</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>contacts.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 5 plus.l.google.com;::ffff:142.250.186.142;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:09:01+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:09:01.871875700Z'/><EventRecordID>976</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:09:00.893</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>docs.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:142.250.186.110;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:08:57+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:57.749789900Z'/><EventRecordID>975</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:57.614</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>peoplestack-pa.clients6.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:216.58.206.42;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:08:57+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:57.749757000Z'/><EventRecordID>974</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:57.583</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>drivefrontend-pa.clients6.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:142.250.185.202;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:08:57+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:57.749740100Z'/><EventRecordID>973</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:57.558</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>people-pa.clients6.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:216.58.206.42;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T10:08:57+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:57.749724600Z'/><EventRecordID>972</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:57.496</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>addons-pa.clients6.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:142.250.185.138;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:08:57+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:57.749707700Z'/><EventRecordID>971</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:57.434</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>peoplestackwebexperiments-pa.clients6.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:172.217.23.106;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:08:57+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:57.749685900Z'/><EventRecordID>970</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:57.114</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>aa.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 5 www3.l.google.com;::ffff:142.250.181.238;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:08:45+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:45.722128100Z'/><EventRecordID>969</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:44.739</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2900-000000001200}</Data><Data Name='ProcessId'>2692</Data><Data Name='QueryName'>MEEREEN</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.137;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\dfsrs.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:08:45+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:45.722108500Z'/><EventRecordID>968</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:44.721</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2900-000000001200}</Data><Data Name='ProcessId'>2692</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.137;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\dfsrs.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:08:37+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:37.805096100Z'/><EventRecordID>967</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:36.589</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>drive-thirdparty.googleusercontent.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 5 googlehosted.l.googleusercontent.com;::ffff:172.217.18.97;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T10:08:36+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:36.805814800Z'/><EventRecordID>966</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:36.356</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>apis.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 5 plus.l.google.com;::ffff:142.250.186.142;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:08:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:35.801681000Z'/><EventRecordID>965</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:34.688</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>android.clients.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 5 android.l.google.com;::ffff:172.217.18.14;::ffff:142.250.186.174;::ffff:216.58.206.46;::ffff:142.250.186.46;::ffff:142.250.186.78;::ffff:216.58.212.174;::ffff:142.250.185.110;::ffff:142.250.185.174;::ffff:142.250.185.142;::ffff:172.217.23.110;::ffff:216.58.212.142;::ffff:142.250.185.78;::ffff:142.250.185.238;::ffff:172.217.18.110;::ffff:172.217.16.206;::ffff:142.250.185.206;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:08:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:34.799770000Z'/><EventRecordID>964</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:34.092</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>drive.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:172.217.18.14;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:08:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:34.799751300Z'/><EventRecordID>963</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:33.573</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>accounts.google.fr</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 5 accounts-cctld.l.google.com;::ffff:66.102.1.94;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:08:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:33.798461600Z'/><EventRecordID>962</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:33.247</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>accountcapabilities-pa.googleapis.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:142.250.185.234;::ffff:142.250.185.74;::ffff:142.250.185.138;::ffff:216.58.206.42;::ffff:142.250.185.170;::ffff:172.217.23.106;::ffff:216.58.212.170;::ffff:142.250.186.106;::ffff:142.250.185.202;::ffff:172.217.18.106;::ffff:142.250.186.42;::ffff:172.217.16.202;::ffff:142.250.186.170;::ffff:142.250.186.74;::ffff:172.217.18.10;::ffff:142.250.185.106;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:08:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:33.798434000Z'/><EventRecordID>961</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:32.996</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>www.googleapis.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:142.250.185.234;::ffff:172.217.16.138;::ffff:142.250.181.234;::ffff:142.250.186.106;::ffff:142.250.185.138;::ffff:142.250.184.234;::ffff:142.250.186.74;::ffff:172.217.23.106;::ffff:142.250.186.42;::ffff:216.58.212.138;::ffff:142.250.185.74;::ffff:142.250.185.202;::ffff:142.250.185.170;::ffff:142.250.185.106;::ffff:142.250.184.202;::ffff:142.250.186.138;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T10:08:23+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:23.992674500Z'/><EventRecordID>960</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:22.791</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>accounts.youtube.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 5 www3.l.google.com;::ffff:142.250.181.238;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:08:23+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:23.003696300Z'/><EventRecordID>959</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:22.730</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>lh3.googleusercontent.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 5 googlehosted.l.googleusercontent.com;::ffff:142.251.37.225;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:08:23+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:23.003652300Z'/><EventRecordID>958</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:21.705</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>accounts.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:66.102.1.84;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:08:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:20.979368200Z'/><EventRecordID>957</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:20.634</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>csp.withgoogle.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:216.58.212.145;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:08:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:20.979321600Z'/><EventRecordID>956</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:20.000</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>kstatic.googleusercontent.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:35.241.11.240;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T10:08:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:19.649406800Z'/><EventRecordID>955</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:19.637</Data><Data Name='ProcessGuid'>{3CBB8FBE-8B83-6571-760B-000000001200}</Data><Data Name='ProcessId'>2460</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:08:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:18.631708100Z'/><EventRecordID>954</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:18.622</Data><Data Name='ProcessGuid'>{3CBB8FBE-8B82-6571-750B-000000001200}</Data><Data Name='ProcessId'>8680</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:08:17+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:17.629995600Z'/><EventRecordID>953</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:17.621</Data><Data Name='ProcessGuid'>{3CBB8FBE-8B81-6571-740B-000000001200}</Data><Data Name='ProcessId'>6212</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:08:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:16.616441000Z'/><EventRecordID>952</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:16.606</Data><Data Name='ProcessGuid'>{3CBB8FBE-8B80-6571-730B-000000001200}</Data><Data Name='ProcessId'>7448</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:08:14+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:14.585381000Z'/><EventRecordID>951</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:14.575</Data><Data Name='ProcessGuid'>{3CBB8FBE-8B7E-6571-720B-000000001200}</Data><Data Name='ProcessId'>9832</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:08:12+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:08:12.570830300Z'/><EventRecordID>950</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:08:12.560</Data><Data Name='ProcessGuid'>{3CBB8FBE-8B7C-6571-710B-000000001200}</Data><Data Name='ProcessId'>8368</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:07:26+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:07:26.800575300Z'/><EventRecordID>949</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:07:25.817</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>www.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:142.250.185.132;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:07:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:07:18.179586100Z'/><EventRecordID>948</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:07:18.169</Data><Data Name='ProcessGuid'>{3CBB8FBE-8B46-6571-680B-000000001200}</Data><Data Name='ProcessId'>5740</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:07:17+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:07:17.166608800Z'/><EventRecordID>947</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:07:17.154</Data><Data Name='ProcessGuid'>{3CBB8FBE-8B45-6571-670B-000000001200}</Data><Data Name='ProcessId'>9456</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:07:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:07:16.162082600Z'/><EventRecordID>946</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:07:16.154</Data><Data Name='ProcessGuid'>{3CBB8FBE-8B44-6571-660B-000000001200}</Data><Data Name='ProcessId'>1304</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:07:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:07:15.163574500Z'/><EventRecordID>945</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:07:15.153</Data><Data Name='ProcessGuid'>{3CBB8FBE-8B43-6571-650B-000000001200}</Data><Data Name='ProcessId'>2644</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:07:14+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:07:14.162775400Z'/><EventRecordID>944</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:07:14.154</Data><Data Name='ProcessGuid'>{3CBB8FBE-8B42-6571-640B-000000001200}</Data><Data Name='ProcessId'>3616</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:07:12+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:07:12.150816800Z'/><EventRecordID>943</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:07:12.138</Data><Data Name='ProcessGuid'>{3CBB8FBE-8B40-6571-630B-000000001200}</Data><Data Name='ProcessId'>6772</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:07:00+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:07:00.575973400Z'/><EventRecordID>942</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:06:59.581</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.sevenkingdoms.local.</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 33 ;192.168.56.10;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:07:00+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:07:00.575946800Z'/><EventRecordID>941</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:06:59.576</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>kingslanding.sevenkingdoms.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:192.168.56.10;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:06:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:06:43.217829600Z'/><EventRecordID>940</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:06:43.210</Data><Data Name='ProcessGuid'>{3CBB8FBE-8B23-6571-5F0B-000000001200}</Data><Data Name='ProcessId'>9484</Data><Data Name='Image'>C:\Windows\System32\ipconfig.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>IP Configuration Utility</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>ipconfig.exe</Data><Data Name='CommandLine'>ipconfig</Data><Data Name='CurrentDirectory'>C:\Program Files\SplunkUniversalForwarder\bin\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-99C8-040000000000}</Data><Data Name='LogonId'>0x4c899</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=29916DCEA5377C19996B417D9235F42F,SHA256=5EE3FD7CA1AC876D0DE539D469BFC333594FCA3DF9F377CC96C756D9648697F1,IMPHASH=3636F50089F8190E3308E8AEA8F2043A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-FA33-656E-2B01-000000001200}</Data><Data Name='ParentProcessId'>8096</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"C:\Windows\system32\cmd.exe" </Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:06:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:06:18.633536100Z'/><EventRecordID>939</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:06:18.623</Data><Data Name='ProcessGuid'>{3CBB8FBE-8B0A-6571-5E0B-000000001200}</Data><Data Name='ProcessId'>1928</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:06:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:06:18.543471100Z'/><EventRecordID>938</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:06:17.559</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>www.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:142.250.184.228;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:06:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:06:16.617393900Z'/><EventRecordID>937</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:06:16.607</Data><Data Name='ProcessGuid'>{3CBB8FBE-8B08-6571-5D0B-000000001200}</Data><Data Name='ProcessId'>11000</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:06:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:06:15.618645500Z'/><EventRecordID>936</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:06:15.607</Data><Data Name='ProcessGuid'>{3CBB8FBE-8B07-6571-5C0B-000000001200}</Data><Data Name='ProcessId'>8756</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:06:14+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:06:14.601641400Z'/><EventRecordID>935</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:06:14.591</Data><Data Name='ProcessGuid'>{3CBB8FBE-8B06-6571-5B0B-000000001200}</Data><Data Name='ProcessId'>10540</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:06:11+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:06:11.589526700Z'/><EventRecordID>934</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:06:11.576</Data><Data Name='ProcessGuid'>{3CBB8FBE-8B03-6571-5A0B-000000001200}</Data><Data Name='ProcessId'>10408</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:06:10+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:06:10.587098700Z'/><EventRecordID>933</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:06:10.576</Data><Data Name='ProcessGuid'>{3CBB8FBE-8B02-6571-590B-000000001200}</Data><Data Name='ProcessId'>10444</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:05:48+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:05:48.965342900Z'/><EventRecordID>932</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:05:47.531</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1200-000000001200}</Data><Data Name='ProcessId'>392</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.137;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\LOCAL SERVICE</Data></EventData></Event>
2023-12-07T10:05:47+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:05:47.951039800Z'/><EventRecordID>931</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:05:47.420</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1700-000000001200}</Data><Data Name='ProcessId'>1340</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.137;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:05:47+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:05:47.951027300Z'/><EventRecordID>930</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:05:47.420</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.137;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:05:47+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:05:47.951002400Z'/><EventRecordID>929</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:05:47.420</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>meereen</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>10.202.0.137;192.168.56.12;10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:05:46+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:05:46.349559500Z'/><EventRecordID>928</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>Downloads</Data><Data Name='UtcTime'>2023-12-07 09:05:46.340</Data><Data Name='ProcessGuid'>{3CBB8FBE-A67F-6570-EB02-000000001200}</Data><Data Name='ProcessId'>8620</Data><Data Name='Image'>C:\Windows\system32\SnippingTool.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\Downloads\splunk4.png</Data><Data Name='CreationUtcTime'>2023-12-07 09:05:46.277</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:05:46+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:05:46.282913700Z'/><EventRecordID>927</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>Downloads</Data><Data Name='UtcTime'>2023-12-07 09:05:46.277</Data><Data Name='ProcessGuid'>{3CBB8FBE-A67F-6570-EB02-000000001200}</Data><Data Name='ProcessId'>8620</Data><Data Name='Image'>C:\Windows\system32\SnippingTool.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\Downloads\splunk4.png</Data><Data Name='CreationUtcTime'>2023-12-07 09:05:46.277</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:05:23+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:05:23.137016700Z'/><EventRecordID>926</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:05:21.482</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2300-000000001200}</Data><Data Name='ProcessId'>2520</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.137;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:05:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:05:18.101784300Z'/><EventRecordID>925</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:05:18.091</Data><Data Name='ProcessGuid'>{3CBB8FBE-8ACE-6571-570B-000000001200}</Data><Data Name='ProcessId'>3868</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:05:17+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:05:17.084675400Z'/><EventRecordID>924</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:05:17.076</Data><Data Name='ProcessGuid'>{3CBB8FBE-8ACD-6571-560B-000000001200}</Data><Data Name='ProcessId'>1064</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:05:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:05:15.088623400Z'/><EventRecordID>923</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:05:15.076</Data><Data Name='ProcessGuid'>{3CBB8FBE-8ACB-6571-550B-000000001200}</Data><Data Name='ProcessId'>5620</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:05:13+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:05:13.057567800Z'/><EventRecordID>922</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:05:13.045</Data><Data Name='ProcessGuid'>{3CBB8FBE-8AC9-6571-540B-000000001200}</Data><Data Name='ProcessId'>6344</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:05:11+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:05:11.039300300Z'/><EventRecordID>921</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:05:11.029</Data><Data Name='ProcessGuid'>{3CBB8FBE-8AC7-6571-530B-000000001200}</Data><Data Name='ProcessId'>436</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:05:10+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:05:10.024761600Z'/><EventRecordID>920</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:05:10.014</Data><Data Name='ProcessGuid'>{3CBB8FBE-8AC6-6571-520B-000000001200}</Data><Data Name='ProcessId'>6316</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:04:46+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:46.749484600Z'/><EventRecordID>919</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:45.759</Data><Data Name='ProcessGuid'>{3CBB8FBE-7D54-6571-5B08-000000001200}</Data><Data Name='ProcessId'>10156</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.137;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\mmc.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:04:46+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:46.749466400Z'/><EventRecordID>918</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:45.759</Data><Data Name='ProcessGuid'>{3CBB8FBE-7D54-6571-5B08-000000001200}</Data><Data Name='ProcessId'>10156</Data><Data Name='QueryName'>MEEREEN</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.137;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\mmc.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:04:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:32.934230900Z'/><EventRecordID>917</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:32.090</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2100-000000001200}</Data><Data Name='ProcessId'>2472</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.137;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\dns.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:29.918563800Z'/><EventRecordID>916</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:28.945</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1500-000000001200}</Data><Data Name='ProcessId'>1096</Data><Data Name='QueryName'>meereen</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>10.202.0.165;fe80::3076:9c8f:3acb:98de;10.202.8.12;fe80::6db1:37b4:dbdb:df69;</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\NETWORK SERVICE</Data></EventData></Event>
2023-12-07T10:04:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:28.918458800Z'/><EventRecordID>915</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:27.959</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1500-000000001200}</Data><Data Name='ProcessId'>1096</Data><Data Name='QueryName'>meereen</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>10.202.0.133;fe80::446b:fc66:adec:e3bd;10.202.0.165;fe80::3076:9c8f:3acb:98de;10.202.8.12;fe80::6db1:37b4:dbdb:df69;10.202.0.171;fe80::78eb:329:5dc5:9f69;</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\NETWORK SERVICE</Data></EventData></Event>
2023-12-07T10:04:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:28.918422000Z'/><EventRecordID>914</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:27.921</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2000-000000001200}</Data><Data Name='ProcessId'>2408</Data><Data Name='QueryName'>MEEREEN</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>10.202.0.137;192.168.56.12;10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\spoolsv.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:04:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:28.918407300Z'/><EventRecordID>913</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:27.919</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>MEEREEN</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.137;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:19.309304000Z'/><EventRecordID>912</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:18.255</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2100-000000001200}</Data><Data Name='ProcessId'>2472</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\dns.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:16.138012800Z'/><EventRecordID>911</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:15.252</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2100-000000001200}</Data><Data Name='ProcessId'>2472</Data><Data Name='QueryName'>essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\dns.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:16.138004400Z'/><EventRecordID>910</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:15.252</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2100-000000001200}</Data><Data Name='ProcessId'>2472</Data><Data Name='QueryName'>essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 2 meereen.essos.local;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\dns.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:16.137994600Z'/><EventRecordID>909</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:15.251</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2100-000000001200}</Data><Data Name='ProcessId'>2472</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\dns.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:16.137984400Z'/><EventRecordID>908</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:15.250</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2100-000000001200}</Data><Data Name='ProcessId'>2472</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\dns.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:04:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:16.137971900Z'/><EventRecordID>907</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:15.250</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1500-000000001200}</Data><Data Name='ProcessId'>1096</Data><Data Name='QueryName'>essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 2 meereen.essos.local;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\NETWORK SERVICE</Data></EventData></Event>
2023-12-07T10:04:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:16.137948800Z'/><EventRecordID>906</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:15.242</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2100-000000001200}</Data><Data Name='ProcessId'>2472</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\system32\dns.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:16.137508400Z'/><EventRecordID>905</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:15.237</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1500-000000001200}</Data><Data Name='ProcessId'>1096</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\NETWORK SERVICE</Data></EventData></Event>
2023-12-07T10:04:14+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:14.139103000Z'/><EventRecordID>904</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:13.135</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1500-000000001200}</Data><Data Name='ProcessId'>1096</Data><Data Name='QueryName'>meereen</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>10.202.8.12;fe80::6db1:37b4:dbdb:df69;10.202.0.165;fe80::3076:9c8f:3acb:98de;10.202.0.133;fe80::446b:fc66:adec:e3bd;</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\NETWORK SERVICE</Data></EventData></Event>
2023-12-07T10:04:13+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:13.463526200Z'/><EventRecordID>903</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:13.450</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A8D-6571-510B-000000001200}</Data><Data Name='ProcessId'>6040</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-winprintmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Windows Print Monitor </Data><Data Name='Product'>splunk Application </Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-winprintmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-winprintmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=FDEB6BA573575665D847C8C88DFA6B28,SHA256=00FC8040D205B3290D204EB5E6AEAF5E21CF6F5EDB081555CDF81AD61F306218,IMPHASH=355E487ADBCE53AA00CC9620C5813D5A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:04:13+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:13.122976700Z'/><EventRecordID>902</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:12.991</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A8C-6571-500B-000000001200}</Data><Data Name='ProcessId'>1036</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:12+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:12.860774900Z'/><EventRecordID>901</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:12.841</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A8C-6571-500B-000000001200}</Data><Data Name='ProcessId'>1036</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Monitor windows event logs</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-winevtlog.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AE95292862972429C2FBD9541C739C2B,SHA256=C1899D942B83A761EADA6303334A9E6946A7206A59E678F0039D3AB527785522,IMPHASH=EDE9B13E7663B8E763DD4604CD8C3BF7</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:12+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:12.423948900Z'/><EventRecordID>900</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:12.264</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1500-000000001200}</Data><Data Name='ProcessId'>1096</Data><Data Name='QueryName'>meereen</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>10.202.0.165;fe80::3076:9c8f:3acb:98de;10.202.0.133;fe80::446b:fc66:adec:e3bd;</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\NETWORK SERVICE</Data></EventData></Event>
2023-12-07T10:04:12+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:12.423890200Z'/><EventRecordID>899</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:12.198</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2000-000000001200}</Data><Data Name='ProcessId'>2408</Data><Data Name='QueryName'>MEEREEN</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;</Data><Data Name='Image'>C:\Windows\System32\spoolsv.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:12+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:12.423878200Z'/><EventRecordID>898</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:12.198</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2000-000000001200}</Data><Data Name='ProcessId'>2408</Data><Data Name='QueryName'>MEEREEN</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>10.202.0.166;192.168.56.12;10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\spoolsv.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:04:12+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:12.089079900Z'/><EventRecordID>897</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:12.078</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A8C-6571-4F0B-000000001200}</Data><Data Name='ProcessId'>9908</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:11+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:11.336067500Z'/><EventRecordID>896</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:11.326</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A8B-6571-4E0B-000000001200}</Data><Data Name='ProcessId'>1364</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:10+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:10.584254300Z'/><EventRecordID>895</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:10.575</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A8A-6571-4D0B-000000001200}</Data><Data Name='ProcessId'>8120</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:04:09+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:09.819926000Z'/><EventRecordID>894</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:09.810</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A89-6571-4C0B-000000001200}</Data><Data Name='ProcessId'>9464</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-perfmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Performance monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-perfmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-perfmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=37F610EA3267B4C636A52CC17C72F5E9,SHA256=154252976F3CDC663C1999E5BF6958E4A9717874E2117061A0E40F2F1D97BE27,IMPHASH=35AE00EA6705AD0DB2C706FD3FAF93B6</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:09+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:09.055531800Z'/><EventRecordID>893</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:09.044</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A89-6571-4B0B-000000001200}</Data><Data Name='ProcessId'>8172</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:08+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:08.308902200Z'/><EventRecordID>892</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:08.294</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A88-6571-4A0B-000000001200}</Data><Data Name='ProcessId'>7200</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:04:07+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:07.538729400Z'/><EventRecordID>891</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:07.528</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A87-6571-490B-000000001200}</Data><Data Name='ProcessId'>8704</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:06+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:06.793978800Z'/><EventRecordID>890</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:06.765</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A86-6571-480B-000000001200}</Data><Data Name='ProcessId'>3348</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-wmi.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Remote Performance monitor using WMI</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-wmi.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-wmi.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=7A440F2DF244985160C5B54CDBBA547D,SHA256=7E1DBA295076C76618106FD18E882B190BF0542AD2981200D01074B021BF76CF,IMPHASH=7C7770CDB275E49574E79FDF395C7C60</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:04.795334800Z'/><EventRecordID>889</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:04.784</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A84-6571-470B-000000001200}</Data><Data Name='ProcessId'>10892</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\powershell2.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:04:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:04.672872600Z'/><EventRecordID>888</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:04.659</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A84-6571-460B-000000001200}</Data><Data Name='ProcessId'>2268</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\powershell.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:04.545295600Z'/><EventRecordID>887</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:04.535</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A84-6571-450B-000000001200}</Data><Data Name='ProcessId'>11040</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\perfmon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:04.420276400Z'/><EventRecordID>886</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:04.410</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A84-6571-440B-000000001200}</Data><Data Name='ProcessId'>9388</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\admon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:04:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:04.295102200Z'/><EventRecordID>885</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:04.285</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A84-6571-430B-000000001200}</Data><Data Name='ProcessId'>7556</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinRegMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:04.170445200Z'/><EventRecordID>884</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:04.159</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A84-6571-420B-000000001200}</Data><Data Name='ProcessId'>3272</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinPrintMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:04.045724800Z'/><EventRecordID>883</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:04.034</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A84-6571-410B-000000001200}</Data><Data Name='ProcessId'>5428</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinNetMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:04:03+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:03.920047800Z'/><EventRecordID>882</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:03.910</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A83-6571-400B-000000001200}</Data><Data Name='ProcessId'>6540</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinHostMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:03+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:03.794497100Z'/><EventRecordID>881</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:03.784</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A83-6571-3F0B-000000001200}</Data><Data Name='ProcessId'>8336</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinEventLog.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:03+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:03.663763700Z'/><EventRecordID>880</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:03.653</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A83-6571-3E0B-000000001200}</Data><Data Name='ProcessId'>3252</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\MonitorNoHandle.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:04:03+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:03.002919800Z'/><EventRecordID>879</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:02.998</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A82-6571-3D0B-000000001200}</Data><Data Name='ProcessId'>10012</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal check-xml-files --answer-yes --no-prompt </Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A82-6571-3C0B-000000001200}</Data><Data Name='ParentProcessId'>9612</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal check-xml-files --answer-yes --no-prompt 2>&1</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:02+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:02.993587400Z'/><EventRecordID>878</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:02.984</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A82-6571-3C0B-000000001200}</Data><Data Name='ProcessId'>9612</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal check-xml-files --answer-yes --no-prompt 2>&1</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:02+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:02.718976100Z'/><EventRecordID>877</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:02.712</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A82-6571-3B0B-000000001200}</Data><Data Name='ProcessId'>9676</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A82-6571-3A0B-000000001200}</Data><Data Name='ParentProcessId'>8884</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:04:02+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:02.706775700Z'/><EventRecordID>876</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:02.702</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A82-6571-3A0B-000000001200}</Data><Data Name='ProcessId'>8884</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A82-6571-390B-000000001200}</Data><Data Name='ParentProcessId'>2952</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:02+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:02.697675700Z'/><EventRecordID>875</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:02.693</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A82-6571-390B-000000001200}</Data><Data Name='ProcessId'>2952</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7F-6571-2C0B-000000001200}</Data><Data Name='ParentProcessId'>2112</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:02+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:02.429374600Z'/><EventRecordID>874</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:02.421</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A82-6571-380B-000000001200}</Data><Data Name='ProcessId'>356</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list replication_port --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A82-6571-370B-000000001200}</Data><Data Name='ParentProcessId'>6580</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list replication_port --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:04:02+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:02.416666700Z'/><EventRecordID>873</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:02.411</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A82-6571-370B-000000001200}</Data><Data Name='ProcessId'>6580</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list replication_port --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A82-6571-360B-000000001200}</Data><Data Name='ParentProcessId'>9524</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list replication_port --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:02+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:02.408260900Z'/><EventRecordID>872</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:02.404</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A82-6571-360B-000000001200}</Data><Data Name='ProcessId'>9524</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list replication_port --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7F-6571-2C0B-000000001200}</Data><Data Name='ParentProcessId'>2112</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:02+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:02.101453600Z'/><EventRecordID>871</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:02.094</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A82-6571-350B-000000001200}</Data><Data Name='ProcessId'>8316</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd" check-transforms-keys</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7F-6571-2C0B-000000001200}</Data><Data Name='ParentProcessId'>2112</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:04:01+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:01.572886800Z'/><EventRecordID>870</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:01.566</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A81-6571-340B-000000001200}</Data><Data Name='ProcessId'>9252</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool validate-regex --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A81-6571-330B-000000001200}</Data><Data Name='ParentProcessId'>9644</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-regex --log-warnings</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:01+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:01.561021000Z'/><EventRecordID>869</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:01.556</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A81-6571-330B-000000001200}</Data><Data Name='ProcessId'>9644</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-regex --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7F-6571-2C0B-000000001200}</Data><Data Name='ParentProcessId'>2112</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:01+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:01.092615400Z'/><EventRecordID>868</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:01.086</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A81-6571-320B-000000001200}</Data><Data Name='ProcessId'>9508</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool validate-strptime --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A81-6571-310B-000000001200}</Data><Data Name='ParentProcessId'>3772</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-strptime --log-warnings</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:04:01+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:01.081846100Z'/><EventRecordID>867</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:01.077</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A81-6571-310B-000000001200}</Data><Data Name='ProcessId'>3772</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>" C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-strptime --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7F-6571-2C0B-000000001200}</Data><Data Name='ParentProcessId'>2112</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:00+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:00.494457800Z'/><EventRecordID>866</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:00.488</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A80-6571-300B-000000001200}</Data><Data Name='ProcessId'>1476</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool check --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A80-6571-2F0B-000000001200}</Data><Data Name='ParentProcessId'>10780</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" check --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:04:00+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:00.483069000Z'/><EventRecordID>865</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:00.478</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A80-6571-2F0B-000000001200}</Data><Data Name='ProcessId'>10780</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>" C:\Program Files\SplunkUniversalForwarder\bin\btool" check --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7F-6571-2C0B-000000001200}</Data><Data Name='ParentProcessId'>2112</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:04:00+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:04:00.207499900Z'/><EventRecordID>864</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:04:00.200</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A80-6571-2E0B-000000001200}</Data><Data Name='ProcessId'>2136</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" check-license</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7F-6571-2C0B-000000001200}</Data><Data Name='ParentProcessId'>2112</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:59+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:59.919455300Z'/><EventRecordID>863</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:59.913</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7F-6571-2D0B-000000001200}</Data><Data Name='ProcessId'>10868</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" generate-ssl</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7F-6571-2C0B-000000001200}</Data><Data Name='ParentProcessId'>2112</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:59+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:59.903745100Z'/><EventRecordID>862</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:59.899</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7F-6571-2C0B-000000001200}</Data><Data Name='ProcessId'>2112</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7F-6571-2B0B-000000001200}</Data><Data Name='ParentProcessId'>6232</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt 2>&1</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:03:59+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:59.891801100Z'/><EventRecordID>861</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:59.884</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7F-6571-2B0B-000000001200}</Data><Data Name='ProcessId'>6232</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt 2>&1</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:59+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:59.373681400Z'/><EventRecordID>860</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:59.367</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7F-6571-2A0B-000000001200}</Data><Data Name='ProcessId'>5780</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list sslConfig --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7F-6571-290B-000000001200}</Data><Data Name='ParentProcessId'>2132</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list sslConfig --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:59+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:59.361360900Z'/><EventRecordID>859</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:59.356</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7F-6571-290B-000000001200}</Data><Data Name='ProcessId'>2132</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list sslConfig --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7F-6571-280B-000000001200}</Data><Data Name='ParentProcessId'>9000</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list sslConfig --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:03:59+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:59.352360800Z'/><EventRecordID>858</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:59.347</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7F-6571-280B-000000001200}</Data><Data Name='ProcessId'>9000</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list sslConfig --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-1B0B-000000001200}</Data><Data Name='ParentProcessId'>4396</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:59+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:59.081594100Z'/><EventRecordID>857</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:59.074</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7F-6571-270B-000000001200}</Data><Data Name='ProcessId'>8988</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list watchdog --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7F-6571-260B-000000001200}</Data><Data Name='ParentProcessId'>3124</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list watchdog --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:59+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:59.069930000Z'/><EventRecordID>856</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:59.065</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7F-6571-260B-000000001200}</Data><Data Name='ProcessId'>3124</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list watchdog --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7F-6571-250B-000000001200}</Data><Data Name='ParentProcessId'>9516</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list watchdog --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:03:59+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:59.062048200Z'/><EventRecordID>855</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:59.056</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7F-6571-250B-000000001200}</Data><Data Name='ProcessId'>9516</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list watchdog --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-1B0B-000000001200}</Data><Data Name='ParentProcessId'>4396</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:58+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:58.800717500Z'/><EventRecordID>854</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:58.794</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7E-6571-240B-000000001200}</Data><Data Name='ProcessId'>10980</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list kvstore --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-230B-000000001200}</Data><Data Name='ParentProcessId'>11116</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list kvstore --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:58+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:58.788526400Z'/><EventRecordID>853</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:58.784</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7E-6571-230B-000000001200}</Data><Data Name='ProcessId'>11116</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list kvstore --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-220B-000000001200}</Data><Data Name='ParentProcessId'>10412</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list kvstore --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:03:58+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:58.780893900Z'/><EventRecordID>852</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:58.775</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7E-6571-220B-000000001200}</Data><Data Name='ProcessId'>10412</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list kvstore --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-1B0B-000000001200}</Data><Data Name='ParentProcessId'>4396</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:58+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:58.514948000Z'/><EventRecordID>851</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:58.507</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7E-6571-210B-000000001200}</Data><Data Name='ProcessId'>6268</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-200B-000000001200}</Data><Data Name='ParentProcessId'>6120</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:58+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:58.503227600Z'/><EventRecordID>850</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:58.499</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7E-6571-200B-000000001200}</Data><Data Name='ProcessId'>6120</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-1F0B-000000001200}</Data><Data Name='ParentProcessId'>10992</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:03:58+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:58.494714300Z'/><EventRecordID>849</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:58.489</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7E-6571-1F0B-000000001200}</Data><Data Name='ProcessId'>10992</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-1B0B-000000001200}</Data><Data Name='ParentProcessId'>4396</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:58+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:58.224011100Z'/><EventRecordID>848</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:58.218</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7E-6571-1E0B-000000001200}</Data><Data Name='ProcessId'>9020</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool web list settings --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-1D0B-000000001200}</Data><Data Name='ParentProcessId'>10748</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool web list settings --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:58+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:58.212176800Z'/><EventRecordID>847</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:58.207</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7E-6571-1D0B-000000001200}</Data><Data Name='ProcessId'>10748</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool web list settings --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-1C0B-000000001200}</Data><Data Name='ParentProcessId'>6296</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool web list settings --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:03:58+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:58.204923000Z'/><EventRecordID>846</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:58.200</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7E-6571-1C0B-000000001200}</Data><Data Name='ProcessId'>6296</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool web list settings --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-1B0B-000000001200}</Data><Data Name='ParentProcessId'>4396</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:58+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:58.190415000Z'/><EventRecordID>845</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:58.186</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7E-6571-1B0B-000000001200}</Data><Data Name='ProcessId'>4396</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-1A0B-000000001200}</Data><Data Name='ParentProcessId'>9696</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:58+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:58.182585600Z'/><EventRecordID>844</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:58.175</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7E-6571-1A0B-000000001200}</Data><Data Name='ProcessId'>9696</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:03:58+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:58.143776800Z'/><EventRecordID>843</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:58.140</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7E-6571-180B-000000001200}</Data><Data Name='ProcessId'>9504</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _RAW_envvars</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-160B-000000001200}</Data><Data Name='ParentProcessId'>7400</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _RAW_envvars</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:58+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:58.121014000Z'/><EventRecordID>842</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:58.115</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7E-6571-160B-000000001200}</Data><Data Name='ProcessId'>7400</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _RAW_envvars</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:58+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:58.037239800Z'/><EventRecordID>841</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:58.029</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ProcessId'>9920</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0205-656E-0A00-000000001200}</Data><Data Name='ParentProcessId'>612</Data><Data Name='ParentImage'>C:\Windows\System32\services.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\services.exe</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:03:45+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:45.938962000Z'/><EventRecordID>840</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:45.927</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A71-6571-140B-000000001200}</Data><Data Name='ProcessId'>9176</Data><Data Name='Image'>C:\Program Files\Notepad++\notepad++.exe</Data><Data Name='FileVersion'>8.5.8</Data><Data Name='Description'>Notepad++</Data><Data Name='Product'>Notepad++</Data><Data Name='Company'>Don HO don.h@free.fr</Data><Data Name='OriginalFileName'>notepad++.exe</Data><Data Name='CommandLine'>"C:\Program Files\Notepad++\notepad++.exe" "C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\local\inputs.conf" </Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-AFC8-040000000000}</Data><Data Name='LogonId'>0x4c8af</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>MD5=FE341DC1732B4BA290E1C37766DD36DC,SHA256=5AA09176BB1689B87A8E0B98D32E758F5055452C4147EFCBFB91944F1752DC48,IMPHASH=B5856C8A9E980785E72BFA3C2DA2DC24</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0240-656E-5100-000000001200}</Data><Data Name='ParentProcessId'>4984</Data><Data Name='ParentImage'>C:\Windows\explorer.exe</Data><Data Name='ParentCommandLine'>C:\Windows\Explorer.EXE</Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:03:41+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:41.414480900Z'/><EventRecordID>839</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:41.410</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A6D-6571-130B-000000001200}</Data><Data Name='ProcessId'>5400</Data><Data Name='Image'>C:\Windows\System32\notepad.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Notepad</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>NOTEPAD.EXE</Data><Data Name='CommandLine'>"C:\Windows\system32\NOTEPAD.EXE" C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\local\inputs.conf</Data><Data Name='CurrentDirectory'>C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\local\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-AFC8-040000000000}</Data><Data Name='LogonId'>0x4c8af</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>MD5=3B508CAE5DEBCBA928B5BC355517E2E6,SHA256=DA0ACEE8F60A460CFB5249E262D3D53211EBC4C777579E99C8202B761541110A,IMPHASH=968239BE2020F1C0DAFFDCDBD49E9C82</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0240-656E-5100-000000001200}</Data><Data Name='ParentProcessId'>4984</Data><Data Name='ParentImage'>C:\Windows\explorer.exe</Data><Data Name='ParentCommandLine'>C:\Windows\Explorer.EXE</Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:03:24+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:24.845969500Z'/><EventRecordID>838</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>Downloads</Data><Data Name='UtcTime'>2023-12-07 09:03:24.840</Data><Data Name='ProcessGuid'>{3CBB8FBE-A67F-6570-EB02-000000001200}</Data><Data Name='ProcessId'>8620</Data><Data Name='Image'>C:\Windows\system32\SnippingTool.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\Downloads\splunk3.png</Data><Data Name='CreationUtcTime'>2023-12-07 09:03:24.761</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:03:24+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:24.772642000Z'/><EventRecordID>837</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>Downloads</Data><Data Name='UtcTime'>2023-12-07 09:03:24.761</Data><Data Name='ProcessGuid'>{3CBB8FBE-A67F-6570-EB02-000000001200}</Data><Data Name='ProcessId'>8620</Data><Data Name='Image'>C:\Windows\system32\SnippingTool.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\Downloads\splunk3.png</Data><Data Name='CreationUtcTime'>2023-12-07 09:03:24.761</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T10:03:10+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:10.089453600Z'/><EventRecordID>836</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:08.088</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A4B-6571-110B-000000001200}</Data><Data Name='ProcessId'>2036</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:08+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:08.731419200Z'/><EventRecordID>835</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:08.716</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A4C-6571-120B-000000001200}</Data><Data Name='ProcessId'>10736</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-winprintmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Windows Print Monitor </Data><Data Name='Product'>splunk Application </Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-winprintmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-winprintmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=FDEB6BA573575665D847C8C88DFA6B28,SHA256=00FC8040D205B3290D204EB5E6AEAF5E21CF6F5EDB081555CDF81AD61F306218,IMPHASH=355E487ADBCE53AA00CC9620C5813D5A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:07+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:07.961830400Z'/><EventRecordID>834</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:07.950</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A4B-6571-110B-000000001200}</Data><Data Name='ProcessId'>2036</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Monitor windows event logs</Data><Data Name='Product'>splunk Application </Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-winevtlog.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AE95292862972429C2FBD9541C739C2B,SHA256=C1899D942B83A761EADA6303334A9E6946A7206A59E678F0039D3AB527785522,IMPHASH=EDE9B13E7663B8E763DD4604CD8C3BF7</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:03:07+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:07.225591100Z'/><EventRecordID>833</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:07.215</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A4B-6571-100B-000000001200}</Data><Data Name='ProcessId'>11172</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:06+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:06.474781400Z'/><EventRecordID>832</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:06.466</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A4A-6571-0F0B-000000001200}</Data><Data Name='ProcessId'>8500</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:05+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:05.726001900Z'/><EventRecordID>831</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:05.715</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A49-6571-0E0B-000000001200}</Data><Data Name='ProcessId'>11048</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:03:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:04.976139300Z'/><EventRecordID>830</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:04.966</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A48-6571-0D0B-000000001200}</Data><Data Name='ProcessId'>9296</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-perfmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Performance monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-perfmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-perfmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=37F610EA3267B4C636A52CC17C72F5E9,SHA256=154252976F3CDC663C1999E5BF6958E4A9717874E2117061A0E40F2F1D97BE27,IMPHASH=35AE00EA6705AD0DB2C706FD3FAF93B6</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:04.210271900Z'/><EventRecordID>829</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:04.200</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A48-6571-0C0B-000000001200}</Data><Data Name='ProcessId'>10940</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:03+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:03.447675100Z'/><EventRecordID>828</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:03.434</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A47-6571-0B0B-000000001200}</Data><Data Name='ProcessId'>10376</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:03:02+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:02.696837500Z'/><EventRecordID>827</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:02.685</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A46-6571-0A0B-000000001200}</Data><Data Name='ProcessId'>10632</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:03:01+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:03:01.932167400Z'/><EventRecordID>826</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:03:01.920</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A45-6571-090B-000000001200}</Data><Data Name='ProcessId'>10944</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-wmi.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Remote Performance monitor using WMI</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-wmi.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-wmi.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=7A440F2DF244985160C5B54CDBBA547D,SHA256=7E1DBA295076C76618106FD18E882B190BF0542AD2981200D01074B021BF76CF,IMPHASH=7C7770CDB275E49574E79FDF395C7C60</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:59+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:59.981427900Z'/><EventRecordID>825</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:59.971</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A43-6571-080B-000000001200}</Data><Data Name='ProcessId'>7988</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\powershell2.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:02:59+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:59.858347300Z'/><EventRecordID>824</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:59.847</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A43-6571-070B-000000001200}</Data><Data Name='ProcessId'>1636</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\powershell.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:59+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:59.733012600Z'/><EventRecordID>823</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:59.722</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A43-6571-060B-000000001200}</Data><Data Name='ProcessId'>9808</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\perfmon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:59+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:59.606561500Z'/><EventRecordID>822</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:59.596</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A43-6571-050B-000000001200}</Data><Data Name='ProcessId'>1892</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\admon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:02:59+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:59.484304900Z'/><EventRecordID>821</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:59.471</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A43-6571-040B-000000001200}</Data><Data Name='ProcessId'>6924</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinRegMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:59+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:59.356433800Z'/><EventRecordID>820</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:59.347</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A43-6571-030B-000000001200}</Data><Data Name='ProcessId'>3868</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinPrintMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:59+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:59.231324800Z'/><EventRecordID>819</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:59.221</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A43-6571-020B-000000001200}</Data><Data Name='ProcessId'>4968</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinNetMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:02:59+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:59.107232700Z'/><EventRecordID>818</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:59.097</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A43-6571-010B-000000001200}</Data><Data Name='ProcessId'>9744</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinHostMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:58+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:58.968572600Z'/><EventRecordID>817</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:58.956</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A42-6571-000B-000000001200}</Data><Data Name='ProcessId'>9884</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinEventLog.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:58+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:58.847848600Z'/><EventRecordID>816</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:58.838</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A42-6571-FF0A-000000001200}</Data><Data Name='ProcessId'>6396</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\MonitorNoHandle.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:02:58+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:58.171729600Z'/><EventRecordID>815</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:58.168</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A42-6571-FE0A-000000001200}</Data><Data Name='ProcessId'>9972</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal check-xml-files --answer-yes --no-prompt </Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A42-6571-FD0A-000000001200}</Data><Data Name='ParentProcessId'>4828</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal check-xml-files --answer-yes --no-prompt 2>&1</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:58+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:58.161451500Z'/><EventRecordID>814</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:58.152</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A42-6571-FD0A-000000001200}</Data><Data Name='ProcessId'>4828</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal check-xml-files --answer-yes --no-prompt 2>&1</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:57+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:57.869199300Z'/><EventRecordID>813</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:57.863</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A41-6571-FC0A-000000001200}</Data><Data Name='ProcessId'>6684</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A41-6571-FB0A-000000001200}</Data><Data Name='ParentProcessId'>1064</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:02:57+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:57.856318500Z'/><EventRecordID>812</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:57.852</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A41-6571-FB0A-000000001200}</Data><Data Name='ProcessId'>1064</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A41-6571-FA0A-000000001200}</Data><Data Name='ParentProcessId'>1772</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:57+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:57.849114400Z'/><EventRecordID>811</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:57.839</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A41-6571-FA0A-000000001200}</Data><Data Name='ProcessId'>1772</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3E-6571-EC0A-000000001200}</Data><Data Name='ParentProcessId'>364</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:57+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:57.575557400Z'/><EventRecordID>810</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:57.568</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A41-6571-F90A-000000001200}</Data><Data Name='ProcessId'>9172</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list replication_port --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A41-6571-F80A-000000001200}</Data><Data Name='ParentProcessId'>3192</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list replication_port --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:02:57+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:57.564238300Z'/><EventRecordID>809</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:57.559</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A41-6571-F80A-000000001200}</Data><Data Name='ProcessId'>3192</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list replication_port --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A41-6571-F70A-000000001200}</Data><Data Name='ParentProcessId'>8376</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list replication_port --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:57+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:57.555967100Z'/><EventRecordID>808</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:57.551</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A41-6571-F70A-000000001200}</Data><Data Name='ProcessId'>8376</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list replication_port --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3E-6571-EC0A-000000001200}</Data><Data Name='ParentProcessId'>364</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:57+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:57.238571500Z'/><EventRecordID>807</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:57.231</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A41-6571-F60A-000000001200}</Data><Data Name='ProcessId'>8164</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd" check-transforms-keys</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3E-6571-EC0A-000000001200}</Data><Data Name='ParentProcessId'>364</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:02:56+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:56.679970300Z'/><EventRecordID>806</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:56.671</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A40-6571-F40A-000000001200}</Data><Data Name='ProcessId'>5620</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool validate-regex --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A40-6571-F30A-000000001200}</Data><Data Name='ParentProcessId'>8520</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-regex --log-warnings</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:56+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:56.664922300Z'/><EventRecordID>805</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:56.660</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A40-6571-F30A-000000001200}</Data><Data Name='ProcessId'>8520</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-regex --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3E-6571-EC0A-000000001200}</Data><Data Name='ParentProcessId'>364</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:56+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:56.188671400Z'/><EventRecordID>804</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:56.183</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A40-6571-F20A-000000001200}</Data><Data Name='ProcessId'>2372</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool validate-strptime --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A40-6571-F10A-000000001200}</Data><Data Name='ParentProcessId'>9132</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-strptime --log-warnings</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:02:56+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:56.177615000Z'/><EventRecordID>803</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:56.172</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A40-6571-F10A-000000001200}</Data><Data Name='ProcessId'>9132</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>" C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-strptime --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3E-6571-EC0A-000000001200}</Data><Data Name='ParentProcessId'>364</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:55+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:55.589004500Z'/><EventRecordID>802</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:55.583</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3F-6571-F00A-000000001200}</Data><Data Name='ProcessId'>2460</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool check --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3F-6571-EF0A-000000001200}</Data><Data Name='ParentProcessId'>10140</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" check --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:55+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:55.578776500Z'/><EventRecordID>801</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:55.572</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3F-6571-EF0A-000000001200}</Data><Data Name='ProcessId'>10140</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>" C:\Program Files\SplunkUniversalForwarder\bin\btool" check --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3E-6571-EC0A-000000001200}</Data><Data Name='ParentProcessId'>364</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:02:55+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:55.292721800Z'/><EventRecordID>800</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:55.286</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3F-6571-EE0A-000000001200}</Data><Data Name='ProcessId'>6988</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" check-license</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3E-6571-EC0A-000000001200}</Data><Data Name='ParentProcessId'>364</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:55+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:55.000449500Z'/><EventRecordID>799</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:54.994</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3E-6571-ED0A-000000001200}</Data><Data Name='ProcessId'>5148</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" generate-ssl</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3E-6571-EC0A-000000001200}</Data><Data Name='ParentProcessId'>364</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:54+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:54.986957100Z'/><EventRecordID>798</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:54.982</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3E-6571-EC0A-000000001200}</Data><Data Name='ProcessId'>364</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3E-6571-EB0A-000000001200}</Data><Data Name='ParentProcessId'>7380</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt 2>&1</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:02:54+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:54.974756700Z'/><EventRecordID>797</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:54.967</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3E-6571-EB0A-000000001200}</Data><Data Name='ProcessId'>7380</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt 2>&1</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:54+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:54.461554200Z'/><EventRecordID>796</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:54.456</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3E-6571-EA0A-000000001200}</Data><Data Name='ProcessId'>6068</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list sslConfig --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3E-6571-E90A-000000001200}</Data><Data Name='ParentProcessId'>6344</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list sslConfig --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:54+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:54.449693800Z'/><EventRecordID>795</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:54.445</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3E-6571-E90A-000000001200}</Data><Data Name='ProcessId'>6344</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list sslConfig --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3E-6571-E80A-000000001200}</Data><Data Name='ParentProcessId'>9076</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list sslConfig --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:02:54+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:54.441536500Z'/><EventRecordID>794</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:54.437</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3E-6571-E80A-000000001200}</Data><Data Name='ProcessId'>9076</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list sslConfig --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-DB0A-000000001200}</Data><Data Name='ParentProcessId'>7228</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:54+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:54.174876300Z'/><EventRecordID>793</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:54.165</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3E-6571-E70A-000000001200}</Data><Data Name='ProcessId'>7468</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list watchdog --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3E-6571-E60A-000000001200}</Data><Data Name='ParentProcessId'>5672</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list watchdog --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:54+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:54.160748800Z'/><EventRecordID>792</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:54.156</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3E-6571-E60A-000000001200}</Data><Data Name='ProcessId'>5672</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list watchdog --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3E-6571-E50A-000000001200}</Data><Data Name='ParentProcessId'>8516</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list watchdog --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:02:54+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:54.150747800Z'/><EventRecordID>791</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:54.146</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3E-6571-E50A-000000001200}</Data><Data Name='ProcessId'>8516</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list watchdog --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-DB0A-000000001200}</Data><Data Name='ParentProcessId'>7228</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:53+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:53.857040200Z'/><EventRecordID>790</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:53.851</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3D-6571-E40A-000000001200}</Data><Data Name='ProcessId'>6452</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list kvstore --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-E30A-000000001200}</Data><Data Name='ParentProcessId'>7448</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list kvstore --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:53+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:53.844246000Z'/><EventRecordID>789</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:53.838</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3D-6571-E30A-000000001200}</Data><Data Name='ProcessId'>7448</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list kvstore --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-E20A-000000001200}</Data><Data Name='ParentProcessId'>2924</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list kvstore --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:02:53+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:53.835077500Z'/><EventRecordID>788</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:53.831</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3D-6571-E20A-000000001200}</Data><Data Name='ProcessId'>2924</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list kvstore --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-DB0A-000000001200}</Data><Data Name='ParentProcessId'>7228</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:53+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:53.553080500Z'/><EventRecordID>787</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:53.545</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3D-6571-E10A-000000001200}</Data><Data Name='ProcessId'>8440</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-E00A-000000001200}</Data><Data Name='ParentProcessId'>10460</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:53+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:53.541201800Z'/><EventRecordID>786</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:53.537</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3D-6571-E00A-000000001200}</Data><Data Name='ProcessId'>10460</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-DF0A-000000001200}</Data><Data Name='ParentProcessId'>1576</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:02:53+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:53.532588500Z'/><EventRecordID>785</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:53.526</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3D-6571-DF0A-000000001200}</Data><Data Name='ProcessId'>1576</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-DB0A-000000001200}</Data><Data Name='ParentProcessId'>7228</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:53+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:53.259223500Z'/><EventRecordID>784</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:53.252</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3D-6571-DE0A-000000001200}</Data><Data Name='ProcessId'>7724</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool web list settings --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-DD0A-000000001200}</Data><Data Name='ParentProcessId'>6348</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool web list settings --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:53+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:53.245253200Z'/><EventRecordID>783</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:53.240</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3D-6571-DD0A-000000001200}</Data><Data Name='ProcessId'>6348</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool web list settings --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-DC0A-000000001200}</Data><Data Name='ParentProcessId'>9680</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool web list settings --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:02:53+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:53.237032400Z'/><EventRecordID>782</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:53.232</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3D-6571-DC0A-000000001200}</Data><Data Name='ProcessId'>9680</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool web list settings --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-DB0A-000000001200}</Data><Data Name='ParentProcessId'>7228</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:53+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:53.222339900Z'/><EventRecordID>781</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:53.218</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3D-6571-DB0A-000000001200}</Data><Data Name='ProcessId'>7228</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-DA0A-000000001200}</Data><Data Name='ParentProcessId'>7596</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:53+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:53.215396800Z'/><EventRecordID>780</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:53.207</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3D-6571-DA0A-000000001200}</Data><Data Name='ProcessId'>7596</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:02:53+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:53.172135000Z'/><EventRecordID>779</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:53.167</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3D-6571-D80A-000000001200}</Data><Data Name='ProcessId'>2856</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _RAW_envvars</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D60A-000000001200}</Data><Data Name='ParentProcessId'>6856</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _RAW_envvars</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:53+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:53.145270600Z'/><EventRecordID>778</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:53.138</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3D-6571-D60A-000000001200}</Data><Data Name='ProcessId'>6856</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _RAW_envvars</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ParentProcessId'>7392</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:53+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:53.053181100Z'/><EventRecordID>777</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:53.044</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A3D-6571-D50A-000000001200}</Data><Data Name='ProcessId'>7392</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0205-656E-0A00-000000001200}</Data><Data Name='ParentProcessId'>612</Data><Data Name='ParentImage'>C:\Windows\System32\services.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\services.exe</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:02:44+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:44.004869100Z'/><EventRecordID>776</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:43.996</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A33-6571-D40A-000000001200}</Data><Data Name='ProcessId'>8964</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:43.192468800Z'/><EventRecordID>775</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:43.184</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A33-6571-D30A-000000001200}</Data><Data Name='ProcessId'>7336</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:42.429266300Z'/><EventRecordID>774</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:42.419</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A32-6571-D20A-000000001200}</Data><Data Name='ProcessId'>6208</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:02:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:40.943915800Z'/><EventRecordID>773</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:40.934</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A30-6571-D10A-000000001200}</Data><Data Name='ProcessId'>2304</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:40.177573700Z'/><EventRecordID>772</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:40.168</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A30-6571-D00A-000000001200}</Data><Data Name='ProcessId'>7156</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:02:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:02:39.396272400Z'/><EventRecordID>771</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:02:39.387</Data><Data Name='ProcessGuid'>{3CBB8FBE-8A2F-6571-CF0A-000000001200}</Data><Data Name='ProcessId'>872</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:46+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:46.885799800Z'/><EventRecordID>770</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:44.872</Data><Data Name='ProcessGuid'>{3CBB8FBE-89F8-6571-CD0A-000000001200}</Data><Data Name='ProcessId'>9660</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:45+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:45.489287600Z'/><EventRecordID>769</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:45.480</Data><Data Name='ProcessGuid'>{3CBB8FBE-89F9-6571-CE0A-000000001200}</Data><Data Name='ProcessId'>6304</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-winprintmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Windows Print Monitor </Data><Data Name='Product'>splunk Application </Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-winprintmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-winprintmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=FDEB6BA573575665D847C8C88DFA6B28,SHA256=00FC8040D205B3290D204EB5E6AEAF5E21CF6F5EDB081555CDF81AD61F306218,IMPHASH=355E487ADBCE53AA00CC9620C5813D5A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:44+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:44.739157900Z'/><EventRecordID>768</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:44.730</Data><Data Name='ProcessGuid'>{3CBB8FBE-89F8-6571-CD0A-000000001200}</Data><Data Name='ProcessId'>9660</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Monitor windows event logs</Data><Data Name='Product'>splunk Application </Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-winevtlog.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AE95292862972429C2FBD9541C739C2B,SHA256=C1899D942B83A761EADA6303334A9E6946A7206A59E678F0039D3AB527785522,IMPHASH=EDE9B13E7663B8E763DD4604CD8C3BF7</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:43.990290500Z'/><EventRecordID>767</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:43.980</Data><Data Name='ProcessGuid'>{3CBB8FBE-89F7-6571-CC0A-000000001200}</Data><Data Name='ProcessId'>7092</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:43.223615000Z'/><EventRecordID>766</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:43.188</Data><Data Name='ProcessGuid'>{3CBB8FBE-89F7-6571-CB0A-000000001200}</Data><Data Name='ProcessId'>5208</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:42.426448500Z'/><EventRecordID>765</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:42.417</Data><Data Name='ProcessGuid'>{3CBB8FBE-89F6-6571-CA0A-000000001200}</Data><Data Name='ProcessId'>8988</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:41+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:41.661651300Z'/><EventRecordID>764</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:41.652</Data><Data Name='ProcessGuid'>{3CBB8FBE-89F5-6571-C90A-000000001200}</Data><Data Name='ProcessId'>1004</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-perfmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Performance monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-perfmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-perfmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=37F610EA3267B4C636A52CC17C72F5E9,SHA256=154252976F3CDC663C1999E5BF6958E4A9717874E2117061A0E40F2F1D97BE27,IMPHASH=35AE00EA6705AD0DB2C706FD3FAF93B6</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:40.911425100Z'/><EventRecordID>763</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:40.902</Data><Data Name='ProcessGuid'>{3CBB8FBE-89F4-6571-C80A-000000001200}</Data><Data Name='ProcessId'>11000</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:40.144369200Z'/><EventRecordID>762</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:40.136</Data><Data Name='ProcessGuid'>{3CBB8FBE-89F4-6571-C70A-000000001200}</Data><Data Name='ProcessId'>5364</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:39.394193700Z'/><EventRecordID>761</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:39.386</Data><Data Name='ProcessGuid'>{3CBB8FBE-89F3-6571-C60A-000000001200}</Data><Data Name='ProcessId'>10980</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:38+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:38.656541000Z'/><EventRecordID>760</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:38.637</Data><Data Name='ProcessGuid'>{3CBB8FBE-89F2-6571-C50A-000000001200}</Data><Data Name='ProcessId'>10060</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-wmi.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Remote Performance monitor using WMI</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-wmi.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-wmi.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=7A440F2DF244985160C5B54CDBBA547D,SHA256=7E1DBA295076C76618106FD18E882B190BF0542AD2981200D01074B021BF76CF,IMPHASH=7C7770CDB275E49574E79FDF395C7C60</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:36+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:36.699211300Z'/><EventRecordID>759</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:36.688</Data><Data Name='ProcessGuid'>{3CBB8FBE-89F0-6571-C40A-000000001200}</Data><Data Name='ProcessId'>11192</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\powershell2.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:36+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:36.575040500Z'/><EventRecordID>758</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:36.564</Data><Data Name='ProcessGuid'>{3CBB8FBE-89F0-6571-C30A-000000001200}</Data><Data Name='ProcessId'>10416</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\powershell.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:36+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:36.450822700Z'/><EventRecordID>757</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:36.440</Data><Data Name='ProcessGuid'>{3CBB8FBE-89F0-6571-C20A-000000001200}</Data><Data Name='ProcessId'>11116</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\perfmon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:36+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:36.309239500Z'/><EventRecordID>756</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:36.298</Data><Data Name='ProcessGuid'>{3CBB8FBE-89F0-6571-C10A-000000001200}</Data><Data Name='ProcessId'>10476</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\admon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:36+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:36.183866100Z'/><EventRecordID>755</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:36.173</Data><Data Name='ProcessGuid'>{3CBB8FBE-89F0-6571-C00A-000000001200}</Data><Data Name='ProcessId'>8124</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinRegMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:36+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:36.058801100Z'/><EventRecordID>754</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:36.048</Data><Data Name='ProcessGuid'>{3CBB8FBE-89F0-6571-BF0A-000000001200}</Data><Data Name='ProcessId'>10412</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinPrintMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:35.936184300Z'/><EventRecordID>753</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:35.924</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EF-6571-BE0A-000000001200}</Data><Data Name='ProcessId'>10408</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinNetMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:35.805119700Z'/><EventRecordID>752</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:35.784</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EF-6571-BD0A-000000001200}</Data><Data Name='ProcessId'>11212</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinHostMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:35.667711700Z'/><EventRecordID>751</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:35.657</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EF-6571-BC0A-000000001200}</Data><Data Name='ProcessId'>9384</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinEventLog.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:35.540873400Z'/><EventRecordID>750</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:35.531</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EF-6571-BB0A-000000001200}</Data><Data Name='ProcessId'>5468</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\MonitorNoHandle.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:34.871368200Z'/><EventRecordID>749</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:34.867</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EE-6571-BA0A-000000001200}</Data><Data Name='ProcessId'>10540</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal check-xml-files --answer-yes --no-prompt </Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EE-6571-B90A-000000001200}</Data><Data Name='ParentProcessId'>10992</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal check-xml-files --answer-yes --no-prompt 2>&1</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:34.860605500Z'/><EventRecordID>748</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:34.850</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EE-6571-B90A-000000001200}</Data><Data Name='ProcessId'>10992</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal check-xml-files --answer-yes --no-prompt 2>&1</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:34.570265900Z'/><EventRecordID>747</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:34.564</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EE-6571-B80A-000000001200}</Data><Data Name='ProcessId'>10320</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EE-6571-B70A-000000001200}</Data><Data Name='ParentProcessId'>9020</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:34.558800100Z'/><EventRecordID>746</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:34.554</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EE-6571-B70A-000000001200}</Data><Data Name='ProcessId'>9020</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EE-6571-B60A-000000001200}</Data><Data Name='ParentProcessId'>8448</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:34.550118300Z'/><EventRecordID>745</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:34.544</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EE-6571-B60A-000000001200}</Data><Data Name='ProcessId'>8448</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EB-6571-A90A-000000001200}</Data><Data Name='ParentProcessId'>9112</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:34.278423000Z'/><EventRecordID>744</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:34.272</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EE-6571-B50A-000000001200}</Data><Data Name='ProcessId'>10748</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list replication_port --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EE-6571-B40A-000000001200}</Data><Data Name='ParentProcessId'>4848</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list replication_port --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:34.266135100Z'/><EventRecordID>743</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:34.261</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EE-6571-B40A-000000001200}</Data><Data Name='ProcessId'>4848</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list replication_port --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EE-6571-B30A-000000001200}</Data><Data Name='ParentProcessId'>10332</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list replication_port --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:34.258383900Z'/><EventRecordID>742</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:34.253</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EE-6571-B30A-000000001200}</Data><Data Name='ProcessId'>10332</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list replication_port --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EB-6571-A90A-000000001200}</Data><Data Name='ParentProcessId'>9112</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:33.945802500Z'/><EventRecordID>741</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:33.939</Data><Data Name='ProcessGuid'>{3CBB8FBE-89ED-6571-B20A-000000001200}</Data><Data Name='ProcessId'>10396</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd" check-transforms-keys</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EB-6571-A90A-000000001200}</Data><Data Name='ParentProcessId'>9112</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:33.397293800Z'/><EventRecordID>740</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:33.391</Data><Data Name='ProcessGuid'>{3CBB8FBE-89ED-6571-B10A-000000001200}</Data><Data Name='ProcessId'>6296</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool validate-regex --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89ED-6571-B00A-000000001200}</Data><Data Name='ParentProcessId'>10592</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-regex --log-warnings</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:33.385038200Z'/><EventRecordID>739</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:33.378</Data><Data Name='ProcessGuid'>{3CBB8FBE-89ED-6571-B00A-000000001200}</Data><Data Name='ProcessId'>10592</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-regex --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EB-6571-A90A-000000001200}</Data><Data Name='ParentProcessId'>9112</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:32.907690000Z'/><EventRecordID>738</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:32.900</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EC-6571-AF0A-000000001200}</Data><Data Name='ProcessId'>10380</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool validate-strptime --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EC-6571-AE0A-000000001200}</Data><Data Name='ParentProcessId'>10280</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-strptime --log-warnings</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:32.896544600Z'/><EventRecordID>737</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:32.891</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EC-6571-AE0A-000000001200}</Data><Data Name='ProcessId'>10280</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>" C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-strptime --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EB-6571-A90A-000000001200}</Data><Data Name='ParentProcessId'>9112</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:32.288159500Z'/><EventRecordID>736</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:32.281</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EC-6571-AD0A-000000001200}</Data><Data Name='ProcessId'>4396</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool check --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EC-6571-AC0A-000000001200}</Data><Data Name='ParentProcessId'>11024</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" check --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:32.274795900Z'/><EventRecordID>735</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:32.270</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EC-6571-AC0A-000000001200}</Data><Data Name='ProcessId'>11024</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>" C:\Program Files\SplunkUniversalForwarder\bin\btool" check --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EB-6571-A90A-000000001200}</Data><Data Name='ParentProcessId'>9112</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:31+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:31.983347400Z'/><EventRecordID>734</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:31.976</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EB-6571-AB0A-000000001200}</Data><Data Name='ProcessId'>2636</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" check-license</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EB-6571-A90A-000000001200}</Data><Data Name='ParentProcessId'>9112</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:31+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:31.680669000Z'/><EventRecordID>733</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:31.674</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EB-6571-AA0A-000000001200}</Data><Data Name='ProcessId'>5388</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" generate-ssl</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EB-6571-A90A-000000001200}</Data><Data Name='ParentProcessId'>9112</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:31+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:31.665677000Z'/><EventRecordID>732</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:31.660</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EB-6571-A90A-000000001200}</Data><Data Name='ProcessId'>9112</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EB-6571-A80A-000000001200}</Data><Data Name='ParentProcessId'>9104</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt 2>&1</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:31+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:31.655446800Z'/><EventRecordID>731</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:31.646</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EB-6571-A80A-000000001200}</Data><Data Name='ProcessId'>9104</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt 2>&1</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:31+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:31.120779500Z'/><EventRecordID>730</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:31.114</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EB-6571-A70A-000000001200}</Data><Data Name='ProcessId'>9044</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list sslConfig --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EB-6571-A60A-000000001200}</Data><Data Name='ParentProcessId'>8408</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list sslConfig --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:31+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:31.108075000Z'/><EventRecordID>729</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:31.103</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EB-6571-A60A-000000001200}</Data><Data Name='ProcessId'>8408</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list sslConfig --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EB-6571-A50A-000000001200}</Data><Data Name='ParentProcessId'>9720</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list sslConfig --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:31+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:31.098905600Z'/><EventRecordID>728</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:31.093</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EB-6571-A50A-000000001200}</Data><Data Name='ProcessId'>9720</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list sslConfig --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-980A-000000001200}</Data><Data Name='ParentProcessId'>9964</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:30.818962900Z'/><EventRecordID>727</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:30.812</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EA-6571-A40A-000000001200}</Data><Data Name='ProcessId'>5800</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list watchdog --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EA-6571-A30A-000000001200}</Data><Data Name='ParentProcessId'>2144</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list watchdog --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:30.806454000Z'/><EventRecordID>726</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:30.801</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EA-6571-A30A-000000001200}</Data><Data Name='ProcessId'>2144</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list watchdog --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EA-6571-A20A-000000001200}</Data><Data Name='ParentProcessId'>5816</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list watchdog --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:30.798541500Z'/><EventRecordID>725</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:30.793</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EA-6571-A20A-000000001200}</Data><Data Name='ProcessId'>5816</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list watchdog --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-980A-000000001200}</Data><Data Name='ParentProcessId'>9964</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:30.524641000Z'/><EventRecordID>724</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:30.518</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EA-6571-A10A-000000001200}</Data><Data Name='ProcessId'>3260</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list kvstore --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EA-6571-A00A-000000001200}</Data><Data Name='ParentProcessId'>9376</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list kvstore --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:30.512130300Z'/><EventRecordID>723</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:30.506</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EA-6571-A00A-000000001200}</Data><Data Name='ProcessId'>9376</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list kvstore --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EA-6571-9F0A-000000001200}</Data><Data Name='ParentProcessId'>5368</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list kvstore --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:30.503718200Z'/><EventRecordID>722</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:30.499</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EA-6571-9F0A-000000001200}</Data><Data Name='ProcessId'>5368</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list kvstore --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-980A-000000001200}</Data><Data Name='ParentProcessId'>9964</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:30.238001700Z'/><EventRecordID>721</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:30.231</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EA-6571-9E0A-000000001200}</Data><Data Name='ProcessId'>8984</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EA-6571-9D0A-000000001200}</Data><Data Name='ParentProcessId'>9504</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:30.225329200Z'/><EventRecordID>720</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:30.221</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EA-6571-9D0A-000000001200}</Data><Data Name='ProcessId'>9504</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89EA-6571-9C0A-000000001200}</Data><Data Name='ParentProcessId'>1264</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:30.217744800Z'/><EventRecordID>719</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:30.213</Data><Data Name='ProcessGuid'>{3CBB8FBE-89EA-6571-9C0A-000000001200}</Data><Data Name='ProcessId'>1264</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-980A-000000001200}</Data><Data Name='ParentProcessId'>9964</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:29.952842000Z'/><EventRecordID>718</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:29.944</Data><Data Name='ProcessGuid'>{3CBB8FBE-89E9-6571-9B0A-000000001200}</Data><Data Name='ProcessId'>8056</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool web list settings --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-9A0A-000000001200}</Data><Data Name='ParentProcessId'>8032</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool web list settings --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:29.939766500Z'/><EventRecordID>717</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:29.935</Data><Data Name='ProcessGuid'>{3CBB8FBE-89E9-6571-9A0A-000000001200}</Data><Data Name='ProcessId'>8032</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool web list settings --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-990A-000000001200}</Data><Data Name='ParentProcessId'>9532</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool web list settings --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:29.930803400Z'/><EventRecordID>716</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:29.925</Data><Data Name='ProcessGuid'>{3CBB8FBE-89E9-6571-990A-000000001200}</Data><Data Name='ProcessId'>9532</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool web list settings --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-980A-000000001200}</Data><Data Name='ParentProcessId'>9964</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:29.916083400Z'/><EventRecordID>715</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:29.912</Data><Data Name='ProcessGuid'>{3CBB8FBE-89E9-6571-980A-000000001200}</Data><Data Name='ProcessId'>9964</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-970A-000000001200}</Data><Data Name='ParentProcessId'>9696</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:29.907937600Z'/><EventRecordID>714</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:29.901</Data><Data Name='ProcessGuid'>{3CBB8FBE-89E9-6571-970A-000000001200}</Data><Data Name='ProcessId'>9696</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:29.865262400Z'/><EventRecordID>713</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:29.861</Data><Data Name='ProcessGuid'>{3CBB8FBE-89E9-6571-950A-000000001200}</Data><Data Name='ProcessId'>9448</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _RAW_envvars</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-930A-000000001200}</Data><Data Name='ParentProcessId'>8464</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _RAW_envvars</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:29.838964600Z'/><EventRecordID>712</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:29.833</Data><Data Name='ProcessGuid'>{3CBB8FBE-89E9-6571-930A-000000001200}</Data><Data Name='ProcessId'>8464</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _RAW_envvars</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ParentProcessId'>8368</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:29.754695200Z'/><EventRecordID>711</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:29.746</Data><Data Name='ProcessGuid'>{3CBB8FBE-89E9-6571-920A-000000001200}</Data><Data Name='ProcessId'>8368</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0205-656E-0A00-000000001200}</Data><Data Name='ParentProcessId'>612</Data><Data Name='ParentImage'>C:\Windows\System32\services.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\services.exe</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:20.208074100Z'/><EventRecordID>710</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:20.198</Data><Data Name='ProcessGuid'>{3CBB8FBE-89E0-6571-910A-000000001200}</Data><Data Name='ProcessId'>7716</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:19.441476900Z'/><EventRecordID>709</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:19.432</Data><Data Name='ProcessGuid'>{3CBB8FBE-89DF-6571-900A-000000001200}</Data><Data Name='ProcessId'>8540</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:18.630507600Z'/><EventRecordID>708</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:18.620</Data><Data Name='ProcessGuid'>{3CBB8FBE-89DE-6571-8F0A-000000001200}</Data><Data Name='ProcessId'>8960</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:01:17+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:17.052766000Z'/><EventRecordID>707</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:17.043</Data><Data Name='ProcessGuid'>{3CBB8FBE-89DD-6571-8E0A-000000001200}</Data><Data Name='ProcessId'>4036</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:16.302193800Z'/><EventRecordID>706</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:16.292</Data><Data Name='ProcessGuid'>{3CBB8FBE-89DC-6571-8D0A-000000001200}</Data><Data Name='ProcessId'>4492</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:01:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:01:15.536254700Z'/><EventRecordID>705</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:01:15.526</Data><Data Name='ProcessGuid'>{3CBB8FBE-89DB-6571-8C0A-000000001200}</Data><Data Name='ProcessId'>4488</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:00:52+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:00:52.393456500Z'/><EventRecordID>704</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:00:52.382</Data><Data Name='ProcessGuid'>{3CBB8FBE-89C4-6571-8B0A-000000001200}</Data><Data Name='ProcessId'>6464</Data><Data Name='Image'>C:\Program Files\Notepad++\notepad++.exe</Data><Data Name='FileVersion'>8.5.8</Data><Data Name='Description'>Notepad++</Data><Data Name='Product'>Notepad++</Data><Data Name='Company'>Don HO don.h@free.fr</Data><Data Name='OriginalFileName'>notepad++.exe</Data><Data Name='CommandLine'>"C:\Program Files\Notepad++\notepad++.exe" "C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\local\inputs.conf" </Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-AFC8-040000000000}</Data><Data Name='LogonId'>0x4c8af</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>MD5=FE341DC1732B4BA290E1C37766DD36DC,SHA256=5AA09176BB1689B87A8E0B98D32E758F5055452C4147EFCBFB91944F1752DC48,IMPHASH=B5856C8A9E980785E72BFA3C2DA2DC24</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0240-656E-5100-000000001200}</Data><Data Name='ParentProcessId'>4984</Data><Data Name='ParentImage'>C:\Windows\explorer.exe</Data><Data Name='ParentCommandLine'>C:\Windows\Explorer.EXE</Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:00:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:00:30.626571200Z'/><EventRecordID>703</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:00:30.622</Data><Data Name='ProcessGuid'>{3CBB8FBE-89AE-6571-8A0A-000000001200}</Data><Data Name='ProcessId'>6812</Data><Data Name='Image'>C:\Windows\System32\notepad.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Notepad</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>NOTEPAD.EXE</Data><Data Name='CommandLine'>"C:\Windows\system32\NOTEPAD.EXE" C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\local\inputs.conf</Data><Data Name='CurrentDirectory'>C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\local\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-AFC8-040000000000}</Data><Data Name='LogonId'>0x4c8af</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>MD5=3B508CAE5DEBCBA928B5BC355517E2E6,SHA256=DA0ACEE8F60A460CFB5249E262D3D53211EBC4C777579E99C8202B761541110A,IMPHASH=968239BE2020F1C0DAFFDCDBD49E9C82</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0240-656E-5100-000000001200}</Data><Data Name='ParentProcessId'>4984</Data><Data Name='ParentImage'>C:\Windows\explorer.exe</Data><Data Name='ParentCommandLine'>C:\Windows\Explorer.EXE</Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T10:00:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:00:30.562953400Z'/><EventRecordID>702</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:00:30.558</Data><Data Name='ProcessGuid'>{3CBB8FBE-89AE-6571-890A-000000001200}</Data><Data Name='ProcessId'>9564</Data><Data Name='Image'>C:\Windows\System32\smartscreen.exe</Data><Data Name='FileVersion'>10.0.14393.1715 (rs1_release_inmarket.170906-1810)</Data><Data Name='Description'>SmartScreen</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>smartscreen.exe</Data><Data Name='CommandLine'>C:\Windows\System32\smartscreen.exe -Embedding</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-AFC8-040000000000}</Data><Data Name='LogonId'>0x4c8af</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>MD5=4A619778CC5B53F92CA6750F840455B7,SHA256=01114EE31AA9B24B6BDD67C3E0AD89C5C758D8AD416A7851E4F24937A57C5223,IMPHASH=A88BD4C4BF193E3DD40E8408EB103B65</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0205-656E-0C00-000000001200}</Data><Data Name='ParentProcessId'>788</Data><Data Name='ParentImage'>C:\Windows\System32\svchost.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\svchost.exe -k DcomLaunch</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:00:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:00:20.206534100Z'/><EventRecordID>701</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:00:20.197</Data><Data Name='ProcessGuid'>{3CBB8FBE-89A4-6571-870A-000000001200}</Data><Data Name='ProcessId'>6636</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:00:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:00:19.439261800Z'/><EventRecordID>700</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:00:19.431</Data><Data Name='ProcessGuid'>{3CBB8FBE-89A3-6571-860A-000000001200}</Data><Data Name='ProcessId'>1576</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:00:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:00:18.627172500Z'/><EventRecordID>699</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:00:18.619</Data><Data Name='ProcessGuid'>{3CBB8FBE-89A2-6571-850A-000000001200}</Data><Data Name='ProcessId'>556</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T10:00:17+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:00:17.053075800Z'/><EventRecordID>698</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:00:17.042</Data><Data Name='ProcessGuid'>{3CBB8FBE-89A1-6571-840A-000000001200}</Data><Data Name='ProcessId'>9556</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:00:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:00:16.302085700Z'/><EventRecordID>697</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:00:16.290</Data><Data Name='ProcessGuid'>{3CBB8FBE-89A0-6571-830A-000000001200}</Data><Data Name='ProcessId'>7596</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T10:00:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T09:00:15.533657000Z'/><EventRecordID>696</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:00:15.525</Data><Data Name='ProcessGuid'>{3CBB8FBE-899F-6571-820A-000000001200}</Data><Data Name='ProcessId'>9492</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:59:53+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:59:53.133457600Z'/><EventRecordID>695</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>Downloads</Data><Data Name='UtcTime'>2023-12-07 08:59:53.117</Data><Data Name='ProcessGuid'>{3CBB8FBE-A67F-6570-EB02-000000001200}</Data><Data Name='ProcessId'>8620</Data><Data Name='Image'>C:\Windows\system32\SnippingTool.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\Downloads\splunk2.png</Data><Data Name='CreationUtcTime'>2023-12-07 08:59:53.054</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:59:53+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:59:53.067334100Z'/><EventRecordID>694</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>Downloads</Data><Data Name='UtcTime'>2023-12-07 08:59:53.054</Data><Data Name='ProcessGuid'>{3CBB8FBE-A67F-6570-EB02-000000001200}</Data><Data Name='ProcessId'>8620</Data><Data Name='Image'>C:\Windows\system32\SnippingTool.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\Downloads\splunk2.png</Data><Data Name='CreationUtcTime'>2023-12-07 08:59:53.054</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:59:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:59:33.598931100Z'/><EventRecordID>693</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>Downloads</Data><Data Name='UtcTime'>2023-12-07 08:59:33.569</Data><Data Name='ProcessGuid'>{3CBB8FBE-A67F-6570-EB02-000000001200}</Data><Data Name='ProcessId'>8620</Data><Data Name='Image'>C:\Windows\system32\SnippingTool.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\Downloads\splunk.png</Data><Data Name='CreationUtcTime'>2023-12-07 08:59:33.523</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:59:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:59:33.534958700Z'/><EventRecordID>692</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>Downloads</Data><Data Name='UtcTime'>2023-12-07 08:59:33.523</Data><Data Name='ProcessGuid'>{3CBB8FBE-A67F-6570-EB02-000000001200}</Data><Data Name='ProcessId'>8620</Data><Data Name='Image'>C:\Windows\system32\SnippingTool.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\Downloads\splunk.png</Data><Data Name='CreationUtcTime'>2023-12-07 08:59:33.523</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:59:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:59:20.206425700Z'/><EventRecordID>691</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:59:20.195</Data><Data Name='ProcessGuid'>{3CBB8FBE-8968-6571-810A-000000001200}</Data><Data Name='ProcessId'>9096</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:59:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:59:19.439436900Z'/><EventRecordID>690</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:59:19.429</Data><Data Name='ProcessGuid'>{3CBB8FBE-8967-6571-800A-000000001200}</Data><Data Name='ProcessId'>3776</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:59:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:59:18.613016500Z'/><EventRecordID>689</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:59:18.602</Data><Data Name='ProcessGuid'>{3CBB8FBE-8966-6571-7F0A-000000001200}</Data><Data Name='ProcessId'>8680</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:59:17+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:59:17.050722000Z'/><EventRecordID>688</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:59:17.040</Data><Data Name='ProcessGuid'>{3CBB8FBE-8965-6571-7E0A-000000001200}</Data><Data Name='ProcessId'>6140</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:59:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:59:16.741708600Z'/><EventRecordID>687</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:59:14.748</Data><Data Name='ProcessGuid'>{3CBB8FBE-54F8-6570-7602-000000001200}</Data><Data Name='ProcessId'>8224</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\system32\mmc.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T09:59:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:59:16.283568400Z'/><EventRecordID>686</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:59:16.273</Data><Data Name='ProcessGuid'>{3CBB8FBE-8964-6571-7D0A-000000001200}</Data><Data Name='ProcessId'>3124</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:59:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:59:15.726450400Z'/><EventRecordID>685</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:59:14.733</Data><Data Name='ProcessGuid'>{3CBB8FBE-02ED-656E-7900-000000001200}</Data><Data Name='ProcessId'>5288</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\mmc.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:59:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:59:15.535103100Z'/><EventRecordID>684</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:59:15.523</Data><Data Name='ProcessGuid'>{3CBB8FBE-8963-6571-7C0A-000000001200}</Data><Data Name='ProcessId'>8920</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:58:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:58:20.178489700Z'/><EventRecordID>683</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:58:20.167</Data><Data Name='ProcessGuid'>{3CBB8FBE-892C-6571-7B0A-000000001200}</Data><Data Name='ProcessId'>11156</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:58:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:58:19.424328500Z'/><EventRecordID>682</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:58:19.414</Data><Data Name='ProcessGuid'>{3CBB8FBE-892B-6571-7A0A-000000001200}</Data><Data Name='ProcessId'>10304</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:58:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:58:18.596810300Z'/><EventRecordID>681</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:58:18.587</Data><Data Name='ProcessGuid'>{3CBB8FBE-892A-6571-790A-000000001200}</Data><Data Name='ProcessId'>1300</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:58:17+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:58:17.034052300Z'/><EventRecordID>680</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:58:17.024</Data><Data Name='ProcessGuid'>{3CBB8FBE-8929-6571-780A-000000001200}</Data><Data Name='ProcessId'>11204</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:58:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:58:16.282449700Z'/><EventRecordID>679</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:58:16.273</Data><Data Name='ProcessGuid'>{3CBB8FBE-8928-6571-770A-000000001200}</Data><Data Name='ProcessId'>1712</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:58:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:58:15.533164500Z'/><EventRecordID>678</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:58:15.524</Data><Data Name='ProcessGuid'>{3CBB8FBE-8927-6571-760A-000000001200}</Data><Data Name='ProcessId'>11020</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:57:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:57:20.160864700Z'/><EventRecordID>677</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:57:20.150</Data><Data Name='ProcessGuid'>{3CBB8FBE-88F0-6571-750A-000000001200}</Data><Data Name='ProcessId'>10948</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:57:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:57:19.398636000Z'/><EventRecordID>676</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:57:19.388</Data><Data Name='ProcessGuid'>{3CBB8FBE-88EF-6571-740A-000000001200}</Data><Data Name='ProcessId'>10984</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:57:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:57:18.581511200Z'/><EventRecordID>675</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:57:18.572</Data><Data Name='ProcessGuid'>{3CBB8FBE-88EE-6571-730A-000000001200}</Data><Data Name='ProcessId'>10944</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:57:17+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:57:17.050973200Z'/><EventRecordID>674</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:57:17.040</Data><Data Name='ProcessGuid'>{3CBB8FBE-88ED-6571-720A-000000001200}</Data><Data Name='ProcessId'>10592</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:57:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:57:16.284480800Z'/><EventRecordID>673</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:57:16.275</Data><Data Name='ProcessGuid'>{3CBB8FBE-88EC-6571-710A-000000001200}</Data><Data Name='ProcessId'>10672</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:57:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:57:15.517695600Z'/><EventRecordID>672</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:57:15.509</Data><Data Name='ProcessGuid'>{3CBB8FBE-88EB-6571-700A-000000001200}</Data><Data Name='ProcessId'>10640</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:56:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:56:20.148788300Z'/><EventRecordID>671</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:56:20.136</Data><Data Name='ProcessGuid'>{3CBB8FBE-88B4-6571-6C0A-000000001200}</Data><Data Name='ProcessId'>10632</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:56:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:56:19.395486200Z'/><EventRecordID>670</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:56:19.386</Data><Data Name='ProcessGuid'>{3CBB8FBE-88B3-6571-6B0A-000000001200}</Data><Data Name='ProcessId'>10960</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:56:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:56:18.567877400Z'/><EventRecordID>669</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:56:18.558</Data><Data Name='ProcessGuid'>{3CBB8FBE-88B2-6571-6A0A-000000001200}</Data><Data Name='ProcessId'>10520</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:56:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:56:16.992670900Z'/><EventRecordID>668</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:56:16.982</Data><Data Name='ProcessGuid'>{3CBB8FBE-88B0-6571-690A-000000001200}</Data><Data Name='ProcessId'>5112</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:56:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:56:16.256602600Z'/><EventRecordID>667</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:56:16.246</Data><Data Name='ProcessGuid'>{3CBB8FBE-88B0-6571-680A-000000001200}</Data><Data Name='ProcessId'>10748</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:56:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:56:15.505685800Z'/><EventRecordID>666</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:56:15.496</Data><Data Name='ProcessGuid'>{3CBB8FBE-88AF-6571-670A-000000001200}</Data><Data Name='ProcessId'>9876</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:55:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:55:20.118351400Z'/><EventRecordID>665</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:55:20.107</Data><Data Name='ProcessGuid'>{3CBB8FBE-8878-6571-660A-000000001200}</Data><Data Name='ProcessId'>11136</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:55:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:55:19.366694200Z'/><EventRecordID>664</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:55:19.356</Data><Data Name='ProcessGuid'>{3CBB8FBE-8877-6571-650A-000000001200}</Data><Data Name='ProcessId'>10876</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:55:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:55:18.553454300Z'/><EventRecordID>663</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:55:18.545</Data><Data Name='ProcessGuid'>{3CBB8FBE-8876-6571-640A-000000001200}</Data><Data Name='ProcessId'>5180</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:55:17+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:55:17.006548700Z'/><EventRecordID>662</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:55:16.997</Data><Data Name='ProcessGuid'>{3CBB8FBE-8874-6571-630A-000000001200}</Data><Data Name='ProcessId'>11216</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:55:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:55:16.257814100Z'/><EventRecordID>661</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:55:16.247</Data><Data Name='ProcessGuid'>{3CBB8FBE-8874-6571-620A-000000001200}</Data><Data Name='ProcessId'>2516</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:55:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:55:15.489840500Z'/><EventRecordID>660</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:55:15.482</Data><Data Name='ProcessGuid'>{3CBB8FBE-8873-6571-610A-000000001200}</Data><Data Name='ProcessId'>6656</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:54:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:54:20.103224300Z'/><EventRecordID>659</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:54:20.093</Data><Data Name='ProcessGuid'>{3CBB8FBE-883C-6571-600A-000000001200}</Data><Data Name='ProcessId'>2636</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:54:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:54:19.353704400Z'/><EventRecordID>658</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:54:19.344</Data><Data Name='ProcessGuid'>{3CBB8FBE-883B-6571-5F0A-000000001200}</Data><Data Name='ProcessId'>10688</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:54:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:54:18.539053800Z'/><EventRecordID>657</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:54:18.530</Data><Data Name='ProcessGuid'>{3CBB8FBE-883A-6571-5E0A-000000001200}</Data><Data Name='ProcessId'>10632</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:54:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:54:16.978451800Z'/><EventRecordID>656</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:54:16.968</Data><Data Name='ProcessGuid'>{3CBB8FBE-8838-6571-5D0A-000000001200}</Data><Data Name='ProcessId'>10108</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:54:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:54:16.228692800Z'/><EventRecordID>655</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:54:16.218</Data><Data Name='ProcessGuid'>{3CBB8FBE-8838-6571-5C0A-000000001200}</Data><Data Name='ProcessId'>8428</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:54:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:54:15.476876400Z'/><EventRecordID>654</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:54:15.468</Data><Data Name='ProcessGuid'>{3CBB8FBE-8837-6571-5B0A-000000001200}</Data><Data Name='ProcessId'>10580</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:53:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:53:20.103749600Z'/><EventRecordID>653</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:53:20.094</Data><Data Name='ProcessGuid'>{3CBB8FBE-8800-6571-5A0A-000000001200}</Data><Data Name='ProcessId'>10464</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:53:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:53:19.341242200Z'/><EventRecordID>652</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:53:19.333</Data><Data Name='ProcessGuid'>{3CBB8FBE-87FF-6571-590A-000000001200}</Data><Data Name='ProcessId'>11116</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:53:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:53:18.527804100Z'/><EventRecordID>651</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:53:18.517</Data><Data Name='ProcessGuid'>{3CBB8FBE-87FE-6571-580A-000000001200}</Data><Data Name='ProcessId'>11108</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:53:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:53:16.997476300Z'/><EventRecordID>650</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:53:16.987</Data><Data Name='ProcessGuid'>{3CBB8FBE-87FC-6571-570A-000000001200}</Data><Data Name='ProcessId'>11000</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:53:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:53:16.245547000Z'/><EventRecordID>649</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:53:16.235</Data><Data Name='ProcessGuid'>{3CBB8FBE-87FC-6571-560A-000000001200}</Data><Data Name='ProcessId'>10976</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:53:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:53:15.464500900Z'/><EventRecordID>648</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:53:15.454</Data><Data Name='ProcessGuid'>{3CBB8FBE-87FB-6571-550A-000000001200}</Data><Data Name='ProcessId'>5224</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:52:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:52:20.096051000Z'/><EventRecordID>647</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:52:20.080</Data><Data Name='ProcessGuid'>{3CBB8FBE-87C4-6571-540A-000000001200}</Data><Data Name='ProcessId'>11156</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:52:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:52:19.321964900Z'/><EventRecordID>646</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:52:19.314</Data><Data Name='ProcessGuid'>{3CBB8FBE-87C3-6571-530A-000000001200}</Data><Data Name='ProcessId'>10844</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:52:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:52:18.527376500Z'/><EventRecordID>645</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:52:18.517</Data><Data Name='ProcessGuid'>{3CBB8FBE-87C2-6571-520A-000000001200}</Data><Data Name='ProcessId'>11212</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:52:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:52:16.951094900Z'/><EventRecordID>644</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:52:16.940</Data><Data Name='ProcessGuid'>{3CBB8FBE-87C0-6571-510A-000000001200}</Data><Data Name='ProcessId'>10360</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:52:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:52:16.198763900Z'/><EventRecordID>643</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:52:16.189</Data><Data Name='ProcessGuid'>{3CBB8FBE-87C0-6571-500A-000000001200}</Data><Data Name='ProcessId'>9020</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:52:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:52:15.450331600Z'/><EventRecordID>642</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:52:15.440</Data><Data Name='ProcessGuid'>{3CBB8FBE-87BF-6571-4F0A-000000001200}</Data><Data Name='ProcessId'>11124</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:51:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:51:39.963543400Z'/><EventRecordID>641</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Ver</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:51:39.954</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\unsecapp.exe|c11d412e85f8935b\BinProductVersion</Data><Data Name='Details'>10.0.14393.0</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:51:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:51:39.963378000Z'/><EventRecordID>640</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-CompileTimeClaim</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:51:39.954</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\unsecapp.exe|c11d412e85f8935b\LinkDate</Data><Data Name='Details'>07/16/2016 02:23:07</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:51:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:51:39.962454500Z'/><EventRecordID>639</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Pub</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:51:39.954</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\unsecapp.exe|c11d412e85f8935b\Publisher</Data><Data Name='Details'>microsoft corporation</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:51:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:51:39.962026900Z'/><EventRecordID>638</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Path</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:51:39.954</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\unsecapp.exe|c11d412e85f8935b\LowerCaseLongPath</Data><Data Name='Details'>c:\windows\system32\wbem\unsecapp.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:51:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:51:20.059086500Z'/><EventRecordID>637</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:51:20.050</Data><Data Name='ProcessGuid'>{3CBB8FBE-8788-6571-4D0A-000000001200}</Data><Data Name='ProcessId'>10624</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:51:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:51:19.307879100Z'/><EventRecordID>636</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:51:19.300</Data><Data Name='ProcessGuid'>{3CBB8FBE-8787-6571-4C0A-000000001200}</Data><Data Name='ProcessId'>820</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:51:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:51:18.513142300Z'/><EventRecordID>635</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:51:18.503</Data><Data Name='ProcessGuid'>{3CBB8FBE-8786-6571-4B0A-000000001200}</Data><Data Name='ProcessId'>10460</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:51:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:51:16.950794500Z'/><EventRecordID>634</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:51:16.941</Data><Data Name='ProcessGuid'>{3CBB8FBE-8784-6571-4A0A-000000001200}</Data><Data Name='ProcessId'>6152</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:51:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:51:16.184955900Z'/><EventRecordID>633</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:51:16.174</Data><Data Name='ProcessGuid'>{3CBB8FBE-8784-6571-490A-000000001200}</Data><Data Name='ProcessId'>11180</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:51:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:51:15.439333800Z'/><EventRecordID>632</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:51:15.428</Data><Data Name='ProcessGuid'>{3CBB8FBE-8783-6571-480A-000000001200}</Data><Data Name='ProcessId'>5224</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:50:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:50:20.058667400Z'/><EventRecordID>631</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:50:20.050</Data><Data Name='ProcessGuid'>{3CBB8FBE-874C-6571-470A-000000001200}</Data><Data Name='ProcessId'>11136</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:50:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:50:19.300321300Z'/><EventRecordID>630</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:50:19.285</Data><Data Name='ProcessGuid'>{3CBB8FBE-874B-6571-460A-000000001200}</Data><Data Name='ProcessId'>11096</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:50:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:50:18.514365800Z'/><EventRecordID>629</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:50:18.503</Data><Data Name='ProcessGuid'>{3CBB8FBE-874A-6571-450A-000000001200}</Data><Data Name='ProcessId'>11080</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:50:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:50:16.952850400Z'/><EventRecordID>628</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:50:16.941</Data><Data Name='ProcessGuid'>{3CBB8FBE-8748-6571-440A-000000001200}</Data><Data Name='ProcessId'>11048</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:50:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:50:16.185312800Z'/><EventRecordID>627</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:50:16.175</Data><Data Name='ProcessGuid'>{3CBB8FBE-8748-6571-430A-000000001200}</Data><Data Name='ProcessId'>10992</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:50:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:50:15.436820900Z'/><EventRecordID>626</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:50:15.426</Data><Data Name='ProcessGuid'>{3CBB8FBE-8747-6571-420A-000000001200}</Data><Data Name='ProcessId'>10920</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:49:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:49:20.029485600Z'/><EventRecordID>625</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:49:20.019</Data><Data Name='ProcessGuid'>{3CBB8FBE-8710-6571-410A-000000001200}</Data><Data Name='ProcessId'>10720</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:49:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:49:19.281435000Z'/><EventRecordID>624</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:49:19.268</Data><Data Name='ProcessGuid'>{3CBB8FBE-870F-6571-400A-000000001200}</Data><Data Name='ProcessId'>10728</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:49:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:49:18.513653300Z'/><EventRecordID>623</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:49:18.504</Data><Data Name='ProcessGuid'>{3CBB8FBE-870E-6571-3F0A-000000001200}</Data><Data Name='ProcessId'>10456</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:49:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:49:16.956276200Z'/><EventRecordID>622</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:49:16.944</Data><Data Name='ProcessGuid'>{3CBB8FBE-870C-6571-3E0A-000000001200}</Data><Data Name='ProcessId'>10668</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:49:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:49:16.185999000Z'/><EventRecordID>621</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:49:16.176</Data><Data Name='ProcessGuid'>{3CBB8FBE-870C-6571-3D0A-000000001200}</Data><Data Name='ProcessId'>10576</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:49:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:49:15.439376400Z'/><EventRecordID>620</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:49:15.428</Data><Data Name='ProcessGuid'>{3CBB8FBE-870B-6571-3C0A-000000001200}</Data><Data Name='ProcessId'>10556</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:48:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:48:20.014256700Z'/><EventRecordID>619</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:48:20.003</Data><Data Name='ProcessGuid'>{3CBB8FBE-86D4-6571-3B0A-000000001200}</Data><Data Name='ProcessId'>5224</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:48:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:48:19.263056400Z'/><EventRecordID>618</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:48:19.253</Data><Data Name='ProcessGuid'>{3CBB8FBE-86D3-6571-3A0A-000000001200}</Data><Data Name='ProcessId'>11132</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:48:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:48:18.500904500Z'/><EventRecordID>617</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:48:18.488</Data><Data Name='ProcessGuid'>{3CBB8FBE-86D2-6571-390A-000000001200}</Data><Data Name='ProcessId'>11100</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:48:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:48:16.955612700Z'/><EventRecordID>616</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:48:16.941</Data><Data Name='ProcessGuid'>{3CBB8FBE-86D0-6571-380A-000000001200}</Data><Data Name='ProcessId'>10588</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:48:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:48:16.188994100Z'/><EventRecordID>615</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:48:16.176</Data><Data Name='ProcessGuid'>{3CBB8FBE-86D0-6571-370A-000000001200}</Data><Data Name='ProcessId'>11004</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:48:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:48:15.436384000Z'/><EventRecordID>614</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:48:15.424</Data><Data Name='ProcessGuid'>{3CBB8FBE-86CF-6571-360A-000000001200}</Data><Data Name='ProcessId'>10988</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:47:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:47:20.012812300Z'/><EventRecordID>613</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:47:20.002</Data><Data Name='ProcessGuid'>{3CBB8FBE-8698-6571-350A-000000001200}</Data><Data Name='ProcessId'>10368</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:47:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:47:19.262919900Z'/><EventRecordID>612</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:47:19.252</Data><Data Name='ProcessGuid'>{3CBB8FBE-8697-6571-340A-000000001200}</Data><Data Name='ProcessId'>10648</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:47:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:47:18.495143200Z'/><EventRecordID>611</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:47:18.485</Data><Data Name='ProcessGuid'>{3CBB8FBE-8696-6571-330A-000000001200}</Data><Data Name='ProcessId'>10612</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:47:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:47:16.949354400Z'/><EventRecordID>610</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:47:16.939</Data><Data Name='ProcessGuid'>{3CBB8FBE-8694-6571-320A-000000001200}</Data><Data Name='ProcessId'>10572</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:47:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:47:16.186937700Z'/><EventRecordID>609</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:47:16.174</Data><Data Name='ProcessGuid'>{3CBB8FBE-8694-6571-310A-000000001200}</Data><Data Name='ProcessId'>10548</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:47:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:47:15.431636000Z'/><EventRecordID>608</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:47:15.422</Data><Data Name='ProcessGuid'>{3CBB8FBE-8693-6571-300A-000000001200}</Data><Data Name='ProcessId'>10524</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:46:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:46:20.009021600Z'/><EventRecordID>607</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:46:19.999</Data><Data Name='ProcessGuid'>{3CBB8FBE-865B-6571-2C0A-000000001200}</Data><Data Name='ProcessId'>11012</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:46:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:46:19.243056800Z'/><EventRecordID>606</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:46:19.233</Data><Data Name='ProcessGuid'>{3CBB8FBE-865B-6571-2B0A-000000001200}</Data><Data Name='ProcessId'>10980</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:46:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:46:18.478964500Z'/><EventRecordID>605</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:46:18.469</Data><Data Name='ProcessGuid'>{3CBB8FBE-865A-6571-2A0A-000000001200}</Data><Data Name='ProcessId'>10952</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:46:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:46:16.932967800Z'/><EventRecordID>604</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:46:16.920</Data><Data Name='ProcessGuid'>{3CBB8FBE-8658-6571-290A-000000001200}</Data><Data Name='ProcessId'>10908</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:46:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:46:16.182052300Z'/><EventRecordID>603</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:46:16.170</Data><Data Name='ProcessGuid'>{3CBB8FBE-8658-6571-280A-000000001200}</Data><Data Name='ProcessId'>10876</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:46:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:46:15.430846700Z'/><EventRecordID>602</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:46:15.420</Data><Data Name='ProcessGuid'>{3CBB8FBE-8657-6571-270A-000000001200}</Data><Data Name='ProcessId'>10844</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:46:07+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:46:07.343596000Z'/><EventRecordID>601</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:46:06.396</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>ForestDnsZones.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:46:07+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:46:07.343582700Z'/><EventRecordID>600</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:46:06.380</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>ForestDnsZones.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:46:07+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:46:07.343568900Z'/><EventRecordID>599</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:46:06.377</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>DomainDnsZones.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:46:07+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:46:07.343555600Z'/><EventRecordID>598</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:46:06.364</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>DomainDnsZones.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:46:07+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:46:07.343541800Z'/><EventRecordID>597</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:46:06.362</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>gc._msdcs.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:46:07+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:46:07.343524900Z'/><EventRecordID>596</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:46:06.349</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>gc._msdcs.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:45:59+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:45:59.934144300Z'/><EventRecordID>595</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:45:57.966</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1500-000000001200}</Data><Data Name='ProcessId'>1096</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\NETWORK SERVICE</Data></EventData></Event>
2023-12-07T09:45:58+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:45:58.933818000Z'/><EventRecordID>594</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:45:57.947</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1500-000000001200}</Data><Data Name='ProcessId'>1096</Data><Data Name='QueryName'>essos.local</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\NETWORK SERVICE</Data></EventData></Event>

Time	Event
2023-12-07T09:45:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:45:20.021305200Z'/><EventRecordID>593</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:45:20.010</Data><Data Name='ProcessGuid'>{3CBB8FBE-8620-6571-250A-000000001200}</Data><Data Name='ProcessId'>10488</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:45:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:45:19.256551500Z'/><EventRecordID>592</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:45:19.245</Data><Data Name='ProcessGuid'>{3CBB8FBE-861F-6571-240A-000000001200}</Data><Data Name='ProcessId'>10456</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:45:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:45:18.488862700Z'/><EventRecordID>591</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:45:18.478</Data><Data Name='ProcessGuid'>{3CBB8FBE-861E-6571-230A-000000001200}</Data><Data Name='ProcessId'>10428</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:45:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:45:16.943388700Z'/><EventRecordID>590</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:45:16.933</Data><Data Name='ProcessGuid'>{3CBB8FBE-861C-6571-220A-000000001200}</Data><Data Name='ProcessId'>10400</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:45:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:45:16.192464800Z'/><EventRecordID>589</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:45:16.182</Data><Data Name='ProcessGuid'>{3CBB8FBE-861C-6571-210A-000000001200}</Data><Data Name='ProcessId'>10368</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:45:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:45:15.426865700Z'/><EventRecordID>588</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:45:15.416</Data><Data Name='ProcessGuid'>{3CBB8FBE-861B-6571-200A-000000001200}</Data><Data Name='ProcessId'>10336</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:45:06+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:45:06.914556700Z'/><EventRecordID>587</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:45:05.904</Data><Data Name='ProcessGuid'>{3CBB8FBE-8611-6571-1F0A-000000001200}</Data><Data Name='ProcessId'>6788</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\taskhostw.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:44:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:44:20.017936800Z'/><EventRecordID>586</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:44:20.007</Data><Data Name='ProcessGuid'>{3CBB8FBE-85E4-6571-1E0A-000000001200}</Data><Data Name='ProcessId'>5404</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:44:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:44:19.234324000Z'/><EventRecordID>585</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:44:19.224</Data><Data Name='ProcessGuid'>{3CBB8FBE-85E3-6571-1D0A-000000001200}</Data><Data Name='ProcessId'>6072</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:44:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:44:18.467929400Z'/><EventRecordID>584</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:44:18.457</Data><Data Name='ProcessGuid'>{3CBB8FBE-85E2-6571-1C0A-000000001200}</Data><Data Name='ProcessId'>8116</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:44:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:44:16.954006000Z'/><EventRecordID>583</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:44:16.943</Data><Data Name='ProcessGuid'>{3CBB8FBE-85E0-6571-1B0A-000000001200}</Data><Data Name='ProcessId'>9356</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:44:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:44:16.192780300Z'/><EventRecordID>582</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:44:16.177</Data><Data Name='ProcessGuid'>{3CBB8FBE-85E0-6571-1A0A-000000001200}</Data><Data Name='ProcessId'>8152</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:44:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:44:15.420773400Z'/><EventRecordID>581</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:44:15.411</Data><Data Name='ProcessGuid'>{3CBB8FBE-85DF-6571-190A-000000001200}</Data><Data Name='ProcessId'>8744</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:44:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:44:15.128511500Z'/><EventRecordID>580</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:44:13.362</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1700-000000001200}</Data><Data Name='ProcessId'>1340</Data><Data Name='QueryName'>isatap</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>-</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:44:12+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:44:12.081171900Z'/><EventRecordID>579</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:44:11.066</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1700-000000001200}</Data><Data Name='ProcessId'>1340</Data><Data Name='QueryName'>isatap.iutbeziers.fr</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>-</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:43:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:43:19.994397500Z'/><EventRecordID>578</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:43:19.982</Data><Data Name='ProcessGuid'>{3CBB8FBE-85A7-6571-180A-000000001200}</Data><Data Name='ProcessId'>8952</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:43:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:43:19.227949300Z'/><EventRecordID>577</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:43:19.216</Data><Data Name='ProcessGuid'>{3CBB8FBE-85A7-6571-170A-000000001200}</Data><Data Name='ProcessId'>5676</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:43:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:43:18.459243100Z'/><EventRecordID>576</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:43:18.450</Data><Data Name='ProcessGuid'>{3CBB8FBE-85A6-6571-160A-000000001200}</Data><Data Name='ProcessId'>8692</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:43:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:43:16.944724600Z'/><EventRecordID>575</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:43:16.934</Data><Data Name='ProcessGuid'>{3CBB8FBE-85A4-6571-150A-000000001200}</Data><Data Name='ProcessId'>9788</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:43:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:43:16.194597200Z'/><EventRecordID>574</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:43:16.184</Data><Data Name='ProcessGuid'>{3CBB8FBE-85A4-6571-140A-000000001200}</Data><Data Name='ProcessId'>3600</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:43:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:43:15.429360800Z'/><EventRecordID>573</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:43:15.418</Data><Data Name='ProcessGuid'>{3CBB8FBE-85A3-6571-130A-000000001200}</Data><Data Name='ProcessId'>3860</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:42:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:42:19.985773500Z'/><EventRecordID>572</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:42:19.974</Data><Data Name='ProcessGuid'>{3CBB8FBE-856B-6571-120A-000000001200}</Data><Data Name='ProcessId'>4944</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:42:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:42:19.215187500Z'/><EventRecordID>571</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:42:19.205</Data><Data Name='ProcessGuid'>{3CBB8FBE-856B-6571-110A-000000001200}</Data><Data Name='ProcessId'>9032</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:42:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:42:18.453953400Z'/><EventRecordID>570</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:42:18.439</Data><Data Name='ProcessGuid'>{3CBB8FBE-856A-6571-100A-000000001200}</Data><Data Name='ProcessId'>1584</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:42:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:42:16.933859300Z'/><EventRecordID>569</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:42:16.923</Data><Data Name='ProcessGuid'>{3CBB8FBE-8568-6571-0F0A-000000001200}</Data><Data Name='ProcessId'>6952</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:42:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:42:16.186610100Z'/><EventRecordID>568</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:42:16.174</Data><Data Name='ProcessGuid'>{3CBB8FBE-8568-6571-0E0A-000000001200}</Data><Data Name='ProcessId'>3660</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:42:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:42:15.419991100Z'/><EventRecordID>567</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:42:15.407</Data><Data Name='ProcessGuid'>{3CBB8FBE-8567-6571-0D0A-000000001200}</Data><Data Name='ProcessId'>7764</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:19.991713100Z'/><EventRecordID>566</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:19.980</Data><Data Name='ProcessGuid'>{3CBB8FBE-852F-6571-0C0A-000000001200}</Data><Data Name='ProcessId'>7420</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:19.208942100Z'/><EventRecordID>565</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:19.199</Data><Data Name='ProcessGuid'>{3CBB8FBE-852F-6571-0B0A-000000001200}</Data><Data Name='ProcessId'>8804</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:41:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:18.445482300Z'/><EventRecordID>564</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:18.434</Data><Data Name='ProcessGuid'>{3CBB8FBE-852E-6571-0A0A-000000001200}</Data><Data Name='ProcessId'>6356</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:16.930080600Z'/><EventRecordID>563</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:16.919</Data><Data Name='ProcessGuid'>{3CBB8FBE-852C-6571-090A-000000001200}</Data><Data Name='ProcessId'>7716</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:16.180202100Z'/><EventRecordID>562</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:16.169</Data><Data Name='ProcessGuid'>{3CBB8FBE-852C-6571-080A-000000001200}</Data><Data Name='ProcessId'>6120</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:41:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:15.414582300Z'/><EventRecordID>561</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:15.403</Data><Data Name='ProcessGuid'>{3CBB8FBE-852B-6571-070A-000000001200}</Data><Data Name='ProcessId'>3904</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:07+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:07.153579500Z'/><EventRecordID>560</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:06.158</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:07+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:07.153566100Z'/><EventRecordID>559</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:06.157</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>essos.local.</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:05+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:05.418148000Z'/><EventRecordID>558</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.958</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402812000Z'/><EventRecordID>557</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.945</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402796000Z'/><EventRecordID>556</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.941</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.ForestDnsZones.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402782200Z'/><EventRecordID>555</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.928</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.ForestDnsZones.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402768400Z'/><EventRecordID>554</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.926</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402752800Z'/><EventRecordID>553</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.925</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402737300Z'/><EventRecordID>552</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.923</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.DomainDnsZones.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402723100Z'/><EventRecordID>551</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.922</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.DomainDnsZones.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402709300Z'/><EventRecordID>550</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.920</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_kpasswd._udp.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402696400Z'/><EventRecordID>549</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.919</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_kpasswd._udp.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402684000Z'/><EventRecordID>548</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.917</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_kpasswd._tcp.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402671500Z'/><EventRecordID>547</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.916</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_kpasswd._tcp.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402658200Z'/><EventRecordID>546</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.914</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_kerberos._udp.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402645300Z'/><EventRecordID>545</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.913</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_kerberos._udp.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402632000Z'/><EventRecordID>544</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.911</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_gc._tcp.Default-First-Site-Name._sites.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402611100Z'/><EventRecordID>543</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.910</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_gc._tcp.Default-First-Site-Name._sites.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402596000Z'/><EventRecordID>542</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.908</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_gc._tcp.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402583500Z'/><EventRecordID>541</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.906</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_gc._tcp.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402570600Z'/><EventRecordID>540</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.904</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_kerberos._tcp.Default-First-Site-Name._sites.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402556000Z'/><EventRecordID>539</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.891</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_kerberos._tcp.Default-First-Site-Name._sites.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402540800Z'/><EventRecordID>538</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.889</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_kerberos._tcp.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402527500Z'/><EventRecordID>537</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.888</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_kerberos._tcp.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402514200Z'/><EventRecordID>536</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.886</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_kerberos._tcp.Default-First-Site-Name._sites.dc._msdcs.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402499100Z'/><EventRecordID>535</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.885</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_kerberos._tcp.Default-First-Site-Name._sites.dc._msdcs.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402484000Z'/><EventRecordID>534</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.883</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_kerberos._tcp.dc._msdcs.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402470200Z'/><EventRecordID>533</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.882</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_kerberos._tcp.dc._msdcs.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402456400Z'/><EventRecordID>532</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.879</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.Default-First-Site-Name._sites.gc._msdcs.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402441300Z'/><EventRecordID>531</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.877</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.Default-First-Site-Name._sites.gc._msdcs.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402425700Z'/><EventRecordID>530</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.875</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.gc._msdcs.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402412400Z'/><EventRecordID>529</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.861</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.gc._msdcs.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402398600Z'/><EventRecordID>528</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.859</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402383500Z'/><EventRecordID>527</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.858</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402368400Z'/><EventRecordID>526</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.855</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.dc._msdcs.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402355100Z'/><EventRecordID>525</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.854</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.dc._msdcs.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402337700Z'/><EventRecordID>524</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.852</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_msdcs.essos.local.</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 2 meereen.essos.local;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402320000Z'/><EventRecordID>523</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.851</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>09a2b3a4-fcd7-4408-b13e-7e45f2eb8e8b._msdcs.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402305300Z'/><EventRecordID>522</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.850</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_msdcs.essos.local.</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402292400Z'/><EventRecordID>521</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.849</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>09a2b3a4-fcd7-4408-b13e-7e45f2eb8e8b._msdcs.essos.local.</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 5 meereen.essos.local;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402277700Z'/><EventRecordID>520</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.846</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.343d90dc-2051-44ae-96f8-dae214c3fa48.domains._msdcs.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402261300Z'/><EventRecordID>519</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.845</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.343d90dc-2051-44ae-96f8-dae214c3fa48.domains._msdcs.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402244800Z'/><EventRecordID>518</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.842</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.pdc._msdcs.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402230600Z'/><EventRecordID>517</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.826</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.pdc._msdcs.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402216000Z'/><EventRecordID>516</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.823</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.Default-First-Site-Name._sites.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402192000Z'/><EventRecordID>515</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.822</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.Default-First-Site-Name._sites.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402172800Z'/><EventRecordID>514</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.820</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.essos.local.</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>type: 6 ;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402159500Z'/><EventRecordID>513</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.819</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>_ldap._tcp.essos.local.</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>type: 6 ;192.168.56.12;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:41:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:41:04.402130600Z'/><EventRecordID>512</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:41:03.809</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>MEEREEN</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:40:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:40:19.964000300Z'/><EventRecordID>511</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:40:19.953</Data><Data Name='ProcessGuid'>{3CBB8FBE-84F3-6571-060A-000000001200}</Data><Data Name='ProcessId'>7184</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:40:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:40:19.197925200Z'/><EventRecordID>510</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:40:19.187</Data><Data Name='ProcessGuid'>{3CBB8FBE-84F3-6571-050A-000000001200}</Data><Data Name='ProcessId'>5404</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:40:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:40:18.431211600Z'/><EventRecordID>509</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:40:18.422</Data><Data Name='ProcessGuid'>{3CBB8FBE-84F2-6571-040A-000000001200}</Data><Data Name='ProcessId'>10216</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:40:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:40:16.917679400Z'/><EventRecordID>508</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:40:16.907</Data><Data Name='ProcessGuid'>{3CBB8FBE-84F0-6571-030A-000000001200}</Data><Data Name='ProcessId'>6520</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:40:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:40:16.168238100Z'/><EventRecordID>507</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:40:16.157</Data><Data Name='ProcessGuid'>{3CBB8FBE-84F0-6571-020A-000000001200}</Data><Data Name='ProcessId'>5988</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:40:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:40:15.402211100Z'/><EventRecordID>506</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:40:15.391</Data><Data Name='ProcessGuid'>{3CBB8FBE-84EF-6571-010A-000000001200}</Data><Data Name='ProcessId'>7756</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:21+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:21.831553100Z'/><EventRecordID>505</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:20.846</Data><Data Name='ProcessGuid'>{3CBB8FBE-84B8-6571-FF09-000000001200}</Data><Data Name='ProcessId'>4860</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:21+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:21.483489300Z'/><EventRecordID>504</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:21.472</Data><Data Name='ProcessGuid'>{3CBB8FBE-84B9-6571-000A-000000001200}</Data><Data Name='ProcessId'>2652</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-winprintmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Windows Print Monitor </Data><Data Name='Product'>splunk Application </Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-winprintmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-winprintmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=FDEB6BA573575665D847C8C88DFA6B28,SHA256=00FC8040D205B3290D204EB5E6AEAF5E21CF6F5EDB081555CDF81AD61F306218,IMPHASH=355E487ADBCE53AA00CC9620C5813D5A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:20.718463200Z'/><EventRecordID>503</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:20.707</Data><Data Name='ProcessGuid'>{3CBB8FBE-84B8-6571-FF09-000000001200}</Data><Data Name='ProcessId'>4860</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Monitor windows event logs</Data><Data Name='Product'>splunk Application </Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-winevtlog.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AE95292862972429C2FBD9541C739C2B,SHA256=C1899D942B83A761EADA6303334A9E6946A7206A59E678F0039D3AB527785522,IMPHASH=EDE9B13E7663B8E763DD4604CD8C3BF7</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:19.953088600Z'/><EventRecordID>502</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:19.942</Data><Data Name='ProcessGuid'>{3CBB8FBE-84B7-6571-FE09-000000001200}</Data><Data Name='ProcessId'>8980</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:19.186410200Z'/><EventRecordID>501</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:19.177</Data><Data Name='ProcessGuid'>{3CBB8FBE-84B7-6571-FD09-000000001200}</Data><Data Name='ProcessId'>5960</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:18+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:18.420813800Z'/><EventRecordID>500</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:18.411</Data><Data Name='ProcessGuid'>{3CBB8FBE-84B6-6571-FC09-000000001200}</Data><Data Name='ProcessId'>5212</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:17+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:17.673030300Z'/><EventRecordID>499</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:17.661</Data><Data Name='ProcessGuid'>{3CBB8FBE-84B5-6571-FB09-000000001200}</Data><Data Name='ProcessId'>4940</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-perfmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Performance monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-perfmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-perfmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=37F610EA3267B4C636A52CC17C72F5E9,SHA256=154252976F3CDC663C1999E5BF6958E4A9717874E2117061A0E40F2F1D97BE27,IMPHASH=35AE00EA6705AD0DB2C706FD3FAF93B6</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:16.907373100Z'/><EventRecordID>498</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:16.895</Data><Data Name='ProcessGuid'>{3CBB8FBE-84B4-6571-FA09-000000001200}</Data><Data Name='ProcessId'>9752</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:16.142014600Z'/><EventRecordID>497</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:16.129</Data><Data Name='ProcessGuid'>{3CBB8FBE-84B4-6571-F909-000000001200}</Data><Data Name='ProcessId'>5836</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:15.391379100Z'/><EventRecordID>496</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:15.380</Data><Data Name='ProcessGuid'>{3CBB8FBE-84B3-6571-F809-000000001200}</Data><Data Name='ProcessId'>5748</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:14+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:14.616099600Z'/><EventRecordID>495</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:14.600</Data><Data Name='ProcessGuid'>{3CBB8FBE-84B2-6571-F709-000000001200}</Data><Data Name='ProcessId'>10076</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-wmi.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Remote Performance monitor using WMI</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-wmi.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-wmi.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=7A440F2DF244985160C5B54CDBBA547D,SHA256=7E1DBA295076C76618106FD18E882B190BF0542AD2981200D01074B021BF76CF,IMPHASH=7C7770CDB275E49574E79FDF395C7C60</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:12+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:12.608932100Z'/><EventRecordID>494</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:12.589</Data><Data Name='ProcessGuid'>{3CBB8FBE-84B0-6571-F609-000000001200}</Data><Data Name='ProcessId'>3860</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\powershell2.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:12+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:12.460170700Z'/><EventRecordID>493</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:12.448</Data><Data Name='ProcessGuid'>{3CBB8FBE-84B0-6571-F509-000000001200}</Data><Data Name='ProcessId'>8468</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\powershell.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:12+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:12.329825300Z'/><EventRecordID>492</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:12.319</Data><Data Name='ProcessGuid'>{3CBB8FBE-84B0-6571-F409-000000001200}</Data><Data Name='ProcessId'>1608</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\perfmon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:12+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:12.210899400Z'/><EventRecordID>491</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:12.199</Data><Data Name='ProcessGuid'>{3CBB8FBE-84B0-6571-F309-000000001200}</Data><Data Name='ProcessId'>2328</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\admon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:12+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:12.076702600Z'/><EventRecordID>490</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:12.062</Data><Data Name='ProcessGuid'>{3CBB8FBE-84B0-6571-F209-000000001200}</Data><Data Name='ProcessId'>948</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinRegMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:11+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:11.945242000Z'/><EventRecordID>489</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:11.933</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AF-6571-F109-000000001200}</Data><Data Name='ProcessId'>2208</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinPrintMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:11+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:11.821304600Z'/><EventRecordID>488</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:11.808</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AF-6571-F009-000000001200}</Data><Data Name='ProcessId'>5676</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinNetMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:11+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:11.680678800Z'/><EventRecordID>487</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:11.668</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AF-6571-EF09-000000001200}</Data><Data Name='ProcessId'>1348</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinHostMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:11+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:11.553148100Z'/><EventRecordID>486</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:11.542</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AF-6571-EE09-000000001200}</Data><Data Name='ProcessId'>1744</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinEventLog.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:11+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:11.420548000Z'/><EventRecordID>485</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:11.410</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AF-6571-ED09-000000001200}</Data><Data Name='ProcessId'>676</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\MonitorNoHandle.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:10+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:10.734933400Z'/><EventRecordID>484</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:10.730</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AE-6571-EC09-000000001200}</Data><Data Name='ProcessId'>6496</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal check-xml-files --answer-yes --no-prompt </Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AE-6571-EB09-000000001200}</Data><Data Name='ParentProcessId'>6892</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal check-xml-files --answer-yes --no-prompt 2>&1</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:10+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:10.725309400Z'/><EventRecordID>483</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:10.712</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AE-6571-EB09-000000001200}</Data><Data Name='ProcessId'>6892</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal check-xml-files --answer-yes --no-prompt 2>&1</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:10+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:10.407095900Z'/><EventRecordID>482</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:10.400</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AE-6571-EA09-000000001200}</Data><Data Name='ProcessId'>9708</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AE-6571-E909-000000001200}</Data><Data Name='ParentProcessId'>6576</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:10+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:10.394841300Z'/><EventRecordID>481</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:10.390</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AE-6571-E909-000000001200}</Data><Data Name='ProcessId'>6576</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AE-6571-E809-000000001200}</Data><Data Name='ParentProcessId'>9160</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:10+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:10.387035600Z'/><EventRecordID>480</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:10.382</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AE-6571-E809-000000001200}</Data><Data Name='ProcessId'>9160</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AB-6571-DB09-000000001200}</Data><Data Name='ParentProcessId'>8692</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:10+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:10.116036700Z'/><EventRecordID>479</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:10.109</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AE-6571-E709-000000001200}</Data><Data Name='ProcessId'>4008</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list replication_port --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AE-6571-E609-000000001200}</Data><Data Name='ParentProcessId'>5900</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list replication_port --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:10+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:10.102486500Z'/><EventRecordID>478</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:10.098</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AE-6571-E609-000000001200}</Data><Data Name='ProcessId'>5900</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list replication_port --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AE-6571-E509-000000001200}</Data><Data Name='ParentProcessId'>6200</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list replication_port --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:10+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:10.094712700Z'/><EventRecordID>477</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:10.090</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AE-6571-E509-000000001200}</Data><Data Name='ProcessId'>6200</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list replication_port --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AB-6571-DB09-000000001200}</Data><Data Name='ParentProcessId'>8692</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:09+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:09.773479300Z'/><EventRecordID>476</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:09.766</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AD-6571-E409-000000001200}</Data><Data Name='ProcessId'>9788</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd" check-transforms-keys</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AB-6571-DB09-000000001200}</Data><Data Name='ParentProcessId'>8692</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:09+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:09.207050600Z'/><EventRecordID>475</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:09.199</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AD-6571-E309-000000001200}</Data><Data Name='ProcessId'>6840</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool validate-regex --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AD-6571-E209-000000001200}</Data><Data Name='ParentProcessId'>9164</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-regex --log-warnings</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:09+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:09.194871000Z'/><EventRecordID>474</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:09.189</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AD-6571-E209-000000001200}</Data><Data Name='ProcessId'>9164</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>" C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-regex --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AB-6571-DB09-000000001200}</Data><Data Name='ParentProcessId'>8692</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:08+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:08.710778800Z'/><EventRecordID>473</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:08.702</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AC-6571-E109-000000001200}</Data><Data Name='ProcessId'>6640</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool validate-strptime --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AC-6571-E009-000000001200}</Data><Data Name='ParentProcessId'>8384</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-strptime --log-warnings</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:08+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:08.697016200Z'/><EventRecordID>472</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:08.692</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AC-6571-E009-000000001200}</Data><Data Name='ProcessId'>8384</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>" C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-strptime --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AB-6571-DB09-000000001200}</Data><Data Name='ParentProcessId'>8692</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:08+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:08.092826500Z'/><EventRecordID>471</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:08.086</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AC-6571-DF09-000000001200}</Data><Data Name='ProcessId'>1192</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool check --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AC-6571-DE09-000000001200}</Data><Data Name='ParentProcessId'>6768</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" check --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:08+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:08.079851900Z'/><EventRecordID>470</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:08.074</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AC-6571-DE09-000000001200}</Data><Data Name='ProcessId'>6768</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" check --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AB-6571-DB09-000000001200}</Data><Data Name='ParentProcessId'>8692</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:07+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:07.762172600Z'/><EventRecordID>469</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:07.755</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AB-6571-DD09-000000001200}</Data><Data Name='ProcessId'>6524</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" check-license</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AB-6571-DB09-000000001200}</Data><Data Name='ParentProcessId'>8692</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:07+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:07.465461800Z'/><EventRecordID>468</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:07.459</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AB-6571-DC09-000000001200}</Data><Data Name='ProcessId'>3600</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" generate-ssl</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AB-6571-DB09-000000001200}</Data><Data Name='ParentProcessId'>8692</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:07+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:07.450615200Z'/><EventRecordID>467</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:07.446</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AB-6571-DB09-000000001200}</Data><Data Name='ProcessId'>8692</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AB-6571-DA09-000000001200}</Data><Data Name='ParentProcessId'>5792</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt 2>&1</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:07+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:07.438745400Z'/><EventRecordID>466</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:07.430</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AB-6571-DA09-000000001200}</Data><Data Name='ProcessId'>5792</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt 2>&1</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:06+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:06.897234900Z'/><EventRecordID>465</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:06.890</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AA-6571-D909-000000001200}</Data><Data Name='ProcessId'>5524</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list sslConfig --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AA-6571-D809-000000001200}</Data><Data Name='ParentProcessId'>9984</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list sslConfig --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:06+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:06.883689500Z'/><EventRecordID>464</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:06.879</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AA-6571-D809-000000001200}</Data><Data Name='ProcessId'>9984</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list sslConfig --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AA-6571-D709-000000001200}</Data><Data Name='ParentProcessId'>9872</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list sslConfig --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:06+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:06.874845500Z'/><EventRecordID>463</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:06.869</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AA-6571-D709-000000001200}</Data><Data Name='ProcessId'>9872</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list sslConfig --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-CA09-000000001200}</Data><Data Name='ParentProcessId'>6536</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:06+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:06.606657000Z'/><EventRecordID>462</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:06.598</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AA-6571-D609-000000001200}</Data><Data Name='ProcessId'>9848</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list watchdog --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AA-6571-D509-000000001200}</Data><Data Name='ParentProcessId'>9352</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list watchdog --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:06+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:06.594242700Z'/><EventRecordID>461</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:06.590</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AA-6571-D509-000000001200}</Data><Data Name='ProcessId'>9352</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list watchdog --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AA-6571-D409-000000001200}</Data><Data Name='ParentProcessId'>9784</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list watchdog --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:06+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:06.586397800Z'/><EventRecordID>460</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:06.580</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AA-6571-D409-000000001200}</Data><Data Name='ProcessId'>9784</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list watchdog --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-CA09-000000001200}</Data><Data Name='ParentProcessId'>6536</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:06+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:06.317025300Z'/><EventRecordID>459</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:06.310</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AA-6571-D309-000000001200}</Data><Data Name='ProcessId'>7296</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list kvstore --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AA-6571-D209-000000001200}</Data><Data Name='ParentProcessId'>8304</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list kvstore --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:06+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:06.303621300Z'/><EventRecordID>458</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:06.297</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AA-6571-D209-000000001200}</Data><Data Name='ProcessId'>8304</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list kvstore --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AA-6571-D109-000000001200}</Data><Data Name='ParentProcessId'>9704</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list kvstore --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:06+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:06.294988400Z'/><EventRecordID>457</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:06.290</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AA-6571-D109-000000001200}</Data><Data Name='ProcessId'>9704</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list kvstore --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-CA09-000000001200}</Data><Data Name='ParentProcessId'>6536</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:06+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:06.017476700Z'/><EventRecordID>456</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:06.010</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AA-6571-D009-000000001200}</Data><Data Name='ProcessId'>10060</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84AA-6571-CF09-000000001200}</Data><Data Name='ParentProcessId'>2756</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:06+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:06.005733200Z'/><EventRecordID>455</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:06.001</Data><Data Name='ProcessGuid'>{3CBB8FBE-84AA-6571-CF09-000000001200}</Data><Data Name='ProcessId'>2756</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-CE09-000000001200}</Data><Data Name='ParentProcessId'>3876</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:05+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:05.997595000Z'/><EventRecordID>454</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:05.993</Data><Data Name='ProcessGuid'>{3CBB8FBE-84A9-6571-CE09-000000001200}</Data><Data Name='ProcessId'>3876</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-CA09-000000001200}</Data><Data Name='ParentProcessId'>6536</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:05+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:05.728080100Z'/><EventRecordID>453</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:05.721</Data><Data Name='ProcessGuid'>{3CBB8FBE-84A9-6571-CD09-000000001200}</Data><Data Name='ProcessId'>3256</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool web list settings --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-CC09-000000001200}</Data><Data Name='ParentProcessId'>10220</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool web list settings --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:05+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:05.715896500Z'/><EventRecordID>452</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:05.711</Data><Data Name='ProcessGuid'>{3CBB8FBE-84A9-6571-CC09-000000001200}</Data><Data Name='ProcessId'>10220</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool web list settings --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-CB09-000000001200}</Data><Data Name='ParentProcessId'>6360</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool web list settings --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:05+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:05.707217500Z'/><EventRecordID>451</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:05.702</Data><Data Name='ProcessGuid'>{3CBB8FBE-84A9-6571-CB09-000000001200}</Data><Data Name='ProcessId'>6360</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool web list settings --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-CA09-000000001200}</Data><Data Name='ParentProcessId'>6536</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:05+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:05.693915300Z'/><EventRecordID>450</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:05.690</Data><Data Name='ProcessGuid'>{3CBB8FBE-84A9-6571-CA09-000000001200}</Data><Data Name='ProcessId'>6536</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C909-000000001200}</Data><Data Name='ParentProcessId'>8992</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:05+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:05.687051200Z'/><EventRecordID>449</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:05.679</Data><Data Name='ProcessGuid'>{3CBB8FBE-84A9-6571-C909-000000001200}</Data><Data Name='ProcessId'>8992</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:05+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:05.647711200Z'/><EventRecordID>448</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:05.643</Data><Data Name='ProcessGuid'>{3CBB8FBE-84A9-6571-C709-000000001200}</Data><Data Name='ProcessId'>5600</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _RAW_envvars</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C509-000000001200}</Data><Data Name='ParentProcessId'>1884</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _RAW_envvars</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:39:05+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:05.623456600Z'/><EventRecordID>447</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:05.616</Data><Data Name='ProcessGuid'>{3CBB8FBE-84A9-6571-C509-000000001200}</Data><Data Name='ProcessId'>1884</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _RAW_envvars</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ParentProcessId'>5668</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:39:05+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:39:05.532449800Z'/><EventRecordID>446</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:39:05.522</Data><Data Name='ProcessGuid'>{3CBB8FBE-84A9-6571-C409-000000001200}</Data><Data Name='ProcessId'>5668</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0205-656E-0A00-000000001200}</Data><Data Name='ParentProcessId'>612</Data><Data Name='ParentImage'>C:\Windows\System32\services.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\services.exe</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:38:49+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:38:49.803346402Z'/><EventRecordID>445</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:38:48.355</Data><Data Name='ProcessGuid'>{3CBB8FBE-02ED-656E-7900-000000001200}</Data><Data Name='ProcessId'>5288</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\system32\mmc.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:38:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:38:43.766119200Z'/><EventRecordID>444</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:38:43.756</Data><Data Name='ProcessGuid'>{3CBB8FBE-8493-6571-C309-000000001200}</Data><Data Name='ProcessId'>5400</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:38:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:38:43.001248300Z'/><EventRecordID>443</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:38:42.992</Data><Data Name='ProcessGuid'>{3CBB8FBE-8492-6571-C209-000000001200}</Data><Data Name='ProcessId'>10132</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:38:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:38:42.236504800Z'/><EventRecordID>442</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:38:42.226</Data><Data Name='ProcessGuid'>{3CBB8FBE-8492-6571-C109-000000001200}</Data><Data Name='ProcessId'>6808</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:38:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:38:40.789083300Z'/><EventRecordID>441</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:38:40.773</Data><Data Name='ProcessGuid'>{3CBB8FBE-8490-6571-C009-000000001200}</Data><Data Name='ProcessId'>944</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:38:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:38:40.017342000Z'/><EventRecordID>440</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:38:40.007</Data><Data Name='ProcessGuid'>{3CBB8FBE-8490-6571-BE09-000000001200}</Data><Data Name='ProcessId'>7352</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:38:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:38:39.491378700Z'/><EventRecordID>439</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:38:39.480</Data><Data Name='ProcessGuid'>{3CBB8FBE-848F-6571-BD09-000000001200}</Data><Data Name='ProcessId'>7868</Data><Data Name='Image'>C:\Windows\System32\vds.exe</Data><Data Name='FileVersion'>10.0.14393.1198 (rs1_release_sec.170427-1353)</Data><Data Name='Description'>Virtual Disk Service</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>vds.exe</Data><Data Name='CommandLine'>C:\Windows\System32\vds.exe</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=70D165B3EA8BC576828DC2B964C8D116,SHA256=92C9381BDECB5C991F848A02AF2F4189CE0119961FB37E57A37594A80704DDC5,IMPHASH=3F541E0A1D775ACA4A7D5FBDFF8433C5</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0205-656E-0A00-000000001200}</Data><Data Name='ParentProcessId'>612</Data><Data Name='ParentImage'>C:\Windows\System32\services.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\services.exe</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:38:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:38:39.351967900Z'/><EventRecordID>438</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:38:39.332</Data><Data Name='ProcessGuid'>{3CBB8FBE-848F-6571-BC09-000000001200}</Data><Data Name='ProcessId'>6140</Data><Data Name='Image'>C:\Windows\System32\vdsldr.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Virtual Disk Service Loader</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>vdsldr.exe</Data><Data Name='CommandLine'>C:\Windows\System32\vdsldr.exe -Embedding</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=E5C3B321907C73E782280BE427599F14,SHA256=43F0AF018DC498619222CF16E1C9BDE2F7710732686DC361E4D692B7EFB4DDF9,IMPHASH=D6207B24445355CEA1AC6C8E9A2BA2B9</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0205-656E-0C00-000000001200}</Data><Data Name='ParentProcessId'>788</Data><Data Name='ParentImage'>C:\Windows\System32\svchost.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\svchost.exe -k DcomLaunch</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:38:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:38:39.263441700Z'/><EventRecordID>437</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:38:39.054</Data><Data Name='ProcessGuid'>{3CBB8FBE-848F-6571-BB09-000000001200}</Data><Data Name='ProcessId'>10056</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:38:36+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:38:36.962876700Z'/><EventRecordID>436</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:38:36.947</Data><Data Name='ProcessGuid'>{3CBB8FBE-848C-6571-B909-000000001200}</Data><Data Name='ProcessId'>8968</Data><Data Name='Image'>C:\Windows\System32\VSSVC.exe</Data><Data Name='FileVersion'>10.0.14393.1198 (rs1_release_sec.170427-1353)</Data><Data Name='Description'>Microsoft® Volume Shadow Copy Service</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>VSSVC.EXE</Data><Data Name='CommandLine'>C:\Windows\system32\vssvc.exe</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=DDA66AEF89DAC320A85AECCB4369D2E7,SHA256=0F267FC985E0CA3624FC5F4DDA25623649BAD544772179261576F793A0485523,IMPHASH=23F8C470949D103A704869EF2FEB7087</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0205-656E-0A00-000000001200}</Data><Data Name='ParentProcessId'>612</Data><Data Name='ParentImage'>C:\Windows\System32\services.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\services.exe</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:38:36+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:38:36.041187400Z'/><EventRecordID>435</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:38:34.069</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2A00-000000001200}</Data><Data Name='ProcessId'>2724</Data><Data Name='QueryName'>artifacts.security.elastic.co</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 5 infra-cdn.elastic.co;::ffff:34.120.127.130;</Data><Data Name='Image'>C:\Program Files\Elastic\Endpoint\elastic-endpoint.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:37:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:37:43.739159700Z'/><EventRecordID>434</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:37:43.729</Data><Data Name='ProcessGuid'>{3CBB8FBE-8457-6571-B809-000000001200}</Data><Data Name='ProcessId'>4056</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:37:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:37:42.990105600Z'/><EventRecordID>433</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:37:42.980</Data><Data Name='ProcessGuid'>{3CBB8FBE-8456-6571-B709-000000001200}</Data><Data Name='ProcessId'>10140</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:37:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:37:42.223627000Z'/><EventRecordID>432</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:37:42.214</Data><Data Name='ProcessGuid'>{3CBB8FBE-8456-6571-B609-000000001200}</Data><Data Name='ProcessId'>3764</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:37:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:37:40.742263700Z'/><EventRecordID>431</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:37:40.732</Data><Data Name='ProcessGuid'>{3CBB8FBE-8454-6571-B509-000000001200}</Data><Data Name='ProcessId'>4448</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:37:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:37:39.989523800Z'/><EventRecordID>430</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:37:39.979</Data><Data Name='ProcessGuid'>{3CBB8FBE-8453-6571-B409-000000001200}</Data><Data Name='ProcessId'>6816</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:37:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:37:39.224567500Z'/><EventRecordID>429</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:37:39.214</Data><Data Name='ProcessGuid'>{3CBB8FBE-8453-6571-B309-000000001200}</Data><Data Name='ProcessId'>2700</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:37:10+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:37:10.664291200Z'/><EventRecordID>428</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:37:10.660</Data><Data Name='ProcessGuid'>{3CBB8FBE-8436-6571-B109-000000001200}</Data><Data Name='ProcessId'>8892</Data><Data Name='Image'>C:\Windows\System32\mmc.exe</Data><Data Name='FileVersion'>10.0.14393.953 (rs1_release_inmarket.170303-1614)</Data><Data Name='Description'>Microsoft Management Console</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>mmc.exe</Data><Data Name='CommandLine'>"C:\Windows\system32\mmc.exe" "C:\Windows\system32\services.msc" </Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-99C8-040000000000}</Data><Data Name='LogonId'>0x4c899</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=C75224D3741563FBD526BB7813488A4A,SHA256=6A9BDBFCF4E2DB18F62C55A46C0C94B765165DA150DA6E8E0A87C740C71887BB,IMPHASH=ED5A55DAB5A02F29D6EE7E0015F91A9F</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0240-656E-5100-000000001200}</Data><Data Name='ParentProcessId'>4984</Data><Data Name='ParentImage'>C:\Windows\explorer.exe</Data><Data Name='ParentCommandLine'>C:\Windows\Explorer.EXE</Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:37:10+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:37:10.482307600Z'/><EventRecordID>427</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:37:10.477</Data><Data Name='ProcessGuid'>{3CBB8FBE-8436-6571-AD09-000000001200}</Data><Data Name='ProcessId'>6664</Data><Data Name='Image'>C:\Windows\System32\mmc.exe</Data><Data Name='FileVersion'>10.0.14393.953 (rs1_release_inmarket.170303-1614)</Data><Data Name='Description'>Microsoft Management Console</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>mmc.exe</Data><Data Name='CommandLine'>"C:\Windows\system32\mmc.exe" "C:\Windows\system32\services.msc" </Data><Data Name='CurrentDirectory'>C:\Users\vagrant\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-AFC8-040000000000}</Data><Data Name='LogonId'>0x4c8af</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>MD5=C75224D3741563FBD526BB7813488A4A,SHA256=6A9BDBFCF4E2DB18F62C55A46C0C94B765165DA150DA6E8E0A87C740C71887BB,IMPHASH=ED5A55DAB5A02F29D6EE7E0015F91A9F</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0240-656E-5100-000000001200}</Data><Data Name='ParentProcessId'>4984</Data><Data Name='ParentImage'>C:\Windows\explorer.exe</Data><Data Name='ParentCommandLine'>C:\Windows\Explorer.EXE</Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:36:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:36:43.759119300Z'/><EventRecordID>426</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:36:43.734</Data><Data Name='ProcessGuid'>{3CBB8FBE-841B-6571-A909-000000001200}</Data><Data Name='ProcessId'>2120</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:36:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:36:42.979627800Z'/><EventRecordID>425</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:36:42.969</Data><Data Name='ProcessGuid'>{3CBB8FBE-841A-6571-A809-000000001200}</Data><Data Name='ProcessId'>10004</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:36:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:36:42.197783000Z'/><EventRecordID>424</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:36:42.187</Data><Data Name='ProcessGuid'>{3CBB8FBE-841A-6571-A709-000000001200}</Data><Data Name='ProcessId'>9200</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:36:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:36:40.743309900Z'/><EventRecordID>423</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:36:40.734</Data><Data Name='ProcessGuid'>{3CBB8FBE-8418-6571-A609-000000001200}</Data><Data Name='ProcessId'>6072</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:36:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:36:39.962441600Z'/><EventRecordID>422</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:36:39.952</Data><Data Name='ProcessGuid'>{3CBB8FBE-8417-6571-A509-000000001200}</Data><Data Name='ProcessId'>9952</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:36:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:36:39.211581200Z'/><EventRecordID>421</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:36:39.202</Data><Data Name='ProcessGuid'>{3CBB8FBE-8417-6571-A409-000000001200}</Data><Data Name='ProcessId'>5364</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:35:47+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:35:47.611986700Z'/><EventRecordID>420</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:35:46.612</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:35:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:35:43.715246800Z'/><EventRecordID>419</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:35:43.706</Data><Data Name='ProcessGuid'>{3CBB8FBE-83DF-6571-A309-000000001200}</Data><Data Name='ProcessId'>980</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:35:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:35:42.964989200Z'/><EventRecordID>418</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:35:42.956</Data><Data Name='ProcessGuid'>{3CBB8FBE-83DE-6571-A209-000000001200}</Data><Data Name='ProcessId'>1896</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:35:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:35:42.185377300Z'/><EventRecordID>417</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:35:42.175</Data><Data Name='ProcessGuid'>{3CBB8FBE-83DE-6571-A109-000000001200}</Data><Data Name='ProcessId'>7536</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:35:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:35:40.698729900Z'/><EventRecordID>416</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:35:40.690</Data><Data Name='ProcessGuid'>{3CBB8FBE-83DC-6571-A009-000000001200}</Data><Data Name='ProcessId'>1960</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:35:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:35:39.934339800Z'/><EventRecordID>415</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:35:39.925</Data><Data Name='ProcessGuid'>{3CBB8FBE-83DB-6571-9F09-000000001200}</Data><Data Name='ProcessId'>6212</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:35:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:35:39.185333700Z'/><EventRecordID>414</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:35:39.174</Data><Data Name='ProcessGuid'>{3CBB8FBE-83DB-6571-9E09-000000001200}</Data><Data Name='ProcessId'>5960</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:34:48+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:34:48.771526000Z'/><EventRecordID>413</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:34:46.775</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2000-000000001200}</Data><Data Name='ProcessId'>2408</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\spoolsv.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:34:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:34:43.746338900Z'/><EventRecordID>412</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:34:43.725</Data><Data Name='ProcessGuid'>{3CBB8FBE-83A3-6571-9D09-000000001200}</Data><Data Name='ProcessId'>4480</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:34:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:34:42.968606000Z'/><EventRecordID>411</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:34:42.959</Data><Data Name='ProcessGuid'>{3CBB8FBE-83A2-6571-9C09-000000001200}</Data><Data Name='ProcessId'>6040</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:34:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:34:42.172930500Z'/><EventRecordID>410</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:34:42.162</Data><Data Name='ProcessGuid'>{3CBB8FBE-83A2-6571-9B09-000000001200}</Data><Data Name='ProcessId'>8400</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:34:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:34:40.719935200Z'/><EventRecordID>409</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:34:40.709</Data><Data Name='ProcessGuid'>{3CBB8FBE-83A0-6571-9A09-000000001200}</Data><Data Name='ProcessId'>9240</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:34:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:34:39.954396200Z'/><EventRecordID>408</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:34:39.944</Data><Data Name='ProcessGuid'>{3CBB8FBE-839F-6571-9909-000000001200}</Data><Data Name='ProcessId'>9132</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:34:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:34:39.176903900Z'/><EventRecordID>407</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:34:39.164</Data><Data Name='ProcessGuid'>{3CBB8FBE-839F-6571-9809-000000001200}</Data><Data Name='ProcessId'>7764</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:33:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:33:43.706981400Z'/><EventRecordID>406</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:33:43.697</Data><Data Name='ProcessGuid'>{3CBB8FBE-8367-6571-9709-000000001200}</Data><Data Name='ProcessId'>2896</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:33:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:33:42.956142100Z'/><EventRecordID>405</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:33:42.947</Data><Data Name='ProcessGuid'>{3CBB8FBE-8366-6571-9609-000000001200}</Data><Data Name='ProcessId'>8824</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:33:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:33:42.153171400Z'/><EventRecordID>404</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:33:42.143</Data><Data Name='ProcessGuid'>{3CBB8FBE-8366-6571-9509-000000001200}</Data><Data Name='ProcessId'>6860</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:33:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:33:40.676931600Z'/><EventRecordID>403</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:33:40.666</Data><Data Name='ProcessGuid'>{3CBB8FBE-8364-6571-9409-000000001200}</Data><Data Name='ProcessId'>10060</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:33:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:33:39.909133500Z'/><EventRecordID>402</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:33:39.900</Data><Data Name='ProcessGuid'>{3CBB8FBE-8363-6571-9309-000000001200}</Data><Data Name='ProcessId'>5784</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:33:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:33:39.158836300Z'/><EventRecordID>401</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:33:39.150</Data><Data Name='ProcessGuid'>{3CBB8FBE-8363-6571-9209-000000001200}</Data><Data Name='ProcessId'>7636</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:32:53+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:32:53.479940900Z'/><EventRecordID>400</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:32:52.486</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>www.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:172.217.18.4;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:32:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:32:43.710327200Z'/><EventRecordID>399</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:32:43.700</Data><Data Name='ProcessGuid'>{3CBB8FBE-832B-6571-9009-000000001200}</Data><Data Name='ProcessId'>2440</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:32:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:32:42.959390000Z'/><EventRecordID>398</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:32:42.949</Data><Data Name='ProcessGuid'>{3CBB8FBE-832A-6571-8F09-000000001200}</Data><Data Name='ProcessId'>9984</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:32:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:32:42.147210100Z'/><EventRecordID>397</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:32:42.138</Data><Data Name='ProcessGuid'>{3CBB8FBE-832A-6571-8E09-000000001200}</Data><Data Name='ProcessId'>3220</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:32:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:32:40.651748100Z'/><EventRecordID>396</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:32:40.639</Data><Data Name='ProcessGuid'>{3CBB8FBE-8328-6571-8D09-000000001200}</Data><Data Name='ProcessId'>7768</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:32:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:32:39.882414000Z'/><EventRecordID>395</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:32:39.872</Data><Data Name='ProcessGuid'>{3CBB8FBE-8327-6571-8C09-000000001200}</Data><Data Name='ProcessId'>3948</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:32:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:32:39.146850600Z'/><EventRecordID>394</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:32:39.137</Data><Data Name='ProcessGuid'>{3CBB8FBE-8327-6571-8B09-000000001200}</Data><Data Name='ProcessId'>5400</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:32:21+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:32:21.153476800Z'/><EventRecordID>393</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:32:21.137</Data><Data Name='ProcessGuid'>{3CBB8FBE-8314-6571-8A09-000000001200}</Data><Data Name='ProcessId'>5536</Data><Data Name='Image'>C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE</Data><Data Name='TargetObject'>HKU\S-1-5-21-2479543311-1709999589-3761869525-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable</Data><Data Name='Details'>DWORD (0x00000000)</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:32:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:32:20.441995600Z'/><EventRecordID>392</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:32:20.416</Data><Data Name='ProcessGuid'>{3CBB8FBE-8314-6571-8A09-000000001200}</Data><Data Name='ProcessId'>5536</Data><Data Name='Image'>C:\Program Files (x86)\Internet Explorer\iexplore.exe</Data><Data Name='FileVersion'>11.00.14393.1715 (rs1_release_inmarket.170906-1810)</Data><Data Name='Description'>Internet Explorer</Data><Data Name='Product'>Internet Explorer</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>IEXPLORE.EXE</Data><Data Name='CommandLine'>"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:8172 CREDAT:17409 /prefetch:2</Data><Data Name='CurrentDirectory'>C:\Users\vagrant\Desktop\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-AFC8-040000000000}</Data><Data Name='LogonId'>0x4c8af</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>MD5=27D8231B9DA1B46F9D3FA238A096A24D,SHA256=EB0AAE374795B6A13227D8A25A92DB1CE36EF4BEB7939BCFE39061524DADB2EA,IMPHASH=F47EDAF3B9B093095911E83BA7D4F612</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8314-6571-8909-000000001200}</Data><Data Name='ParentProcessId'>8172</Data><Data Name='ParentImage'>C:\Program Files\Internet Explorer\iexplore.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\Internet Explorer\iexplore.exe" C:\Users\vagrant\Downloads\Sysmon\sysmon-config.xml</Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:32:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:32:20.395167100Z'/><EventRecordID>391</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:32:20.387</Data><Data Name='ProcessGuid'>{3CBB8FBE-8314-6571-8909-000000001200}</Data><Data Name='ProcessId'>8172</Data><Data Name='Image'>C:\Program Files\Internet Explorer\iexplore.exe</Data><Data Name='TargetObject'>HKU\S-1-5-21-2479543311-1709999589-3761869525-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable</Data><Data Name='Details'>DWORD (0x00000000)</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:32:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:32:20.242571500Z'/><EventRecordID>390</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:32:20.217</Data><Data Name='ProcessGuid'>{3CBB8FBE-8314-6571-8909-000000001200}</Data><Data Name='ProcessId'>8172</Data><Data Name='Image'>C:\Program Files\Internet Explorer\iexplore.exe</Data><Data Name='FileVersion'>11.00.14393.1715 (rs1_release_inmarket.170906-1810)</Data><Data Name='Description'>Internet Explorer</Data><Data Name='Product'>Internet Explorer</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>IEXPLORE.EXE</Data><Data Name='CommandLine'>"C:\Program Files\Internet Explorer\iexplore.exe" C:\Users\vagrant\Downloads\Sysmon\sysmon-config.xml</Data><Data Name='CurrentDirectory'>C:\Users\vagrant\Downloads\Sysmon\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-AFC8-040000000000}</Data><Data Name='LogonId'>0x4c8af</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>MD5=2B328FEB08F104F1973C230D6C25356E,SHA256=63FE944C58EDC23529977031384A7C3FD4EE33AFE201AC78419E066D069F67A8,IMPHASH=F814EEB89ACB44E7EB900AA33DBEB9A3</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0240-656E-5100-000000001200}</Data><Data Name='ParentProcessId'>4984</Data><Data Name='ParentImage'>C:\Windows\explorer.exe</Data><Data Name='ParentCommandLine'>C:\Windows\Explorer.EXE</Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T09:32:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:32:20.211104800Z'/><EventRecordID>389</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:32:20.199</Data><Data Name='ProcessGuid'>{3CBB8FBE-0240-656E-5100-000000001200}</Data><Data Name='ProcessId'>4984</Data><Data Name='Image'>C:\Windows\Explorer.EXE</Data><Data Name='TargetObject'>HKU\S-1-5-21-2479543311-1709999589-3761869525-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{17FE9752-0B5A-4665-84CD-569794602F5C} {7F9185B0-CB92-43C5-80A9-92277A4F7B54} 0xFFFF</Data><Data Name='Details'>Binary Data</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:32:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:32:20.147091900Z'/><EventRecordID>388</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:32:20.143</Data><Data Name='ProcessGuid'>{3CBB8FBE-8314-6571-8809-000000001200}</Data><Data Name='ProcessId'>9460</Data><Data Name='Image'>C:\Windows\System32\smartscreen.exe</Data><Data Name='FileVersion'>10.0.14393.1715 (rs1_release_inmarket.170906-1810)</Data><Data Name='Description'>SmartScreen</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>smartscreen.exe</Data><Data Name='CommandLine'>C:\Windows\System32\smartscreen.exe -Embedding</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-AFC8-040000000000}</Data><Data Name='LogonId'>0x4c8af</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>MD5=4A619778CC5B53F92CA6750F840455B7,SHA256=01114EE31AA9B24B6BDD67C3E0AD89C5C758D8AD416A7851E4F24937A57C5223,IMPHASH=A88BD4C4BF193E3DD40E8408EB103B65</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0205-656E-0C00-000000001200}</Data><Data Name='ParentProcessId'>788</Data><Data Name='ParentImage'>C:\Windows\System32\svchost.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\svchost.exe -k DcomLaunch</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:31:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:31:43.711440200Z'/><EventRecordID>387</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:31:43.702</Data><Data Name='ProcessGuid'>{3CBB8FBE-82EF-6571-8709-000000001200}</Data><Data Name='ProcessId'>7204</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:31:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:31:42.947259400Z'/><EventRecordID>386</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:31:42.937</Data><Data Name='ProcessGuid'>{3CBB8FBE-82EE-6571-8609-000000001200}</Data><Data Name='ProcessId'>6464</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:31:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:31:42.138354600Z'/><EventRecordID>385</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:31:42.128</Data><Data Name='ProcessGuid'>{3CBB8FBE-82EE-6571-8509-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:31:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:31:40.633974800Z'/><EventRecordID>384</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:31:40.624</Data><Data Name='ProcessGuid'>{3CBB8FBE-82EC-6571-8409-000000001200}</Data><Data Name='ProcessId'>980</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:31:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:31:39.885581100Z'/><EventRecordID>383</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:31:39.875</Data><Data Name='ProcessGuid'>{3CBB8FBE-82EB-6571-8309-000000001200}</Data><Data Name='ProcessId'>7104</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:31:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:31:39.118122000Z'/><EventRecordID>382</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:31:39.109</Data><Data Name='ProcessGuid'>{3CBB8FBE-82EB-6571-8209-000000001200}</Data><Data Name='ProcessId'>7196</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:30:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:30:43.682766800Z'/><EventRecordID>381</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:30:43.673</Data><Data Name='ProcessGuid'>{3CBB8FBE-82B3-6571-8009-000000001200}</Data><Data Name='ProcessId'>8400</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:30:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:30:42.916387300Z'/><EventRecordID>380</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:30:42.908</Data><Data Name='ProcessGuid'>{3CBB8FBE-82B2-6571-7F09-000000001200}</Data><Data Name='ProcessId'>10084</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:30:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:30:42.134824800Z'/><EventRecordID>379</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:30:42.126</Data><Data Name='ProcessGuid'>{3CBB8FBE-82B2-6571-7E09-000000001200}</Data><Data Name='ProcessId'>10196</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:30:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:30:40.620283200Z'/><EventRecordID>378</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:30:40.610</Data><Data Name='ProcessGuid'>{3CBB8FBE-82B0-6571-7D09-000000001200}</Data><Data Name='ProcessId'>7980</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:30:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:30:39.854145900Z'/><EventRecordID>377</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:30:39.845</Data><Data Name='ProcessGuid'>{3CBB8FBE-82AF-6571-7C09-000000001200}</Data><Data Name='ProcessId'>9788</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:30:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:30:39.105467900Z'/><EventRecordID>376</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:30:39.095</Data><Data Name='ProcessGuid'>{3CBB8FBE-82AF-6571-7B09-000000001200}</Data><Data Name='ProcessId'>6904</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:29:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:29:43.687216100Z'/><EventRecordID>375</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:29:43.674</Data><Data Name='ProcessGuid'>{3CBB8FBE-8277-6571-7A09-000000001200}</Data><Data Name='ProcessId'>6152</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:29:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:29:42.918103300Z'/><EventRecordID>374</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:29:42.909</Data><Data Name='ProcessGuid'>{3CBB8FBE-8276-6571-7909-000000001200}</Data><Data Name='ProcessId'>10096</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:29:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:29:42.120897700Z'/><EventRecordID>373</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:29:42.112</Data><Data Name='ProcessGuid'>{3CBB8FBE-8276-6571-7809-000000001200}</Data><Data Name='ProcessId'>7512</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:29:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:29:40.604399700Z'/><EventRecordID>372</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:29:40.595</Data><Data Name='ProcessGuid'>{3CBB8FBE-8274-6571-7709-000000001200}</Data><Data Name='ProcessId'>6360</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:29:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:29:39.855355300Z'/><EventRecordID>371</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:29:39.846</Data><Data Name='ProcessGuid'>{3CBB8FBE-8273-6571-7609-000000001200}</Data><Data Name='ProcessId'>6536</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:29:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:29:39.090284300Z'/><EventRecordID>370</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:29:39.080</Data><Data Name='ProcessGuid'>{3CBB8FBE-8273-6571-7509-000000001200}</Data><Data Name='ProcessId'>5372</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:28:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:28:43.654754300Z'/><EventRecordID>369</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:28:43.643</Data><Data Name='ProcessGuid'>{3CBB8FBE-823B-6571-7409-000000001200}</Data><Data Name='ProcessId'>9876</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:28:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:28:42.901805100Z'/><EventRecordID>368</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:28:42.894</Data><Data Name='ProcessGuid'>{3CBB8FBE-823A-6571-7309-000000001200}</Data><Data Name='ProcessId'>7612</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:28:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:28:42.125404800Z'/><EventRecordID>367</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:28:42.116</Data><Data Name='ProcessGuid'>{3CBB8FBE-823A-6571-7209-000000001200}</Data><Data Name='ProcessId'>8476</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:28:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:28:40.607589900Z'/><EventRecordID>366</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:28:40.597</Data><Data Name='ProcessGuid'>{3CBB8FBE-8238-6571-7109-000000001200}</Data><Data Name='ProcessId'>8412</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:28:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:28:39.858017100Z'/><EventRecordID>365</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:28:39.847</Data><Data Name='ProcessGuid'>{3CBB8FBE-8237-6571-7009-000000001200}</Data><Data Name='ProcessId'>3964</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:28:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:28:39.076112800Z'/><EventRecordID>364</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:28:39.066</Data><Data Name='ProcessGuid'>{3CBB8FBE-8237-6571-6F09-000000001200}</Data><Data Name='ProcessId'>7680</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:27:54+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:27:54.148459900Z'/><EventRecordID>363</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:27:52.152</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>www.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:142.250.186.68;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T09:27:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:27:43.638446300Z'/><EventRecordID>362</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:27:43.628</Data><Data Name='ProcessGuid'>{3CBB8FBE-81FF-6571-6E09-000000001200}</Data><Data Name='ProcessId'>6036</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:27:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:27:42.886204200Z'/><EventRecordID>361</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:27:42.877</Data><Data Name='ProcessGuid'>{3CBB8FBE-81FE-6571-6D09-000000001200}</Data><Data Name='ProcessId'>8392</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:27:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:27:42.105522500Z'/><EventRecordID>360</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:27:42.096</Data><Data Name='ProcessGuid'>{3CBB8FBE-81FE-6571-6C09-000000001200}</Data><Data Name='ProcessId'>7232</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:27:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:27:40.590227700Z'/><EventRecordID>359</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:27:40.580</Data><Data Name='ProcessGuid'>{3CBB8FBE-81FC-6571-6B09-000000001200}</Data><Data Name='ProcessId'>9768</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:27:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:27:39.841340700Z'/><EventRecordID>358</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:27:39.831</Data><Data Name='ProcessGuid'>{3CBB8FBE-81FB-6571-6A09-000000001200}</Data><Data Name='ProcessId'>2560</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:27:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:27:39.074946500Z'/><EventRecordID>357</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:27:39.065</Data><Data Name='ProcessGuid'>{3CBB8FBE-81FB-6571-6909-000000001200}</Data><Data Name='ProcessId'>7128</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:26:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:26:43.636197000Z'/><EventRecordID>356</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:26:43.626</Data><Data Name='ProcessGuid'>{3CBB8FBE-81C3-6571-6509-000000001200}</Data><Data Name='ProcessId'>7312</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:26:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:26:42.884818000Z'/><EventRecordID>355</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:26:42.875</Data><Data Name='ProcessGuid'>{3CBB8FBE-81C2-6571-6409-000000001200}</Data><Data Name='ProcessId'>7196</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:26:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:26:42.103263800Z'/><EventRecordID>354</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:26:42.094</Data><Data Name='ProcessGuid'>{3CBB8FBE-81C2-6571-6309-000000001200}</Data><Data Name='ProcessId'>3192</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:26:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:26:40.571976900Z'/><EventRecordID>353</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:26:40.562</Data><Data Name='ProcessGuid'>{3CBB8FBE-81C0-6571-6209-000000001200}</Data><Data Name='ProcessId'>1348</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:26:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:26:39.820624600Z'/><EventRecordID>352</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:26:39.812</Data><Data Name='ProcessGuid'>{3CBB8FBE-81BF-6571-6109-000000001200}</Data><Data Name='ProcessId'>5224</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:26:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:26:39.072261700Z'/><EventRecordID>351</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:26:39.063</Data><Data Name='ProcessGuid'>{3CBB8FBE-81BF-6571-6009-000000001200}</Data><Data Name='ProcessId'>3232</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:25:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:25:43.647565000Z'/><EventRecordID>350</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:25:43.637</Data><Data Name='ProcessGuid'>{3CBB8FBE-8187-6571-5F09-000000001200}</Data><Data Name='ProcessId'>3280</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:25:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:25:42.897242500Z'/><EventRecordID>349</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:25:42.888</Data><Data Name='ProcessGuid'>{3CBB8FBE-8186-6571-5E09-000000001200}</Data><Data Name='ProcessId'>6020</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:25:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:25:42.115099400Z'/><EventRecordID>348</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:25:42.106</Data><Data Name='ProcessGuid'>{3CBB8FBE-8186-6571-5D09-000000001200}</Data><Data Name='ProcessId'>6344</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:25:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:25:40.584617800Z'/><EventRecordID>347</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:25:40.575</Data><Data Name='ProcessGuid'>{3CBB8FBE-8184-6571-5C09-000000001200}</Data><Data Name='ProcessId'>10200</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:25:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:25:39.818540600Z'/><EventRecordID>346</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:25:39.809</Data><Data Name='ProcessGuid'>{3CBB8FBE-8183-6571-5B09-000000001200}</Data><Data Name='ProcessId'>3960</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:25:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:25:39.062396700Z'/><EventRecordID>345</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:25:39.053</Data><Data Name='ProcessGuid'>{3CBB8FBE-8183-6571-5A09-000000001200}</Data><Data Name='ProcessId'>6232</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:24:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:24:43.641408100Z'/><EventRecordID>344</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:24:43.631</Data><Data Name='ProcessGuid'>{3CBB8FBE-814B-6571-5909-000000001200}</Data><Data Name='ProcessId'>10132</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:24:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:24:42.889893100Z'/><EventRecordID>343</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:24:42.882</Data><Data Name='ProcessGuid'>{3CBB8FBE-814A-6571-5809-000000001200}</Data><Data Name='ProcessId'>10036</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:24:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:24:42.109344800Z'/><EventRecordID>342</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:24:42.100</Data><Data Name='ProcessGuid'>{3CBB8FBE-814A-6571-5709-000000001200}</Data><Data Name='ProcessId'>8676</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:24:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:24:40.578537400Z'/><EventRecordID>341</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:24:40.568</Data><Data Name='ProcessGuid'>{3CBB8FBE-8148-6571-5609-000000001200}</Data><Data Name='ProcessId'>7928</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:24:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:24:39.829575700Z'/><EventRecordID>340</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:24:39.819</Data><Data Name='ProcessGuid'>{3CBB8FBE-8147-6571-5509-000000001200}</Data><Data Name='ProcessId'>6316</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:24:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:24:39.061630900Z'/><EventRecordID>339</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:24:39.053</Data><Data Name='ProcessGuid'>{3CBB8FBE-8147-6571-5409-000000001200}</Data><Data Name='ProcessId'>9160</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:23:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:23:43.647257000Z'/><EventRecordID>338</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:23:43.636</Data><Data Name='ProcessGuid'>{3CBB8FBE-810F-6571-5309-000000001200}</Data><Data Name='ProcessId'>6476</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:23:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:23:42.881095300Z'/><EventRecordID>337</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:23:42.870</Data><Data Name='ProcessGuid'>{3CBB8FBE-810E-6571-5209-000000001200}</Data><Data Name='ProcessId'>6796</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:23:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:23:42.114001600Z'/><EventRecordID>336</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:23:42.105</Data><Data Name='ProcessGuid'>{3CBB8FBE-810E-6571-5109-000000001200}</Data><Data Name='ProcessId'>5836</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:23:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:23:40.568995200Z'/><EventRecordID>335</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:23:40.558</Data><Data Name='ProcessGuid'>{3CBB8FBE-810C-6571-5009-000000001200}</Data><Data Name='ProcessId'>8556</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:23:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:23:39.822615700Z'/><EventRecordID>334</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:23:39.808</Data><Data Name='ProcessGuid'>{3CBB8FBE-810B-6571-4F09-000000001200}</Data><Data Name='ProcessId'>9936</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:23:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:23:39.052297600Z'/><EventRecordID>333</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:23:39.043</Data><Data Name='ProcessGuid'>{3CBB8FBE-810B-6571-4E09-000000001200}</Data><Data Name='ProcessId'>7692</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:22:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:22:43.603727200Z'/><EventRecordID>332</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:22:43.595</Data><Data Name='ProcessGuid'>{3CBB8FBE-80D3-6571-4D09-000000001200}</Data><Data Name='ProcessId'>3800</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:22:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:22:42.854012200Z'/><EventRecordID>331</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:22:42.844</Data><Data Name='ProcessGuid'>{3CBB8FBE-80D2-6571-4C09-000000001200}</Data><Data Name='ProcessId'>7976</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:22:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:22:42.104868700Z'/><EventRecordID>330</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:22:42.095</Data><Data Name='ProcessGuid'>{3CBB8FBE-80D2-6571-4B09-000000001200}</Data><Data Name='ProcessId'>5792</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:22:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:22:40.558692500Z'/><EventRecordID>329</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:22:40.548</Data><Data Name='ProcessGuid'>{3CBB8FBE-80D0-6571-4A09-000000001200}</Data><Data Name='ProcessId'>1144</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:22:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:22:39.811117500Z'/><EventRecordID>328</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:22:39.800</Data><Data Name='ProcessGuid'>{3CBB8FBE-80CF-6571-4909-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:22:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:22:39.043269600Z'/><EventRecordID>327</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:22:39.032</Data><Data Name='ProcessGuid'>{3CBB8FBE-80CF-6571-4809-000000001200}</Data><Data Name='ProcessId'>9924</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:22:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:22:19.565292900Z'/><EventRecordID>326</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:22:17.927</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1100-000000001200}</Data><Data Name='ProcessId'>348</Data><Data Name='QueryName'>wpad</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>-</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\LOCAL SERVICE</Data></EventData></Event>
2023-12-07T09:21:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:21:43.607997800Z'/><EventRecordID>325</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:21:43.599</Data><Data Name='ProcessGuid'>{3CBB8FBE-8097-6571-4709-000000001200}</Data><Data Name='ProcessId'>6432</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:21:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:21:42.858173900Z'/><EventRecordID>324</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:21:42.850</Data><Data Name='ProcessGuid'>{3CBB8FBE-8096-6571-4609-000000001200}</Data><Data Name='ProcessId'>9788</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:21:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:21:42.096526600Z'/><EventRecordID>323</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:21:42.087</Data><Data Name='ProcessGuid'>{3CBB8FBE-8096-6571-4509-000000001200}</Data><Data Name='ProcessId'>4084</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:21:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:21:40.548591200Z'/><EventRecordID>322</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:21:40.538</Data><Data Name='ProcessGuid'>{3CBB8FBE-8094-6571-4409-000000001200}</Data><Data Name='ProcessId'>6936</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:21:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:21:39.797786400Z'/><EventRecordID>321</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:21:39.788</Data><Data Name='ProcessGuid'>{3CBB8FBE-8093-6571-4309-000000001200}</Data><Data Name='ProcessId'>10160</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:21:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:21:39.031575800Z'/><EventRecordID>320</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:21:39.022</Data><Data Name='ProcessGuid'>{3CBB8FBE-8093-6571-4209-000000001200}</Data><Data Name='ProcessId'>9536</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:21:21+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:21:21.319656800Z'/><EventRecordID>319</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:21:20.445</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>www.google.fr</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:142.250.185.67;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:20:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:20:43.613290800Z'/><EventRecordID>318</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:20:43.604</Data><Data Name='ProcessGuid'>{3CBB8FBE-805B-6571-4109-000000001200}</Data><Data Name='ProcessId'>1916</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:20:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:20:42.864003300Z'/><EventRecordID>317</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:20:42.854</Data><Data Name='ProcessGuid'>{3CBB8FBE-805A-6571-4009-000000001200}</Data><Data Name='ProcessId'>5372</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:20:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:20:42.097735000Z'/><EventRecordID>316</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:20:42.088</Data><Data Name='ProcessGuid'>{3CBB8FBE-805A-6571-3F09-000000001200}</Data><Data Name='ProcessId'>9896</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:20:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:20:40.534583600Z'/><EventRecordID>315</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:20:40.526</Data><Data Name='ProcessGuid'>{3CBB8FBE-8058-6571-3E09-000000001200}</Data><Data Name='ProcessId'>2352</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:20:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:20:39.772345900Z'/><EventRecordID>314</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:20:39.761</Data><Data Name='ProcessGuid'>{3CBB8FBE-8057-6571-3D09-000000001200}</Data><Data Name='ProcessId'>7624</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:20:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:20:39.022477200Z'/><EventRecordID>313</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:20:39.011</Data><Data Name='ProcessGuid'>{3CBB8FBE-8057-6571-3C09-000000001200}</Data><Data Name='ProcessId'>8472</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:45+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:45.497641400Z'/><EventRecordID>312</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:44.489</Data><Data Name='ProcessGuid'>{3CBB8FBE-8020-6571-3A09-000000001200}</Data><Data Name='ProcessId'>9272</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:45+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:45.145140400Z'/><EventRecordID>311</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:45.134</Data><Data Name='ProcessGuid'>{3CBB8FBE-8021-6571-3B09-000000001200}</Data><Data Name='ProcessId'>7228</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-winprintmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Windows Print Monitor </Data><Data Name='Product'>splunk Application </Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-winprintmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-winprintmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=FDEB6BA573575665D847C8C88DFA6B28,SHA256=00FC8040D205B3290D204EB5E6AEAF5E21CF6F5EDB081555CDF81AD61F306218,IMPHASH=355E487ADBCE53AA00CC9620C5813D5A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:44+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:44.351601300Z'/><EventRecordID>310</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:44.342</Data><Data Name='ProcessGuid'>{3CBB8FBE-8020-6571-3A09-000000001200}</Data><Data Name='ProcessId'>9272</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Monitor windows event logs</Data><Data Name='Product'>splunk Application </Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-winevtlog.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AE95292862972429C2FBD9541C739C2B,SHA256=C1899D942B83A761EADA6303334A9E6946A7206A59E678F0039D3AB527785522,IMPHASH=EDE9B13E7663B8E763DD4604CD8C3BF7</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:43.587359200Z'/><EventRecordID>309</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:43.577</Data><Data Name='ProcessGuid'>{3CBB8FBE-801F-6571-3909-000000001200}</Data><Data Name='ProcessId'>7200</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:42.835505500Z'/><EventRecordID>308</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:42.826</Data><Data Name='ProcessGuid'>{3CBB8FBE-801E-6571-3809-000000001200}</Data><Data Name='ProcessId'>10144</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:42+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:42.071018500Z'/><EventRecordID>307</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:42.061</Data><Data Name='ProcessGuid'>{3CBB8FBE-801E-6571-3709-000000001200}</Data><Data Name='ProcessId'>9804</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:41+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:41.294306600Z'/><EventRecordID>306</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:41.284</Data><Data Name='ProcessGuid'>{3CBB8FBE-801D-6571-3609-000000001200}</Data><Data Name='ProcessId'>7332</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-perfmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Performance monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-perfmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-perfmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=37F610EA3267B4C636A52CC17C72F5E9,SHA256=154252976F3CDC663C1999E5BF6958E4A9717874E2117061A0E40F2F1D97BE27,IMPHASH=35AE00EA6705AD0DB2C706FD3FAF93B6</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:40+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:40.509437000Z'/><EventRecordID>305</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:40.499</Data><Data Name='ProcessGuid'>{3CBB8FBE-801C-6571-3509-000000001200}</Data><Data Name='ProcessId'>6668</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:39.758873500Z'/><EventRecordID>304</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:39.749</Data><Data Name='ProcessGuid'>{3CBB8FBE-801B-6571-3409-000000001200}</Data><Data Name='ProcessId'>8</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:39+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:39.008593600Z'/><EventRecordID>303</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:38.999</Data><Data Name='ProcessGuid'>{3CBB8FBE-801A-6571-3309-000000001200}</Data><Data Name='ProcessId'>7144</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:38+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:38.297826600Z'/><EventRecordID>302</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:38.231</Data><Data Name='ProcessGuid'>{3CBB8FBE-801A-6571-3209-000000001200}</Data><Data Name='ProcessId'>6596</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-wmi.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Remote Performance monitor using WMI</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-wmi.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-wmi.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=7A440F2DF244985160C5B54CDBBA547D,SHA256=7E1DBA295076C76618106FD18E882B190BF0542AD2981200D01074B021BF76CF,IMPHASH=7C7770CDB275E49574E79FDF395C7C60</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:36+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:36.137550500Z'/><EventRecordID>301</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:36.125</Data><Data Name='ProcessGuid'>{3CBB8FBE-8018-6571-3109-000000001200}</Data><Data Name='ProcessId'>7364</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\powershell2.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:35.998638000Z'/><EventRecordID>300</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:35.986</Data><Data Name='ProcessGuid'>{3CBB8FBE-8017-6571-3009-000000001200}</Data><Data Name='ProcessId'>4160</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\powershell.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:35.857601500Z'/><EventRecordID>299</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:35.845</Data><Data Name='ProcessGuid'>{3CBB8FBE-8017-6571-2F09-000000001200}</Data><Data Name='ProcessId'>7812</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\perfmon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:35.716793000Z'/><EventRecordID>298</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:35.705</Data><Data Name='ProcessGuid'>{3CBB8FBE-8017-6571-2E09-000000001200}</Data><Data Name='ProcessId'>8956</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\admon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:35.573018300Z'/><EventRecordID>297</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:35.556</Data><Data Name='ProcessGuid'>{3CBB8FBE-8017-6571-2D09-000000001200}</Data><Data Name='ProcessId'>1612</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinRegMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:35.436374200Z'/><EventRecordID>296</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:35.423</Data><Data Name='ProcessGuid'>{3CBB8FBE-8017-6571-2C09-000000001200}</Data><Data Name='ProcessId'>8716</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinPrintMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:35.279108800Z'/><EventRecordID>295</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:35.267</Data><Data Name='ProcessGuid'>{3CBB8FBE-8017-6571-2B09-000000001200}</Data><Data Name='ProcessId'>9800</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinNetMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:35.146502600Z'/><EventRecordID>294</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:35.133</Data><Data Name='ProcessGuid'>{3CBB8FBE-8017-6571-2A09-000000001200}</Data><Data Name='ProcessId'>5536</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinHostMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:34.999101200Z'/><EventRecordID>293</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:34.987</Data><Data Name='ProcessGuid'>{3CBB8FBE-8016-6571-2909-000000001200}</Data><Data Name='ProcessId'>6780</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinEventLog.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:34.860983700Z'/><EventRecordID>292</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:34.849</Data><Data Name='ProcessGuid'>{3CBB8FBE-8016-6571-2809-000000001200}</Data><Data Name='ProcessId'>7960</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\MonitorNoHandle.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:34.146130100Z'/><EventRecordID>291</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:34.142</Data><Data Name='ProcessGuid'>{3CBB8FBE-8016-6571-2709-000000001200}</Data><Data Name='ProcessId'>7244</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal check-xml-files --answer-yes --no-prompt </Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8016-6571-2609-000000001200}</Data><Data Name='ParentProcessId'>7972</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal check-xml-files --answer-yes --no-prompt 2>&1</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:34.136006100Z'/><EventRecordID>290</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:34.127</Data><Data Name='ProcessGuid'>{3CBB8FBE-8016-6571-2609-000000001200}</Data><Data Name='ProcessId'>7972</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal check-xml-files --answer-yes --no-prompt 2>&1</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:33.839157900Z'/><EventRecordID>289</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:33.832</Data><Data Name='ProcessGuid'>{3CBB8FBE-8015-6571-2509-000000001200}</Data><Data Name='ProcessId'>9176</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8015-6571-2409-000000001200}</Data><Data Name='ParentProcessId'>2976</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:33.825005100Z'/><EventRecordID>288</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:33.821</Data><Data Name='ProcessGuid'>{3CBB8FBE-8015-6571-2409-000000001200}</Data><Data Name='ProcessId'>2976</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8015-6571-2309-000000001200}</Data><Data Name='ParentProcessId'>7308</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:33.818362000Z'/><EventRecordID>287</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:33.813</Data><Data Name='ProcessGuid'>{3CBB8FBE-8015-6571-2309-000000001200}</Data><Data Name='ProcessId'>7308</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8012-6571-1609-000000001200}</Data><Data Name='ParentProcessId'>10004</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:33.543460500Z'/><EventRecordID>286</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:33.536</Data><Data Name='ProcessGuid'>{3CBB8FBE-8015-6571-2209-000000001200}</Data><Data Name='ProcessId'>4268</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list replication_port --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8015-6571-2109-000000001200}</Data><Data Name='ParentProcessId'>152</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list replication_port --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:33.523597300Z'/><EventRecordID>285</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:33.515</Data><Data Name='ProcessGuid'>{3CBB8FBE-8015-6571-2109-000000001200}</Data><Data Name='ProcessId'>152</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list replication_port --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8015-6571-2009-000000001200}</Data><Data Name='ParentProcessId'>6828</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list replication_port --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:33.509756500Z'/><EventRecordID>284</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:33.506</Data><Data Name='ProcessGuid'>{3CBB8FBE-8015-6571-2009-000000001200}</Data><Data Name='ProcessId'>6828</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list replication_port --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8012-6571-1609-000000001200}</Data><Data Name='ParentProcessId'>10004</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:33.130661700Z'/><EventRecordID>283</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:33.122</Data><Data Name='ProcessGuid'>{3CBB8FBE-8015-6571-1F09-000000001200}</Data><Data Name='ProcessId'>8036</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd" check-transforms-keys</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8012-6571-1609-000000001200}</Data><Data Name='ParentProcessId'>10004</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:32.575672900Z'/><EventRecordID>282</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:32.569</Data><Data Name='ProcessGuid'>{3CBB8FBE-8014-6571-1E09-000000001200}</Data><Data Name='ProcessId'>9920</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool validate-regex --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8014-6571-1D09-000000001200}</Data><Data Name='ParentProcessId'>8512</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-regex --log-warnings</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:32.562658300Z'/><EventRecordID>281</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:32.557</Data><Data Name='ProcessGuid'>{3CBB8FBE-8014-6571-1D09-000000001200}</Data><Data Name='ProcessId'>8512</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-regex --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8012-6571-1609-000000001200}</Data><Data Name='ParentProcessId'>10004</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:32.059572200Z'/><EventRecordID>280</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:32.053</Data><Data Name='ProcessGuid'>{3CBB8FBE-8014-6571-1C09-000000001200}</Data><Data Name='ProcessId'>7344</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool validate-strptime --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8014-6571-1B09-000000001200}</Data><Data Name='ParentProcessId'>6268</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-strptime --log-warnings</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:32.047530500Z'/><EventRecordID>279</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:32.042</Data><Data Name='ProcessGuid'>{3CBB8FBE-8014-6571-1B09-000000001200}</Data><Data Name='ProcessId'>6268</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>" C:\Program Files\SplunkUniversalForwarder\bin\btool" validate-strptime --log-warnings</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8012-6571-1609-000000001200}</Data><Data Name='ParentProcessId'>10004</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:31+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:31.172417700Z'/><EventRecordID>278</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:31.164</Data><Data Name='ProcessGuid'>{3CBB8FBE-8013-6571-1A09-000000001200}</Data><Data Name='ProcessId'>6620</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool check --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8013-6571-1909-000000001200}</Data><Data Name='ParentProcessId'>7536</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\btool" check --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:31+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:31.159523000Z'/><EventRecordID>277</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:31.155</Data><Data Name='ProcessGuid'>{3CBB8FBE-8013-6571-1909-000000001200}</Data><Data Name='ProcessId'>7536</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>" C:\Program Files\SplunkUniversalForwarder\bin\btool" check --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8012-6571-1609-000000001200}</Data><Data Name='ParentProcessId'>10004</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:30.884928200Z'/><EventRecordID>276</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:30.878</Data><Data Name='ProcessGuid'>{3CBB8FBE-8012-6571-1809-000000001200}</Data><Data Name='ProcessId'>8168</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" check-license</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8012-6571-1609-000000001200}</Data><Data Name='ParentProcessId'>10004</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:30.567977400Z'/><EventRecordID>275</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:30.559</Data><Data Name='ProcessGuid'>{3CBB8FBE-8012-6571-1709-000000001200}</Data><Data Name='ProcessId'>6796</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" generate-ssl</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8012-6571-1609-000000001200}</Data><Data Name='ParentProcessId'>10004</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:30.549917400Z'/><EventRecordID>274</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:30.544</Data><Data Name='ProcessGuid'>{3CBB8FBE-8012-6571-1609-000000001200}</Data><Data Name='ProcessId'>10004</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt </Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8012-6571-1509-000000001200}</Data><Data Name='ParentProcessId'>8864</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt 2>&1</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:30.532978800Z'/><EventRecordID>273</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:30.524</Data><Data Name='ProcessGuid'>{3CBB8FBE-8012-6571-1509-000000001200}</Data><Data Name='ProcessId'>8864</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal pre-flight-checks --answer-yes --no-prompt 2>&1</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:29.966851400Z'/><EventRecordID>272</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:29.959</Data><Data Name='ProcessGuid'>{3CBB8FBE-8011-6571-1409-000000001200}</Data><Data Name='ProcessId'>6248</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list sslConfig --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8011-6571-1309-000000001200}</Data><Data Name='ParentProcessId'>9336</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list sslConfig --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:29.954678900Z'/><EventRecordID>271</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:29.948</Data><Data Name='ProcessGuid'>{3CBB8FBE-8011-6571-1309-000000001200}</Data><Data Name='ProcessId'>9336</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list sslConfig --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8011-6571-1209-000000001200}</Data><Data Name='ParentProcessId'>2444</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list sslConfig --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:29.945064700Z'/><EventRecordID>270</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:29.940</Data><Data Name='ProcessGuid'>{3CBB8FBE-8011-6571-1209-000000001200}</Data><Data Name='ProcessId'>2444</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list sslConfig --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-0509-000000001200}</Data><Data Name='ParentProcessId'>6844</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:29.670001900Z'/><EventRecordID>269</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:29.663</Data><Data Name='ProcessGuid'>{3CBB8FBE-8011-6571-1109-000000001200}</Data><Data Name='ProcessId'>6820</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list watchdog --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8011-6571-1009-000000001200}</Data><Data Name='ParentProcessId'>5836</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list watchdog --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:29.657071200Z'/><EventRecordID>268</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:29.647</Data><Data Name='ProcessGuid'>{3CBB8FBE-8011-6571-1009-000000001200}</Data><Data Name='ProcessId'>5836</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list watchdog --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8011-6571-0F09-000000001200}</Data><Data Name='ParentProcessId'>1068</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list watchdog --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:29.641890300Z'/><EventRecordID>267</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:29.635</Data><Data Name='ProcessGuid'>{3CBB8FBE-8011-6571-0F09-000000001200}</Data><Data Name='ProcessId'>1068</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list watchdog --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-0509-000000001200}</Data><Data Name='ParentProcessId'>6844</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:29.370133700Z'/><EventRecordID>266</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:29.363</Data><Data Name='ProcessGuid'>{3CBB8FBE-8011-6571-0E09-000000001200}</Data><Data Name='ProcessId'>8336</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list kvstore --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8011-6571-0D09-000000001200}</Data><Data Name='ParentProcessId'>8228</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list kvstore --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:29.356504000Z'/><EventRecordID>265</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:29.352</Data><Data Name='ProcessGuid'>{3CBB8FBE-8011-6571-0D09-000000001200}</Data><Data Name='ProcessId'>8228</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list kvstore --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8011-6571-0C09-000000001200}</Data><Data Name='ParentProcessId'>9460</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list kvstore --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:29.347988400Z'/><EventRecordID>264</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:29.341</Data><Data Name='ProcessGuid'>{3CBB8FBE-8011-6571-0C09-000000001200}</Data><Data Name='ProcessId'>9460</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list kvstore --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-0509-000000001200}</Data><Data Name='ParentProcessId'>6844</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:29.069459000Z'/><EventRecordID>263</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:29.062</Data><Data Name='ProcessGuid'>{3CBB8FBE-8011-6571-0B09-000000001200}</Data><Data Name='ProcessId'>3636</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8011-6571-0A09-000000001200}</Data><Data Name='ParentProcessId'>8556</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:29.055130900Z'/><EventRecordID>262</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:29.051</Data><Data Name='ProcessGuid'>{3CBB8FBE-8011-6571-0A09-000000001200}</Data><Data Name='ProcessId'>8556</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8011-6571-0909-000000001200}</Data><Data Name='ParentProcessId'>8636</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:29+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:29.047733600Z'/><EventRecordID>261</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:29.042</Data><Data Name='ProcessGuid'>{3CBB8FBE-8011-6571-0909-000000001200}</Data><Data Name='ProcessId'>8636</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool server list general --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-0509-000000001200}</Data><Data Name='ParentProcessId'>6844</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:28.761835700Z'/><EventRecordID>260</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:28.755</Data><Data Name='ProcessGuid'>{3CBB8FBE-8010-6571-0809-000000001200}</Data><Data Name='ProcessId'>2152</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\SplunkD.EXE" btool web list settings --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-0709-000000001200}</Data><Data Name='ParentProcessId'>9400</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='ParentCommandLine'>btool web list settings --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:28.748155300Z'/><EventRecordID>259</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:28.742</Data><Data Name='ProcessGuid'>{3CBB8FBE-8010-6571-0709-000000001200}</Data><Data Name='ProcessId'>9400</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\btool.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>btool</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>btool.exe</Data><Data Name='CommandLine'>btool web list settings --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C66CF3D2C88617FF1E1272FB763D4388,SHA256=30EBA66BA04B41164AF059B7C8B86ED763AA895B9C8ABD9B5046C338A87B1617,IMPHASH=DD0AFFE2E392CB9B2B68D2769A733208</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-0609-000000001200}</Data><Data Name='ParentProcessId'>1896</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c btool web list settings --no-log</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:28.722604600Z'/><EventRecordID>258</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:28.717</Data><Data Name='ProcessGuid'>{3CBB8FBE-8010-6571-0609-000000001200}</Data><Data Name='ProcessId'>1896</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c btool web list settings --no-log</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-0509-000000001200}</Data><Data Name='ParentProcessId'>6844</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:28.706882400Z'/><EventRecordID>257</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:28.703</Data><Data Name='ProcessGuid'>{3CBB8FBE-8010-6571-0509-000000001200}</Data><Data Name='ProcessId'>6844</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-0409-000000001200}</Data><Data Name='ParentProcessId'>9068</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:28.697267200Z'/><EventRecordID>256</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:28.689</Data><Data Name='ProcessGuid'>{3CBB8FBE-8010-6571-0409-000000001200}</Data><Data Name='ProcessId'>9068</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal_extra_splunkd_service_args</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:19:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:28.644148100Z'/><EventRecordID>255</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:28.639</Data><Data Name='ProcessGuid'>{3CBB8FBE-8010-6571-0209-000000001200}</Data><Data Name='ProcessId'>6036</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _RAW_envvars</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-0009-000000001200}</Data><Data Name='ParentProcessId'>5144</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _RAW_envvars</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:28.596597900Z'/><EventRecordID>254</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:28.589</Data><Data Name='ProcessGuid'>{3CBB8FBE-8010-6571-0009-000000001200}</Data><Data Name='ProcessId'>5144</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _RAW_envvars</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ParentProcessId'>3312</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:19:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:19:28.495145900Z'/><EventRecordID>253</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:19:28.484</Data><Data Name='ProcessGuid'>{3CBB8FBE-8010-6571-FF08-000000001200}</Data><Data Name='ProcessId'>3312</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0205-656E-0A00-000000001200}</Data><Data Name='ParentProcessId'>612</Data><Data Name='ParentImage'>C:\Windows\System32\services.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\services.exe</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:18:53+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:53.015505200Z'/><EventRecordID>252</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:18:51.616</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>www.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:172.217.16.196;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T09:18:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:35.653420100Z'/><EventRecordID>251</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:18:35.642</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FDB-6571-FE08-000000001200}</Data><Data Name='ProcessId'>7788</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:18:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:34.887242900Z'/><EventRecordID>250</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:18:34.877</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FDA-6571-FD08-000000001200}</Data><Data Name='ProcessId'>7716</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:18:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:34.135775900Z'/><EventRecordID>249</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:18:34.126</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FDA-6571-FC08-000000001200}</Data><Data Name='ProcessId'>3964</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:18:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:32.515120500Z'/><EventRecordID>248</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:18:32.502</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FD8-6571-FB08-000000001200}</Data><Data Name='ProcessId'>332</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:18:31+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:31.761580600Z'/><EventRecordID>247</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:18:31.751</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FD7-6571-FA08-000000001200}</Data><Data Name='ProcessId'>5364</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:18:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:30.997314000Z'/><EventRecordID>246</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:18:30.986</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FD6-6571-F908-000000001200}</Data><Data Name='ProcessId'>7680</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:18:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:04.933935800Z'/><EventRecordID>245</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Ver</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:18:04.922</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FBB-6571-F608-000000001200}</Data><Data Name='ProcessId'>1284</Data><Data Name='Image'>C:\Windows\system32\compattelrunner.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\uninstall.exe|bd4762a4deb0ebdc\BinProductVersion</Data><Data Name='Details'>8.5.8.0</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:18:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:04.933772600Z'/><EventRecordID>244</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-CompileTimeClaim</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:18:04.922</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FBB-6571-F608-000000001200}</Data><Data Name='ProcessId'>1284</Data><Data Name='Image'>C:\Windows\system32\compattelrunner.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\uninstall.exe|bd4762a4deb0ebdc\LinkDate</Data><Data Name='Details'>09/25/2021 21:56:47</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:18:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:04.932671300Z'/><EventRecordID>243</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Pub</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:18:04.922</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FBB-6571-F608-000000001200}</Data><Data Name='ProcessId'>1284</Data><Data Name='Image'>C:\Windows\system32\compattelrunner.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\uninstall.exe|bd4762a4deb0ebdc\Publisher</Data><Data Name='Details'>don ho don.h@free.fr</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:18:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:04.932184600Z'/><EventRecordID>242</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Path</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:18:04.922</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FBB-6571-F608-000000001200}</Data><Data Name='ProcessId'>1284</Data><Data Name='Image'>C:\Windows\system32\compattelrunner.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\uninstall.exe|bd4762a4deb0ebdc\LowerCaseLongPath</Data><Data Name='Details'>c:\program files\notepad++\uninstall.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:18:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:04.928654900Z'/><EventRecordID>241</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Pub</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:18:04.922</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FBB-6571-F608-000000001200}</Data><Data Name='ProcessId'>1284</Data><Data Name='Image'>C:\Windows\system32\compattelrunner.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplication\000020f391625db12269c87ae3a56ca674970000ffff\Publisher</Data><Data Name='Details'>Notepad++ Team</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:18:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:04.659627700Z'/><EventRecordID>240</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Ver</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:18:04.656</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FBB-6571-F608-000000001200}</Data><Data Name='ProcessId'>1284</Data><Data Name='Image'>C:\Windows\system32\compattelrunner.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\gup.exe|eaab466dc417ed01\BinProductVersion</Data><Data Name='Details'>(Empty)</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:18:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:04.659427700Z'/><EventRecordID>239</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-CompileTimeClaim</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:18:04.656</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FBB-6571-F608-000000001200}</Data><Data Name='ProcessId'>1284</Data><Data Name='Image'>C:\Windows\system32\compattelrunner.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\gup.exe|eaab466dc417ed01\LinkDate</Data><Data Name='Details'>(Empty)</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:18:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:04.658467200Z'/><EventRecordID>238</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Pub</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:18:04.656</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FBB-6571-F608-000000001200}</Data><Data Name='ProcessId'>1284</Data><Data Name='Image'>C:\Windows\system32\compattelrunner.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\gup.exe|eaab466dc417ed01\Publisher</Data><Data Name='Details'>don ho don.h@free.fr</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:18:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:04.657952500Z'/><EventRecordID>237</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Path</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:18:04.656</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FBB-6571-F608-000000001200}</Data><Data Name='ProcessId'>1284</Data><Data Name='Image'>C:\Windows\system32\compattelrunner.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\gup.exe|eaab466dc417ed01\LowerCaseLongPath</Data><Data Name='Details'>c:\program files\notepad++\updater\gup.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:18:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:04.634512100Z'/><EventRecordID>236</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Ver</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:18:04.625</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FBB-6571-F608-000000001200}</Data><Data Name='ProcessId'>1284</Data><Data Name='Image'>C:\Windows\system32\compattelrunner.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\notepad++.exe|9b63189e96115672\BinProductVersion</Data><Data Name='Details'>(Empty)</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:18:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:04.634348100Z'/><EventRecordID>235</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-CompileTimeClaim</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:18:04.625</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FBB-6571-F608-000000001200}</Data><Data Name='ProcessId'>1284</Data><Data Name='Image'>C:\Windows\system32\compattelrunner.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\notepad++.exe|9b63189e96115672\LinkDate</Data><Data Name='Details'>(Empty)</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:18:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:04.633338800Z'/><EventRecordID>234</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Pub</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:18:04.625</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FBB-6571-F608-000000001200}</Data><Data Name='ProcessId'>1284</Data><Data Name='Image'>C:\Windows\system32\compattelrunner.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\notepad++.exe|9b63189e96115672\Publisher</Data><Data Name='Details'>don ho don.h@free.fr</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:18:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:18:04.632835300Z'/><EventRecordID>233</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Path</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:18:04.625</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FBB-6571-F608-000000001200}</Data><Data Name='ProcessId'>1284</Data><Data Name='Image'>C:\Windows\system32\compattelrunner.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\notepad++.exe|9b63189e96115672\LowerCaseLongPath</Data><Data Name='Details'>c:\program files\notepad++\notepad++.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:36+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:36.227252400Z'/><EventRecordID>232</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:36.214</Data><Data Name='ProcessGuid'>{3CBB8FBE-7FA0-6571-F508-000000001200}</Data><Data Name='ProcessId'>8888</Data><Data Name='Image'>C:\Program Files\Notepad++\notepad++.exe</Data><Data Name='FileVersion'>8.5.8</Data><Data Name='Description'>Notepad++</Data><Data Name='Product'>Notepad++</Data><Data Name='Company'>Don HO don.h@free.fr</Data><Data Name='OriginalFileName'>notepad++.exe</Data><Data Name='CommandLine'>"C:\Program Files\Notepad++\notepad++.exe" "C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\default\inputs.conf" </Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-AFC8-040000000000}</Data><Data Name='LogonId'>0x4c8af</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>MD5=FE341DC1732B4BA290E1C37766DD36DC,SHA256=5AA09176BB1689B87A8E0B98D32E758F5055452C4147EFCBFB91944F1752DC48,IMPHASH=B5856C8A9E980785E72BFA3C2DA2DC24</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0240-656E-5100-000000001200}</Data><Data Name='ParentProcessId'>4984</Data><Data Name='ParentImage'>C:\Windows\explorer.exe</Data><Data Name='ParentCommandLine'>C:\Windows\Explorer.EXE</Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:35.668102800Z'/><EventRecordID>231</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:35.658</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F9F-6571-F408-000000001200}</Data><Data Name='ProcessId'>1608</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:35.219849200Z'/><EventRecordID>230</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:35.219</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1300-000000001200}</Data><Data Name='ProcessId'>480</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>HKU\S-1-5-21-2479543311-1709999589-3761869525-1000\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Program Files\Notepad++\notepad++.exe</Data><Data Name='Details'>Binary Data</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:17:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:34.902211300Z'/><EventRecordID>229</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:34.892</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F9E-6571-F308-000000001200}</Data><Data Name='ProcessId'>6520</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:34.612008500Z'/><EventRecordID>228</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:34.609</Data><Data Name='ProcessGuid'>{3CBB8FBE-0240-656E-5100-000000001200}</Data><Data Name='ProcessId'>4984</Data><Data Name='Image'>C:\Windows\Explorer.EXE</Data><Data Name='TargetObject'>HKU\S-1-5-21-2479543311-1709999589-3761869525-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{B298D29A-A6ED-11DE-BA8C-A68E55D89593} {A08CE4D0-FA25-44AB-B57C-C7B1C323E0B9} 0xFFFF</Data><Data Name='Details'>Binary Data</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:34.140411000Z'/><EventRecordID>227</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:34.130</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F9E-6571-F208-000000001200}</Data><Data Name='ProcessId'>7180</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:17:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:32.497681800Z'/><EventRecordID>226</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:32.486</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F9C-6571-F108-000000001200}</Data><Data Name='ProcessId'>7184</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:31+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:31.728867700Z'/><EventRecordID>225</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:31.719</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F9B-6571-F008-000000001200}</Data><Data Name='ProcessId'>5988</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:30.978725600Z'/><EventRecordID>224</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:30.970</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F9A-6571-EF08-000000001200}</Data><Data Name='ProcessId'>8920</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:17:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:28.859158900Z'/><EventRecordID>223</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:27.876</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F97-6571-EC08-000000001200}</Data><Data Name='ProcessId'>7688</Data><Data Name='QueryName'>notepad-plus-plus.org</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:84.32.84.247;</Data><Data Name='Image'>C:\Program Files\Notepad++\updater\GUP.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>5</EventID><Version>3</Version><Level>4</Level><Task>5</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:28.802737600Z'/><EventRecordID>222</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:28.800</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:28.495196000Z'/><EventRecordID>221</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:28.485</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F98-6571-EE08-000000001200}</Data><Data Name='ProcessId'>4444</Data><Data Name='Image'>C:\Program Files\Notepad++\notepad++.exe</Data><Data Name='FileVersion'>8.5.8</Data><Data Name='Description'>Notepad++</Data><Data Name='Product'>Notepad++</Data><Data Name='Company'>Don HO don.h@free.fr</Data><Data Name='OriginalFileName'>notepad++.exe</Data><Data Name='CommandLine'>"C:\Program Files\Notepad++\notepad++.exe" "C:\Program Files\Notepad++\change.log" </Data><Data Name='CurrentDirectory'>C:\Program Files\Notepad++\contextMenu\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-99C8-040000000000}</Data><Data Name='LogonId'>0x4c899</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=FE341DC1732B4BA290E1C37766DD36DC,SHA256=5AA09176BB1689B87A8E0B98D32E758F5055452C4147EFCBFB91944F1752DC48,IMPHASH=B5856C8A9E980785E72BFA3C2DA2DC24</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ParentProcessId'>6736</Data><Data Name='ParentImage'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='ParentCommandLine'>"C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe" </Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:28.003211400Z'/><EventRecordID>220</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Ver</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:27.953</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\gup.exe|eaab466dc417ed01\BinProductVersion</Data><Data Name='Details'>5.2.6.0</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:28.003140300Z'/><EventRecordID>219</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-CompileTimeClaim</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:27.953</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\gup.exe|eaab466dc417ed01\LinkDate</Data><Data Name='Details'>08/15/2023 12:30:24</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:17:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:28.002430000Z'/><EventRecordID>218</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Pub</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:27.953</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\gup.exe|eaab466dc417ed01\Publisher</Data><Data Name='Details'>don ho don.h@free.fr</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:28.002238000Z'/><EventRecordID>217</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Path</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:27.953</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\gup.exe|eaab466dc417ed01\LowerCaseLongPath</Data><Data Name='Details'>c:\program files\notepad++\updater\gup.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:28.000580300Z'/><EventRecordID>216</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Ver</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:27.953</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\notepad++.exe|9b63189e96115672\BinProductVersion</Data><Data Name='Details'>8.5.8.0</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:28.000514000Z'/><EventRecordID>215</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-CompileTimeClaim</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:27.953</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\notepad++.exe|9b63189e96115672\LinkDate</Data><Data Name='Details'>10/15/2023 19:45:20</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:28+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:28.000099800Z'/><EventRecordID>214</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Pub</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:27.953</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\notepad++.exe|9b63189e96115672\Publisher</Data><Data Name='Details'>don ho don.h@free.fr</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:27+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:27.999882900Z'/><EventRecordID>213</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Path</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:27.953</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\notepad++.exe|9b63189e96115672\LowerCaseLongPath</Data><Data Name='Details'>c:\program files\notepad++\notepad++.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:17:27+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:27.820981500Z'/><EventRecordID>212</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:27.807</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F97-6571-EC08-000000001200}</Data><Data Name='ProcessId'>7688</Data><Data Name='Image'>C:\Program Files\Notepad++\updater\GUP.exe</Data><Data Name='FileVersion'>5.26</Data><Data Name='Description'>WinGup for Notepad++</Data><Data Name='Product'>WinGup for Notepad++</Data><Data Name='Company'>Don HO don.h@free.fr</Data><Data Name='OriginalFileName'>gup.exe</Data><Data Name='CommandLine'>"C:\Program Files\Notepad++\updater\gup.exe" -v8.58 -px64</Data><Data Name='CurrentDirectory'>C:\Program Files\Notepad++\updater\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-AFC8-040000000000}</Data><Data Name='LogonId'>0x4c8af</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>MD5=DBD70A5F2E8210EDA561E53B575CCC46,SHA256=4205D2CC3F3153517B97E98595DF351546D2FA7CCBB503F6E6297CC97A058A70,IMPHASH=2B01D1E6F097308C51E2174A892534F3</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7F97-6571-EB08-000000001200}</Data><Data Name='ParentProcessId'>2548</Data><Data Name='ParentImage'>C:\Program Files\Notepad++\notepad++.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\Notepad++\notepad++.exe" </Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:27+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:27.645248100Z'/><EventRecordID>211</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:27.640</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1300-000000001200}</Data><Data Name='ProcessId'>480</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>HKU\S-1-5-21-2479543311-1709999589-3761869525-1000\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Program Files\Notepad++\notepad++.exe</Data><Data Name='Details'>Binary Data</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:27+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:27.630012500Z'/><EventRecordID>210</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:27.582</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F97-6571-EB08-000000001200}</Data><Data Name='ProcessId'>2548</Data><Data Name='Image'>C:\Program Files\Notepad++\notepad++.exe</Data><Data Name='FileVersion'>8.5.8</Data><Data Name='Description'>Notepad++</Data><Data Name='Product'>Notepad++</Data><Data Name='Company'>Don HO don.h@free.fr</Data><Data Name='OriginalFileName'>notepad++.exe</Data><Data Name='CommandLine'>"C:\Program Files\Notepad++\notepad++.exe" </Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-AFC8-040000000000}</Data><Data Name='LogonId'>0x4c8af</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>MD5=FE341DC1732B4BA290E1C37766DD36DC,SHA256=5AA09176BB1689B87A8E0B98D32E758F5055452C4147EFCBFB91944F1752DC48,IMPHASH=B5856C8A9E980785E72BFA3C2DA2DC24</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7F97-6571-EA08-000000001200}</Data><Data Name='ParentProcessId'>1828</Data><Data Name='ParentImage'>C:\Windows\explorer.exe</Data><Data Name='ParentCommandLine'>C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding</Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:27+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:27.516334300Z'/><EventRecordID>209</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:27.513</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F97-6571-EA08-000000001200}</Data><Data Name='ProcessId'>1828</Data><Data Name='Image'>C:\Windows\explorer.exe</Data><Data Name='FileVersion'>10.0.14393.1532 (rs1_release_d.170711-1840)</Data><Data Name='Description'>Windows Explorer</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>EXPLORER.EXE</Data><Data Name='CommandLine'>C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-AFC8-040000000000}</Data><Data Name='LogonId'>0x4c8af</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>MD5=577119EC77525D3F80FFB03BFACC17D4,SHA256=0327B7630D585AD01F6EC2EB847622645B81DF94A1370B5E466DB9F09F933951,IMPHASH=78778FA5EEA09D1982C509A9E1117980</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0205-656E-0C00-000000001200}</Data><Data Name='ParentProcessId'>788</Data><Data Name='ParentImage'>C:\Windows\System32\svchost.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\svchost.exe -k DcomLaunch</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:17:27+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:27.477756900Z'/><EventRecordID>208</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:27.327</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F97-6571-E908-000000001200}</Data><Data Name='ProcessId'>1612</Data><Data Name='Image'>C:\Windows\explorer.exe</Data><Data Name='FileVersion'>10.0.14393.1532 (rs1_release_d.170711-1840)</Data><Data Name='Description'>Windows Explorer</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>EXPLORER.EXE</Data><Data Name='CommandLine'>"C:\Windows\explorer.exe" "C:\Program Files\Notepad++\notepad++.exe"</Data><Data Name='CurrentDirectory'>C:\Program Files\Notepad++\contextMenu\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-99C8-040000000000}</Data><Data Name='LogonId'>0x4c899</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=577119EC77525D3F80FFB03BFACC17D4,SHA256=0327B7630D585AD01F6EC2EB847622645B81DF94A1370B5E466DB9F09F933951,IMPHASH=78778FA5EEA09D1982C509A9E1117980</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ParentProcessId'>6736</Data><Data Name='ParentImage'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='ParentCommandLine'>"C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe" </Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:25+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:25.522900900Z'/><EventRecordID>207</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Ver</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:25.515</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\regsvr32.exe|8f2966bc37740081\BinProductVersion</Data><Data Name='Details'>10.0.14393.1378</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:25+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:25.522778700Z'/><EventRecordID>206</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-CompileTimeClaim</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:25.515</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\regsvr32.exe|8f2966bc37740081\LinkDate</Data><Data Name='Details'>06/21/2017 06:55:55</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:25+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:25.522160900Z'/><EventRecordID>205</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Pub</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:25.515</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\regsvr32.exe|8f2966bc37740081\Publisher</Data><Data Name='Details'>microsoft corporation</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:25+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:25.521936500Z'/><EventRecordID>204</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Path</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:25.515</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\regsvr32.exe|8f2966bc37740081\LowerCaseLongPath</Data><Data Name='Details'>c:\windows\syswow64\regsvr32.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:17:25+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:25.211724800Z'/><EventRecordID>203</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Ver</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:25.187</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\regsvr32.exe|20eb212352f3412a\BinProductVersion</Data><Data Name='Details'>10.0.14393.0</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:25+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:25.211636000Z'/><EventRecordID>202</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-CompileTimeClaim</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:25.187</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\regsvr32.exe|20eb212352f3412a\LinkDate</Data><Data Name='Details'>07/16/2016 02:25:18</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:25+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:25.211263100Z'/><EventRecordID>201</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Pub</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:25.187</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\regsvr32.exe|20eb212352f3412a\Publisher</Data><Data Name='Details'>microsoft corporation</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:25+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:25.211052000Z'/><EventRecordID>200</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Path</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:25.187</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\regsvr32.exe|20eb212352f3412a\LowerCaseLongPath</Data><Data Name='Details'>c:\windows\system32\regsvr32.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:25+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:25.153471500Z'/><EventRecordID>199</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>EXE</Data><Data Name='UtcTime'>2023-12-07 08:17:25.140</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='TargetFilename'>C:\Program Files\Notepad++\uninstall.exe</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:25.140</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:25+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:25.105174500Z'/><EventRecordID>198</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Pub</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:25.093</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='TargetObject'>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Notepad++\Publisher</Data><Data Name='Details'>Notepad++ Team</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T09:17:25+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:25.104052300Z'/><EventRecordID>197</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:25.093</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='TargetObject'>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\notepad++.exe\(Default)</Data><Data Name='Details'>C:\Program Files\Notepad++\notepad++.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:25+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:25.090746100Z'/><EventRecordID>196</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>T1122</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:25.078</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F95-6571-E808-000000001200}</Data><Data Name='ProcessId'>8388</Data><Data Name='Image'>C:\Windows\system32\regsvr32.exe</Data><Data Name='TargetObject'>HKCR\CLSID\{B298D29A-A6ED-11DE-BA8C-A68E55D89593}\InProcServer32\(Default)</Data><Data Name='Details'>C:\Program Files\Notepad++\contextMenu\NppShell.dll</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:25+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:25.043382900Z'/><EventRecordID>195</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:25.024</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F95-6571-E808-000000001200}</Data><Data Name='ProcessId'>8388</Data><Data Name='Image'>C:\Windows\System32\regsvr32.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Microsoft(C) Register Server</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>REGSVR32.EXE</Data><Data Name='CommandLine'> /s "C:\Program Files\Notepad++\contextMenu\NppShell.dll"</Data><Data Name='CurrentDirectory'>C:\Program Files\Notepad++\contextMenu\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-99C8-040000000000}</Data><Data Name='LogonId'>0x4c899</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=8CF9086BE38A15E905924B4A45D814D9,SHA256=00A1CF85C6AB96DF38A4023F0CEE4DF60F62280768FC9C06A235E6D2D644169D,IMPHASH=1C8D7F52BBDAEF92EB0104CB6362D5D0</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7F94-6571-E708-000000001200}</Data><Data Name='ParentProcessId'>3248</Data><Data Name='ParentImage'>C:\Windows\SysWOW64\regsvr32.exe</Data><Data Name='ParentCommandLine'>regsvr32 /s "C:\Program Files\Notepad++\contextMenu\NppShell.dll"</Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:24+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:24.908437500Z'/><EventRecordID>194</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:24.883</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F94-6571-E708-000000001200}</Data><Data Name='ProcessId'>3248</Data><Data Name='Image'>C:\Windows\SysWOW64\regsvr32.exe</Data><Data Name='FileVersion'>10.0.14393.1378 (rs1_release.170620-2008)</Data><Data Name='Description'>Microsoft(C) Register Server</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>REGSVR32.EXE</Data><Data Name='CommandLine'>regsvr32 /s "C:\Program Files\Notepad++\contextMenu\NppShell.dll"</Data><Data Name='CurrentDirectory'>C:\Program Files\Notepad++\contextMenu\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-99C8-040000000000}</Data><Data Name='LogonId'>0x4c899</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=56CF190F4143DC68800C4125D6001B07,SHA256=F72ED4D11C9971A9B7CE0A5681EE35968A6B4CCDC2F2B3A9F3E81418605FA467,IMPHASH=D053774A49BA83FF54C68888CB687C6C</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ParentProcessId'>6736</Data><Data Name='ParentImage'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='ParentCommandLine'>"C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe" </Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T09:17:24+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:24.839156200Z'/><EventRecordID>193</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>DLL</Data><Data Name='UtcTime'>2023-12-07 08:17:24.827</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='TargetFilename'>C:\Program Files\Notepad++\contextMenu\NppShell.dll</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:24.827</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:24+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:24.610976100Z'/><EventRecordID>192</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>T1023</Data><Data Name='UtcTime'>2023-12-07 08:17:24.593</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='TargetFilename'>C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Notepad++.lnk</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:24.593</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:24+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:24.365647600Z'/><EventRecordID>191</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>DLL</Data><Data Name='UtcTime'>2023-12-07 08:17:24.358</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\AppData\Local\Temp\nsIEE3F.tmp\UserInfo.dll</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:24.358</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:22+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:22.891606900Z'/><EventRecordID>190</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>EXE</Data><Data Name='UtcTime'>2023-12-07 08:17:22.874</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='TargetFilename'>C:\Program Files\Notepad++\notepad++.exe</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:22.874</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:22+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:22.759497900Z'/><EventRecordID>189</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>DLL</Data><Data Name='UtcTime'>2023-12-07 08:17:22.753</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='TargetFilename'>C:\Program Files\Notepad++\plugins\Config\nppPluginList.dll</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:22.753</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:22+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:22.483421800Z'/><EventRecordID>188</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>DLL</Data><Data Name='UtcTime'>2023-12-07 08:17:22.476</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='TargetFilename'>C:\Program Files\Notepad++\updater\libcurl.dll</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:22.476</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T09:17:22+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:22.407465300Z'/><EventRecordID>187</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>EXE</Data><Data Name='UtcTime'>2023-12-07 08:17:22.405</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='TargetFilename'>C:\Program Files\Notepad++\updater\GUP.exe</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:22.405</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:22+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:22.379093300Z'/><EventRecordID>186</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>DLL</Data><Data Name='UtcTime'>2023-12-07 08:17:22.359</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='TargetFilename'>C:\Program Files\Notepad++\plugins\NppConverter\NppConverter.dll</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:22.359</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:22+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:22.342202200Z'/><EventRecordID>185</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>DLL</Data><Data Name='UtcTime'>2023-12-07 08:17:22.328</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='TargetFilename'>C:\Program Files\Notepad++\plugins\mimeTools\mimeTools.dll</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:22.328</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:22+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:22.308971900Z'/><EventRecordID>184</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>DLL</Data><Data Name='UtcTime'>2023-12-07 08:17:22.308</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='TargetFilename'>C:\Program Files\Notepad++\plugins\NppExport\NppExport.dll</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:22.308</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:20.585987600Z'/><EventRecordID>183</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>DLL</Data><Data Name='UtcTime'>2023-12-07 08:17:20.577</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\AppData\Local\Temp\nsIEE3F.tmp\nsDialogs.dll</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:20.577</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:15.813564200Z'/><EventRecordID>182</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>DLL</Data><Data Name='UtcTime'>2023-12-07 08:17:15.811</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\AppData\Local\Temp\nsIEE3F.tmp\InstallOptions.dll</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:15.811</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T09:17:11+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:11.704527700Z'/><EventRecordID>181</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>DLL</Data><Data Name='UtcTime'>2023-12-07 08:17:11.702</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\AppData\Local\Temp\nsIEE3F.tmp\LangDLL.dll</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:11.702</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:11+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:11.674310800Z'/><EventRecordID>180</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>DLL</Data><Data Name='UtcTime'>2023-12-07 08:17:11.671</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\AppData\Local\Temp\nsIEE3F.tmp\System.dll</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:11.671</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:11+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:11.385366200Z'/><EventRecordID>179</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:11.380</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F87-6571-E608-000000001200}</Data><Data Name='ProcessId'>6736</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='FileVersion'>8.5.8.0</Data><Data Name='Description'>Notepad++ : a free (GNU) source code editor</Data><Data Name='Product'>Notepad++</Data><Data Name='Company'>Don HO don.h@free.fr</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe" </Data><Data Name='CurrentDirectory'>C:\Users\vagrant\Downloads\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-99C8-040000000000}</Data><Data Name='LogonId'>0x4c899</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=BB24BFE6B03ED859D38D7AC653617417,SHA256=D50A46E7FFB799D501D60D9D3689D0B3FBE668D16AA421D67216269F83974220,IMPHASH=61259B55B8912888E90F516CA08DC514</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7AF8-6571-CD07-000000001200}</Data><Data Name='ParentProcessId'>6000</Data><Data Name='ParentImage'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\Google\Chrome\Application\chrome.exe" </Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:09+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:09.361805300Z'/><EventRecordID>178</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Ver</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:09.358</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\npp.8.5.8.instal|c3e35d6071b5cc98\BinProductVersion</Data><Data Name='Details'>8.5.8.0</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:09+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:09.360383100Z'/><EventRecordID>177</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-CompileTimeClaim</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:09.358</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\npp.8.5.8.instal|c3e35d6071b5cc98\LinkDate</Data><Data Name='Details'>09/25/2021 21:56:47</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:17:09+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:09.353704900Z'/><EventRecordID>176</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Pub</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:09.342</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\npp.8.5.8.instal|c3e35d6071b5cc98\Publisher</Data><Data Name='Details'>don ho don.h@free.fr</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:09+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:09.353464900Z'/><EventRecordID>175</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Path</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:09.342</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\npp.8.5.8.install|c3e35d6071b5cc98\LowerCaseLongPath</Data><Data Name='Details'>c:\users\vagrant\downloads\npp.8.5.8.installer.x64.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:17:09+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>5</EventID><Version>3</Version><Level>4</Level><Task>5</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:09.273203500Z'/><EventRecordID>174</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:09.264</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F85-6571-E208-000000001200}</Data><Data Name='ProcessId'>4928</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:09+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:09.237875400Z'/><EventRecordID>173</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:09.196</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F85-6571-E208-000000001200}</Data><Data Name='ProcessId'>4928</Data><Data Name='Image'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='FileVersion'>8.5.8.0</Data><Data Name='Description'>Notepad++ : a free (GNU) source code editor</Data><Data Name='Product'>Notepad++</Data><Data Name='Company'>Don HO don.h@free.fr</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe" </Data><Data Name='CurrentDirectory'>C:\Users\vagrant\Downloads\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-AFC8-040000000000}</Data><Data Name='LogonId'>0x4c8af</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>MD5=BB24BFE6B03ED859D38D7AC653617417,SHA256=D50A46E7FFB799D501D60D9D3689D0B3FBE668D16AA421D67216269F83974220,IMPHASH=61259B55B8912888E90F516CA08DC514</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7AF8-6571-CD07-000000001200}</Data><Data Name='ParentProcessId'>6000</Data><Data Name='ParentImage'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\Google\Chrome\Application\chrome.exe" </Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:09+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>15</EventID><Version>2</Version><Level>4</Level><Task>15</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:09.184663900Z'/><EventRecordID>172</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:09.171</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-CD07-000000001200}</Data><Data Name='ProcessId'>6000</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe:Zone.Identifier</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:02.513</Data><Data Name='Hash'>MD5=431D239BCE86CA2D93FDD4D38E2C0A45,SHA256=76652508B09BAE5EF7B6FCD049006D0285BE99CAA2008DD746A4BCD66F90AA1E,IMPHASH=00000000000000000000000000000000</Data><Data Name='Contents'>[ZoneTransfer] AppZoneId=4 </Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T09:17:09+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>15</EventID><Version>2</Version><Level>4</Level><Task>15</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:09.184484800Z'/><EventRecordID>171</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:09.155</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-CD07-000000001200}</Data><Data Name='ProcessId'>6000</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:02.513</Data><Data Name='Hash'>MD5=BB24BFE6B03ED859D38D7AC653617417,SHA256=D50A46E7FFB799D501D60D9D3689D0B3FBE668D16AA421D67216269F83974220,IMPHASH=61259B55B8912888E90F516CA08DC514</Data><Data Name='Contents'>-</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:09+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>15</EventID><Version>2</Version><Level>4</Level><Task>15</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:09.162379000Z'/><EventRecordID>170</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:09.155</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-CD07-000000001200}</Data><Data Name='ProcessId'>6000</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe:Zone.Identifier</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:02.513</Data><Data Name='Hash'>Unknown</Data><Data Name='Contents'>-</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:09+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:09.162333300Z'/><EventRecordID>169</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>Downloads</Data><Data Name='UtcTime'>2023-12-07 08:17:09.155</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-CD07-000000001200}</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe:Zone.Identifier</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:02.513</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:09+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>15</EventID><Version>2</Version><Level>4</Level><Task>15</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:09.162264800Z'/><EventRecordID>168</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:09.139</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-CD07-000000001200}</Data><Data Name='ProcessId'>6000</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:02.513</Data><Data Name='Hash'>MD5=BB24BFE6B03ED859D38D7AC653617417,SHA256=D50A46E7FFB799D501D60D9D3689D0B3FBE668D16AA421D67216269F83974220,IMPHASH=61259B55B8912888E90F516CA08DC514</Data><Data Name='Contents'>-</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:08+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:08.891426900Z'/><EventRecordID>167</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:08.889</Data><Data Name='ProcessGuid'>{3CBB8FBE-7ED9-6571-B908-000000001200}</Data><Data Name='ProcessId'>564</Data><Data Name='Image'>C:\Windows\System32\smartscreen.exe</Data><Data Name='TargetObject'>HKU\S-1-5-21-2479543311-1709999589-3761869525-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable</Data><Data Name='Details'>DWORD (0x00000000)</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T09:17:06+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>15</EventID><Version>2</Version><Level>4</Level><Task>15</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:06.277374600Z'/><EventRecordID>166</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:06.264</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F81-6571-DF08-000000001200}</Data><Data Name='ProcessId'>7600</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe:Zone.Identifier</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:02.513</Data><Data Name='Hash'>MD5=FBCCF14D504B7B2DBCB5A5BDA75BD93B,SHA256=EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913,IMPHASH=00000000000000000000000000000000</Data><Data Name='Contents'>[ZoneTransfer] ZoneId=3 </Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:06+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:06.277270600Z'/><EventRecordID>165</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>Downloads</Data><Data Name='UtcTime'>2023-12-07 08:17:06.264</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F81-6571-DF08-000000001200}</Data><Data Name='ProcessId'>7600</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe:Zone.Identifier</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:02.513</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:06+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>15</EventID><Version>2</Version><Level>4</Level><Task>15</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:06.277161200Z'/><EventRecordID>164</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:06.251</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F81-6571-DF08-000000001200}</Data><Data Name='ProcessId'>7600</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\Downloads\npp.8.5.8.Installer.x64.exe</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:02.513</Data><Data Name='Hash'>MD5=BB24BFE6B03ED859D38D7AC653617417,SHA256=D50A46E7FFB799D501D60D9D3689D0B3FBE668D16AA421D67216269F83974220,IMPHASH=61259B55B8912888E90F516CA08DC514</Data><Data Name='Contents'>-</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:06+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:06.129491500Z'/><EventRecordID>163</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:17:06.100</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F81-6571-DF08-000000001200}</Data><Data Name='ProcessId'>7600</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='TargetObject'>HKU\S-1-5-21-2479543311-1709999589-3761869525-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable</Data><Data Name='Details'>DWORD (0x00000000)</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:04.218072800Z'/><EventRecordID>162</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:03.790</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>sb-ssl.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 5 sb-ssl.l.google.com;::ffff:142.250.185.174;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:04+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:04.218013200Z'/><EventRecordID>161</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:03.770</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>wpad</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>-</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T09:17:03+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:03.219577200Z'/><EventRecordID>160</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:02.303</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>objects.githubusercontent.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:185.199.108.133;::ffff:185.199.109.133;::ffff:185.199.110.133;::ffff:185.199.111.133;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:03+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:03.219558100Z'/><EventRecordID>159</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:02.205</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>github.githubassets.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:185.199.109.154;::ffff:185.199.111.154;::ffff:185.199.110.154;::ffff:185.199.108.154;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:03+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:03.219539000Z'/><EventRecordID>158</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:17:02.049</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>github.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:140.82.121.3;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:17:02+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:17:02.540239600Z'/><EventRecordID>157</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>Downloads</Data><Data Name='UtcTime'>2023-12-07 08:17:02.513</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-CD07-000000001200}</Data><Data Name='ProcessId'>6000</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='TargetFilename'>C:\Users\vagrant\Downloads\a7f10b30-57f2-4994-adc1-7386496f5a27.tmp</Data><Data Name='CreationUtcTime'>2023-12-07 08:17:02.513</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:16:37+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:16:37.131032700Z'/><EventRecordID>156</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:16:36.216</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>m.servedby-buysellads.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 5 d2yy6p64xsttp1.cloudfront.net;::ffff:18.161.111.31;::ffff:18.161.111.113;::ffff:18.161.111.36;::ffff:18.161.111.102;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T09:16:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:16:35.640894400Z'/><EventRecordID>155</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:16:35.630</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F63-6571-D708-000000001200}</Data><Data Name='ProcessId'>1928</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:16:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:16:34.884046900Z'/><EventRecordID>154</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:16:34.872</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F62-6571-D608-000000001200}</Data><Data Name='ProcessId'>5492</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:16:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:16:34.125258600Z'/><EventRecordID>153</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:16:34.114</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F62-6571-D508-000000001200}</Data><Data Name='ProcessId'>9272</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:16:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:16:33.816621500Z'/><EventRecordID>152</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:16:33.105</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>www.google.fr</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:142.250.186.99;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T09:16:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:16:33.816602400Z'/><EventRecordID>151</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:16:33.097</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>region1.analytics.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:216.239.34.36;::ffff:216.239.32.36;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:16:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:16:33.816521900Z'/><EventRecordID>150</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:16:32.884</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>cdn.carbonads.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 5 d2w5yq7htjp2h0.cloudfront.net;::ffff:65.9.66.66;::ffff:65.9.66.19;::ffff:65.9.66.111;::ffff:65.9.66.129;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:16:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:16:32.508110700Z'/><EventRecordID>149</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:16:32.497</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F60-6571-D408-000000001200}</Data><Data Name='ProcessId'>5828</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C8287681895 99BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:16:31+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:16:31.733802000Z'/><EventRecordID>148</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:16:31.723</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F5F-6571-D308-000000001200}</Data><Data Name='ProcessId'>6960</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:16:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:16:30.967831300Z'/><EventRecordID>147</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:16:30.957</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F5E-6571-D208-000000001200}</Data><Data Name='ProcessId'>3892</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:16:24+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:16:24.893702400Z'/><EventRecordID>146</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:16:23.424</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>www.youtube.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 5 youtube-ui.l.google.com;::ffff:142.250.185.110;::ffff:142.250.185.142;::ffff:142.250.186.174;::ffff:172.217.16.206;::ffff:142.250.184.206;::ffff:172.217.16.142;::ffff:142.250.185.78;::ffff:172.217.18.110;::ffff:142.250.185.174;::ffff:172.217.23.110;::ffff:142.250.185.238;::ffff:216.58.206.46;::ffff:142.250.181.238;::ffff:142.250.186.110;::ffff:142.250.185.206;::ffff:142.250.186.78;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:16:23+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:16:23.887439300Z'/><EventRecordID>145</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:16:22.683</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>tunnel.googlezip.net</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:216.239.34.157;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:16:23+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:16:23.887421500Z'/><EventRecordID>144</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:16:22.590</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>notepad-plus-plus.org</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:154.62.105.251;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:16:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:16:20.862170900Z'/><EventRecordID>143</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:16:19.887</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>collector.github.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>type: 5 glb-db52c2cf8be544.github.com;::ffff:140.82.114.22;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T09:16:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:16:20.862155400Z'/><EventRecordID>142</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:16:19.874</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>api.github.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:140.82.121.6;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:15:57+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:15:57.015093600Z'/><EventRecordID>141</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:15:55.153</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1100-000000001200}</Data><Data Name='ProcessId'>348</Data><Data Name='QueryName'>poor.ntp.org</Data><Data Name='QueryStatus'>9501</Data><Data Name='QueryResults'>-</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\LOCAL SERVICE</Data></EventData></Event>
2023-12-07T09:15:48+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:15:48.104959402Z'/><EventRecordID>140</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:15:46.202</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1500-000000001200}</Data><Data Name='ProcessId'>1096</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\NETWORK SERVICE</Data></EventData></Event>
2023-12-07T09:15:38+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:15:38.777056600Z'/><EventRecordID>139</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:15:36.731</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1200-000000001200}</Data><Data Name='ProcessId'>392</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\LOCAL SERVICE</Data></EventData></Event>
2023-12-07T09:15:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:15:35.633039602Z'/><EventRecordID>138</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:15:35.622</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F27-6571-C608-000000001200}</Data><Data Name='ProcessId'>9308</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:15:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:15:34.880520200Z'/><EventRecordID>137</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:15:34.872</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F26-6571-C508-000000001200}</Data><Data Name='ProcessId'>9080</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:15:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:15:34.115683900Z'/><EventRecordID>136</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:15:34.106</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F26-6571-C408-000000001200}</Data><Data Name='ProcessId'>10132</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:15:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:15:32.490665400Z'/><EventRecordID>135</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:15:32.482</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F24-6571-C308-000000001200}</Data><Data Name='ProcessId'>6532</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:15:31+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:15:31.693961000Z'/><EventRecordID>134</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:15:31.685</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F23-6571-C208-000000001200}</Data><Data Name='ProcessId'>7044</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:15:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:15:30.944689600Z'/><EventRecordID>133</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:15:30.935</Data><Data Name='ProcessGuid'>{3CBB8FBE-7F22-6571-C108-000000001200}</Data><Data Name='ProcessId'>7972</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:14:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:14:35.637799200Z'/><EventRecordID>132</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:14:35.627</Data><Data Name='ProcessGuid'>{3CBB8FBE-7EEB-6571-C008-000000001200}</Data><Data Name='ProcessId'>2264</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:14:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:14:34.886719800Z'/><EventRecordID>131</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:14:34.877</Data><Data Name='ProcessGuid'>{3CBB8FBE-7EEA-6571-BF08-000000001200}</Data><Data Name='ProcessId'>1260</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:14:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:14:34.107503800Z'/><EventRecordID>130</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:14:34.096</Data><Data Name='ProcessGuid'>{3CBB8FBE-7EEA-6571-BE08-000000001200}</Data><Data Name='ProcessId'>8544</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:14:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:14:32.481020900Z'/><EventRecordID>129</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:14:32.471</Data><Data Name='ProcessGuid'>{3CBB8FBE-7EE8-6571-BD08-000000001200}</Data><Data Name='ProcessId'>8368</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:14:31+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:14:31.684777500Z'/><EventRecordID>128</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:14:31.674</Data><Data Name='ProcessGuid'>{3CBB8FBE-7EE7-6571-BC08-000000001200}</Data><Data Name='ProcessId'>6072</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:14:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:14:30.932693200Z'/><EventRecordID>127</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:14:30.923</Data><Data Name='ProcessGuid'>{3CBB8FBE-7EE6-6571-BB08-000000001200}</Data><Data Name='ProcessId'>6892</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:14:17+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:14:17.898258000Z'/><EventRecordID>126</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:14:17.892</Data><Data Name='ProcessGuid'>{3CBB8FBE-7ED9-6571-BA08-000000001200}</Data><Data Name='ProcessId'>9032</Data><Data Name='Image'>C:\Windows\System32\notepad.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Notepad</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>NOTEPAD.EXE</Data><Data Name='CommandLine'>"C:\Windows\system32\NOTEPAD.EXE" C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\default\inputs.conf</Data><Data Name='CurrentDirectory'>C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\default\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-AFC8-040000000000}</Data><Data Name='LogonId'>0x4c8af</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>MD5=3B508CAE5DEBCBA928B5BC355517E2E6,SHA256=DA0ACEE8F60A460CFB5249E262D3D53211EBC4C777579E99C8202B761541110A,IMPHASH=968239BE2020F1C0DAFFDCDBD49E9C82</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0240-656E-5100-000000001200}</Data><Data Name='ParentProcessId'>4984</Data><Data Name='ParentImage'>C:\Windows\explorer.exe</Data><Data Name='ParentCommandLine'>C:\Windows\Explorer.EXE</Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T09:14:17+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:14:17.832123700Z'/><EventRecordID>125</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:14:17.811</Data><Data Name='ProcessGuid'>{3CBB8FBE-7ED9-6571-B908-000000001200}</Data><Data Name='ProcessId'>564</Data><Data Name='Image'>C:\Windows\System32\smartscreen.exe</Data><Data Name='FileVersion'>10.0.14393.1715 (rs1_release_inmarket.170906-1810)</Data><Data Name='Description'>SmartScreen</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>smartscreen.exe</Data><Data Name='CommandLine'>C:\Windows\System32\smartscreen.exe -Embedding</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-AFC8-040000000000}</Data><Data Name='LogonId'>0x4c8af</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>MD5=4A619778CC5B53F92CA6750F840455B7,SHA256=01114EE31AA9B24B6BDD67C3E0AD89C5C758D8AD416A7851E4F24937A57C5223,IMPHASH=A88BD4C4BF193E3DD40E8408EB103B65</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0205-656E-0C00-000000001200}</Data><Data Name='ParentProcessId'>788</Data><Data Name='ParentImage'>C:\Windows\System32\svchost.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\svchost.exe -k DcomLaunch</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:13:50+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:13:50.517824100Z'/><EventRecordID>124</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:13:49.519</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2900-000000001200}</Data><Data Name='ProcessId'>2692</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\dfsrs.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:13:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:13:35.638746800Z'/><EventRecordID>123</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:13:35.627</Data><Data Name='ProcessGuid'>{3CBB8FBE-7EAF-6571-B808-000000001200}</Data><Data Name='ProcessId'>6180</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:13:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:13:34.869318000Z'/><EventRecordID>122</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:13:34.861</Data><Data Name='ProcessGuid'>{3CBB8FBE-7EAE-6571-B708-000000001200}</Data><Data Name='ProcessId'>6028</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:13:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:13:34.105738900Z'/><EventRecordID>121</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:13:34.095</Data><Data Name='ProcessGuid'>{3CBB8FBE-7EAE-6571-B608-000000001200}</Data><Data Name='ProcessId'>7396</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:13:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:13:32.464185400Z'/><EventRecordID>120</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:13:32.454</Data><Data Name='ProcessGuid'>{3CBB8FBE-7EAC-6571-B508-000000001200}</Data><Data Name='ProcessId'>2836</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:13:31+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:13:31.683186800Z'/><EventRecordID>119</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:13:31.673</Data><Data Name='ProcessGuid'>{3CBB8FBE-7EAB-6571-B408-000000001200}</Data><Data Name='ProcessId'>1712</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:13:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:13:30.934799800Z'/><EventRecordID>118</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:13:30.924</Data><Data Name='ProcessGuid'>{3CBB8FBE-7EAA-6571-B308-000000001200}</Data><Data Name='ProcessId'>7984</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:12:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:12:35.640697400Z'/><EventRecordID>117</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:12:35.631</Data><Data Name='ProcessGuid'>{3CBB8FBE-7E73-6571-B208-000000001200}</Data><Data Name='ProcessId'>2336</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:12:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:12:34.858364200Z'/><EventRecordID>116</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:12:34.849</Data><Data Name='ProcessGuid'>{3CBB8FBE-7E72-6571-B108-000000001200}</Data><Data Name='ProcessId'>6344</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:12:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:12:34.097382100Z'/><EventRecordID>115</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:12:34.087</Data><Data Name='ProcessGuid'>{3CBB8FBE-7E72-6571-B008-000000001200}</Data><Data Name='ProcessId'>2204</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:12:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:12:32.707486300Z'/><EventRecordID>114</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:12:30.693</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1200-000000001200}</Data><Data Name='ProcessId'>392</Data><Data Name='QueryName'>MEEREEN</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\LOCAL SERVICE</Data></EventData></Event>
2023-12-07T09:12:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:12:32.453268500Z'/><EventRecordID>113</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:12:32.442</Data><Data Name='ProcessGuid'>{3CBB8FBE-7E70-6571-AF08-000000001200}</Data><Data Name='ProcessId'>276</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:12:31+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:12:31.686190400Z'/><EventRecordID>112</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:12:31.676</Data><Data Name='ProcessGuid'>{3CBB8FBE-7E6F-6571-AE08-000000001200}</Data><Data Name='ProcessId'>7344</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:12:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:12:30.905401900Z'/><EventRecordID>111</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:12:30.895</Data><Data Name='ProcessGuid'>{3CBB8FBE-7E6E-6571-AD08-000000001200}</Data><Data Name='ProcessId'>10024</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:12:19+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:12:19.733929900Z'/><EventRecordID>110</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:12:17.931</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1100-000000001200}</Data><Data Name='ProcessId'>348</Data><Data Name='QueryName'>wpad</Data><Data Name='QueryStatus'>9003</Data><Data Name='QueryResults'>-</Data><Data Name='Image'>C:\Windows\system32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\LOCAL SERVICE</Data></EventData></Event>
2023-12-07T09:11:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:11:35.617730800Z'/><EventRecordID>109</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:11:35.608</Data><Data Name='ProcessGuid'>{3CBB8FBE-7E37-6571-AC08-000000001200}</Data><Data Name='ProcessId'>10036</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:11:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:11:34.852078400Z'/><EventRecordID>108</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:11:34.842</Data><Data Name='ProcessGuid'>{3CBB8FBE-7E36-6571-AB08-000000001200}</Data><Data Name='ProcessId'>1916</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:11:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:11:34.090453600Z'/><EventRecordID>107</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:11:34.080</Data><Data Name='ProcessGuid'>{3CBB8FBE-7E36-6571-AA08-000000001200}</Data><Data Name='ProcessId'>9248</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:11:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:11:32.430938700Z'/><EventRecordID>106</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:11:32.421</Data><Data Name='ProcessGuid'>{3CBB8FBE-7E34-6571-A908-000000001200}</Data><Data Name='ProcessId'>4204</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:11:31+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:11:31.665565900Z'/><EventRecordID>105</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:11:31.656</Data><Data Name='ProcessGuid'>{3CBB8FBE-7E33-6571-A808-000000001200}</Data><Data Name='ProcessId'>7352</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:11:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:11:30.900670900Z'/><EventRecordID>104</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:11:30.891</Data><Data Name='ProcessGuid'>{3CBB8FBE-7E32-6571-A708-000000001200}</Data><Data Name='ProcessId'>8572</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:10:47+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:47.947130500Z'/><EventRecordID>103</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:46.060</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1200-000000001200}</Data><Data Name='ProcessId'>392</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\system32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\LOCAL SERVICE</Data></EventData></Event>
2023-12-07T09:10:46+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:46.935940300Z'/><EventRecordID>102</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:45.949</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1700-000000001200}</Data><Data Name='ProcessId'>1340</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:10:38+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:38.386194600Z'/><EventRecordID>101</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:36.632</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DFC-6571-A508-000000001200}</Data><Data Name='ProcessId'>1960</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:10:37+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:37.402410700Z'/><EventRecordID>100</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:37.278</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DFD-6571-A608-000000001200}</Data><Data Name='ProcessId'>4596</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-winprintmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Windows Print Monitor </Data><Data Name='Product'>splunk Application </Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-winprintmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-winprintmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=FDEB6BA573575665D847C8C88DFA6B28,SHA256=00FC8040D205B3290D204EB5E6AEAF5E21CF6F5EDB081555CDF81AD61F306218,IMPHASH=355E487ADBCE53AA00CC9620C5813D5A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:10:36+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:36.491107600Z'/><EventRecordID>99</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:36.357</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DFC-6571-A508-000000001200}</Data><Data Name='ProcessId'>1960</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Monitor windows event logs</Data><Data Name='Product'>splunk Application </Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-winevtlog.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AE95292862972429C2FBD9541C739C2B,SHA256=C1899D942B83A761EADA6303334A9E6946A7206A59E678F0039D3AB527785522,IMPHASH=EDE9B13E7663B8E763DD4604CD8C3BF7</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:10:35+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:35.614718300Z'/><EventRecordID>98</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:35.606</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DFB-6571-A408-000000001200}</Data><Data Name='ProcessId'>6228</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:10:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:34.850646000Z'/><EventRecordID>97</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:34.841</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DFA-6571-A308-000000001200}</Data><Data Name='ProcessId'>332</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:10:34+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:34.086931400Z'/><EventRecordID>96</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:34.075</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DFA-6571-A208-000000001200}</Data><Data Name='ProcessId'>4860</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:10:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:33.332427000Z'/><EventRecordID>95</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:33.204</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DF9-6571-A108-000000001200}</Data><Data Name='ProcessId'>10172</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-perfmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Performance monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-perfmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-perfmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=37F610EA3267B4C636A52CC17C72F5E9,SHA256=154252976F3CDC663C1999E5BF6958E4A9717874E2117061A0E40F2F1D97BE27,IMPHASH=35AE00EA6705AD0DB2C706FD3FAF93B6</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:10:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:32.419241400Z'/><EventRecordID>94</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:32.405</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DF8-6571-A008-000000001200}</Data><Data Name='ProcessId'>6644</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:10:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:32.090217700Z'/><EventRecordID>93</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:31.088</Data><Data Name='ProcessGuid'>{3CBB8FBE-7D54-6571-5B08-000000001200}</Data><Data Name='ProcessId'>10156</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\mmc.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:10:32+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:32.090193700Z'/><EventRecordID>92</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:31.084</Data><Data Name='ProcessGuid'>{3CBB8FBE-7D54-6571-5B08-000000001200}</Data><Data Name='ProcessId'>10156</Data><Data Name='QueryName'>MEEREEN</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\mmc.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T09:10:31+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:31.647488600Z'/><EventRecordID>91</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:31.638</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DF7-6571-9F08-000000001200}</Data><Data Name='ProcessId'>1260</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:10:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:30.883550000Z'/><EventRecordID>90</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:30.873</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DF6-6571-9E08-000000001200}</Data><Data Name='ProcessId'>10208</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:10:30+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:30.141630100Z'/><EventRecordID>89</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:29.986</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DF5-6571-9D08-000000001200}</Data><Data Name='ProcessId'>5212</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-wmi.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Remote Performance monitor using WMI</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-wmi.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-wmi.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=7A440F2DF244985160C5B54CDBBA547D,SHA256=7E1DBA295076C76618106FD18E882B190BF0542AD2981200D01074B021BF76CF,IMPHASH=7C7770CDB275E49574E79FDF395C7C60</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:10:27+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:27.889374000Z'/><EventRecordID>88</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:27.876</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DF3-6571-9C08-000000001200}</Data><Data Name='ProcessId'>7252</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\powershell2.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:10:27+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:27.748483300Z'/><EventRecordID>87</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:27.736</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DF3-6571-9B08-000000001200}</Data><Data Name='ProcessId'>8404</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\powershell.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:10:27+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:27.595247200Z'/><EventRecordID>86</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:27.583</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DF3-6571-9A08-000000001200}</Data><Data Name='ProcessId'>3876</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\perfmon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:10:27+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:27.449876500Z'/><EventRecordID>85</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:27.439</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DF3-6571-9908-000000001200}</Data><Data Name='ProcessId'>3232</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\admon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:10:27+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:27.317376400Z'/><EventRecordID>84</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:27.306</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DF3-6571-9808-000000001200}</Data><Data Name='ProcessId'>9032</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinRegMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:10:27+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:27.186642100Z'/><EventRecordID>83</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:27.175</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DF3-6571-9708-000000001200}</Data><Data Name='ProcessId'>8744</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinPrintMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:10:27+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:27.048938100Z'/><EventRecordID>82</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:27.038</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DF3-6571-9608-000000001200}</Data><Data Name='ProcessId'>796</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinNetMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:10:26+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:26.916416200Z'/><EventRecordID>81</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:26.905</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DF2-6571-9508-000000001200}</Data><Data Name='ProcessId'>7312</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinHostMon.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:10:26+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:26.767489500Z'/><EventRecordID>80</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:26.756</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DF2-6571-9408-000000001200}</Data><Data Name='ProcessId'>6892</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\WinEventLog.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:10:26+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:26.634213900Z'/><EventRecordID>79</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:26.621</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DF2-6571-9308-000000001200}</Data><Data Name='ProcessId'>9284</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\system\bin\MonitorNoHandle.cmd" --scheme"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:10:25+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:25.894566000Z'/><EventRecordID>78</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:25.888</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DF1-6571-9208-000000001200}</Data><Data Name='ProcessId'>7532</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunk Application</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal check-xml-files --answer-yes --no-prompt </Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=BD8C7370FA8F766EBA8A9D20C0B81200,SHA256=01D95E37437562DCC6178D44ADC8F88E1415D71C250A474BBA4D8257AD0560EB,IMPHASH=517EF37A9934AD1B9661680CF576924B</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DF1-6571-9108-000000001200}</Data><Data Name='ParentProcessId'>1308</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal check-xml-files --answer-yes --no-prompt 2>&1</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:10:25+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:25.883240700Z'/><EventRecordID>77</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:25.873</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DF1-6571-9108-000000001200}</Data><Data Name='ProcessId'>1308</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _internal check-xml-files --answer-yes --no-prompt 2>&1</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:10:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:20.182978100Z'/><EventRecordID>41</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:20.174</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DEC-6571-6B08-000000001200}</Data><Data Name='ProcessId'>7740</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>C:\Windows\system32\cmd.exe /c "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" _RAW_envvars</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ParentProcessId'>9936</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:10:20+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:20.077121700Z'/><EventRecordID>40</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:19.704</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DEB-6571-6A08-000000001200}</Data><Data Name='ProcessId'>9936</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>splunkd service</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunkd.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=AEA10BEEA3FFC51CFA1D79A44977E2B5,SHA256=220BF961FEAF43F83E2131578CDB4FA0556FFA3EA3A3F9D6FB97829D5424E161,IMPHASH=07F6211F1A67D0777ED04995B456E6FD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0205-656E-0A00-000000001200}</Data><Data Name='ParentProcessId'>612</Data><Data Name='ParentImage'>C:\Windows\System32\services.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\services.exe</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:10:12+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:12.703778000Z'/><EventRecordID>39</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:12.692</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DE4-6571-6908-000000001200}</Data><Data Name='ProcessId'>8072</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7966-6571-6807-000000001200}</Data><Data Name='ParentProcessId'>4036</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:10:12+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>8</EventID><Version>2</Version><Level>4</Level><Task>8</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:10:12.691278300Z'/><EventRecordID>38</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:10:12.672</Data><Data Name='SourceProcessGuid'>{3CBB8FBE-0205-656E-0500-000000001200}</Data><Data Name='SourceProcessId'>400</Data><Data Name='SourceImage'><unknown process></Data><Data Name='TargetProcessGuid'>{3CBB8FBE-7975-6571-A307-000000001200}</Data><Data Name='TargetProcessId'>6140</Data><Data Name='TargetImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-winevtlog.exe</Data><Data Name='NewThreadId'>7204</Data><Data Name='StartAddress'>0x00007FFA6BED7B80</Data><Data Name='StartModule'>C:\Windows\System32\KERNELBASE.dll</Data><Data Name='StartFunction'>CtrlRoutine</Data><Data Name='SourceUser'>NT AUTHORITY\SYSTEM</Data><Data Name='TargetUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:09:52+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:09:52.066919000Z'/><EventRecordID>37</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:09:51.058</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>www.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:142.250.186.100;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:09:22+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:09:22.978032300Z'/><EventRecordID>36</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:09:20.963</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2300-000000001200}</Data><Data Name='ProcessId'>2520</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:09:17+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:09:17.303715000Z'/><EventRecordID>35</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:09:17.291</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DAD-6571-6808-000000001200}</Data><Data Name='ProcessId'>9000</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7966-6571-6807-000000001200}</Data><Data Name='ParentProcessId'>4036</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:09:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:09:16.539117800Z'/><EventRecordID>34</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:09:16.526</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DAC-6571-6708-000000001200}</Data><Data Name='ProcessId'>7976</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7966-6571-6807-000000001200}</Data><Data Name='ParentProcessId'>4036</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:09:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:09:15.769450800Z'/><EventRecordID>33</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:09:15.761</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DAB-6571-6608-000000001200}</Data><Data Name='ProcessId'>1584</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7966-6571-6807-000000001200}</Data><Data Name='ParentProcessId'>4036</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:09:14+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:09:14.318248000Z'/><EventRecordID>32</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:09:14.307</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DAA-6571-6508-000000001200}</Data><Data Name='ProcessId'>2364</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7966-6571-6807-000000001200}</Data><Data Name='ParentProcessId'>4036</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:09:13+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:09:13.568540000Z'/><EventRecordID>31</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:09:13.558</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DA9-6571-6408-000000001200}</Data><Data Name='ProcessId'>6620</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7966-6571-6807-000000001200}</Data><Data Name='ParentProcessId'>4036</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:09:12+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:09:12.692637900Z'/><EventRecordID>30</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:09:12.683</Data><Data Name='ProcessGuid'>{3CBB8FBE-7DA8-6571-6308-000000001200}</Data><Data Name='ProcessId'>8936</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7966-6571-6807-000000001200}</Data><Data Name='ParentProcessId'>4036</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:09:10+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:09:10.167204300Z'/><EventRecordID>29</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:09:08.355</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1500-000000001200}</Data><Data Name='ProcessId'>1096</Data><Data Name='QueryName'>openwec.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:10.202.0.140;</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\NETWORK SERVICE</Data></EventData></Event>
2023-12-07T09:08:52+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:08:52.981774100Z'/><EventRecordID>28</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:08:51.001</Data><Data Name='ProcessGuid'>{3CBB8FBE-7AF8-6571-D007-000000001200}</Data><Data Name='ProcessId'>992</Data><Data Name='QueryName'>www.google.com</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:142.250.186.68;</Data><Data Name='Image'>C:\Program Files\Google\Chrome\Application\chrome.exe</Data><Data Name='User'>ESSOS\vagrant</Data></EventData></Event>

Time	Event
2023-12-07T09:08:49+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:08:49.966756300Z'/><EventRecordID>27</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:08:48.992</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2900-000000001200}</Data><Data Name='ProcessId'>2692</Data><Data Name='QueryName'>MEEREEN</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\dfsrs.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:08:49+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:08:49.966720300Z'/><EventRecordID>26</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:08:48.966</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2900-000000001200}</Data><Data Name='ProcessId'>2692</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\system32\DFSRs.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:08:22+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:08:22.277949700Z'/><EventRecordID>25</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:08:20.950</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2300-000000001200}</Data><Data Name='ProcessId'>2520</Data><Data Name='QueryName'>meereen.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>fe80::71ea:2b1:64c2:cbc0;fe80::5dfe:4bb0:25:eb7f;fe80::b96d:3f7b:76bd:70ac;::ffff:10.202.0.166;::ffff:192.168.56.12;::ffff:10.0.2.15;</Data><Data Name='Image'>C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:08:17+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:08:17.589712500Z'/><EventRecordID>24</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:08:17.451</Data><Data Name='ProcessGuid'>{3CBB8FBE-7D71-6571-6208-000000001200}</Data><Data Name='ProcessId'>780</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F,SHA256=394540275287F579C4A86AAD5EFAE89330D76DF2AB1E667C6D335792607EDC96,IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7966-6571-6807-000000001200}</Data><Data Name='ParentProcessId'>4036</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:08:16+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:08:16.647499700Z'/><EventRecordID>23</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:08:16.637</Data><Data Name='ProcessGuid'>{3CBB8FBE-7D70-6571-6108-000000001200}</Data><Data Name='ProcessId'>6664</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe" --ps2</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7966-6571-6807-000000001200}</Data><Data Name='ParentProcessId'>4036</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:08:15+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:08:15.888614400Z'/><EventRecordID>22</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:08:15.761</Data><Data Name='ProcessGuid'>{3CBB8FBE-7D6F-6571-6008-000000001200}</Data><Data Name='ProcessId'>5212</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe</Data><Data Name='FileVersion'>-</Data><Data Name='Description'>-</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Data Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=637CE6449C9A92C9D39A56B39DBB6BAE,SHA256=8F6D579B2CDAA13DE76C6956A556AEFE9E4B2AD2389CD3E4C84E4AC156C849A3,IMPHASH=03EECCD22564A6E804E38A5D73FF88DD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7966-6571-6807-000000001200}</Data><Data Name='ParentProcessId'>4036</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:08:14+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:08:14.565682300Z'/><EventRecordID>21</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:08:14.434</Data><Data Name='ProcessGuid'>{3CBB8FBE-7D6E-6571-5F08-000000001200}</Data><Data Name='ProcessId'>7160</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Network monitor</Data><Data Name='Product'>Splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-netmon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=C49DC73C13C5E138E7E141203AE5754A,SHA256=0C828768189599BABC34B77FF9E919EBC2E6400DD35F8641979843C98A5F6FA4,IMPHASH=00F79FCF768C2C4EC8D958D1A56A52CD</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7966-6571-6807-000000001200}</Data><Data Name='ParentProcessId'>4036</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:08:13+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:08:13.667454800Z'/><EventRecordID>20</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:08:13.543</Data><Data Name='ProcessGuid'>{3CBB8FBE-7D6D-6571-5E08-000000001200}</Data><Data Name='ProcessId'>4492</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Active Directory monitor</Data><Data Name='Product'>splunk Application</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-admon.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=6ABB2397D4E93A51F11AEED0318F215C,SHA256=33C9E76382F302D92B319DB8B65F4ADC483720077A468EE7E3FCBAABD2DBF805,IMPHASH=5C0C66433BBEBC709F578BED5B6C0F53</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7966-6571-6807-000000001200}</Data><Data Name='ParentProcessId'>4036</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:08:12+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:08:12.799306000Z'/><EventRecordID>19</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:08:12.668</Data><Data Name='ProcessGuid'>{3CBB8FBE-7D6C-6571-5D08-000000001200}</Data><Data Name='ProcessId'>6676</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe</Data><Data Name='FileVersion'>10.0.10011.16384</Data><Data Name='Description'>SplunkMonNoHandle Control Program</Data><Data Name='Product'>Windows (R) Win 7 DDK driver</Data><Data Name='Company'>Windows (R) Win 7 DDK provider</Data><Data Name='OriginalFileName'>SplunkMonNoHandle.exe</Data><Data Name='CommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe"</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=19EBC6858DD8F01C44D4E1F90CC8E5AC,SHA256=C7A5FB5E012C8A44FF9BFDB6CD4F027FB6BA2F5A00D9D74BC44BBED0AF9ABE84,IMPHASH=B1B81F575C3B0B1443DE136CA53EFECE</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-7966-6571-6807-000000001200}</Data><Data Name='ParentProcessId'>4036</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:07:49+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:07:49.008080300Z'/><EventRecordID>18</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:07:48.073</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>meereen</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>10.202.0.166;192.168.56.12;10.0.2.15;</Data><Data Name='Image'>C:\Windows\System32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:07:49+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:07:49.008056300Z'/><EventRecordID>17</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:07:48.035</Data><Data Name='ProcessGuid'>{3CBB8FBE-0205-656E-0B00-000000001200}</Data><Data Name='ProcessId'>620</Data><Data Name='QueryName'>meereen</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>10.202.0.166;192.168.56.12;10.0.2.15;</Data><Data Name='Image'>C:\Windows\system32\lsass.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:07:48+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:07:48.104246100Z'/><EventRecordID>16</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:07:48.098</Data><Data Name='ProcessGuid'>{3CBB8FBE-7D54-6571-5B08-000000001200}</Data><Data Name='ProcessId'>10156</Data><Data Name='Image'>C:\Windows\System32\mmc.exe</Data><Data Name='FileVersion'>10.0.14393.953 (rs1_release_inmarket.170303-1614)</Data><Data Name='Description'>Microsoft Management Console</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>mmc.exe</Data><Data Name='CommandLine'>"C:\Windows\system32\mmc.exe" "C:\Windows\system32\eventvwr.msc" /s</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-99C8-040000000000}</Data><Data Name='LogonId'>0x4c899</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=C75224D3741563FBD526BB7813488A4A,SHA256=6A9BDBFCF4E2DB18F62C55A46C0C94B765165DA150DA6E8E0A87C740C71887BB,IMPHASH=ED5A55DAB5A02F29D6EE7E0015F91A9F</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0240-656E-5100-000000001200}</Data><Data Name='ParentProcessId'>4984</Data><Data Name='ParentImage'>C:\Windows\explorer.exe</Data><Data Name='ParentCommandLine'>C:\Windows\Explorer.EXE</Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:07:47+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:07:47.900595400Z'/><EventRecordID>15</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:07:47.886</Data><Data Name='ProcessGuid'>{3CBB8FBE-7D53-6571-5708-000000001200}</Data><Data Name='ProcessId'>9608</Data><Data Name='Image'>C:\Windows\System32\mmc.exe</Data><Data Name='FileVersion'>10.0.14393.953 (rs1_release_inmarket.170303-1614)</Data><Data Name='Description'>Microsoft Management Console</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>mmc.exe</Data><Data Name='CommandLine'>"C:\Windows\system32\mmc.exe" "C:\Windows\system32\eventvwr.msc" /s</Data><Data Name='CurrentDirectory'>C:\Windows\system32\</Data><Data Name='User'>ESSOS\vagrant</Data><Data Name='LogonGuid'>{3CBB8FBE-023E-656E-AFC8-040000000000}</Data><Data Name='LogonId'>0x4c8af</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>MD5=C75224D3741563FBD526BB7813488A4A,SHA256=6A9BDBFCF4E2DB18F62C55A46C0C94B765165DA150DA6E8E0A87C740C71887BB,IMPHASH=ED5A55DAB5A02F29D6EE7E0015F91A9F</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-0240-656E-5100-000000001200}</Data><Data Name='ParentProcessId'>4984</Data><Data Name='ParentImage'>C:\Windows\explorer.exe</Data><Data Name='ParentCommandLine'>C:\Windows\Explorer.EXE</Data><Data Name='ParentUser'>ESSOS\vagrant</Data></EventData></Event>
2023-12-07T09:07:43+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:07:43.364269300Z'/><EventRecordID>14</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='4044'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 08:07:41.363</Data><Data Name='ProcessGuid'>{3CBB8FBE-0206-656E-1500-000000001200}</Data><Data Name='ProcessId'>1096</Data><Data Name='QueryName'>openwec.essos.local</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>::ffff:10.202.0.140;</Data><Data Name='Image'>C:\Windows\system32\svchost.exe</Data><Data Name='User'>NT AUTHORITY\NETWORK SERVICE</Data></EventData></Event>
2023-12-07T09:07:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:07:33.045532700Z'/><EventRecordID>13</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Ver</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:07:33.031</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\sysmon64.exe|7dec52f2d2929003\BinProductVersion</Data><Data Name='Details'>15.11.0.0</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>

Time	Event
2023-12-07T09:07:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:07:33.045450500Z'/><EventRecordID>12</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-CompileTimeClaim</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:07:33.031</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\sysmon64.exe|7dec52f2d2929003\LinkDate</Data><Data Name='Details'>11/13/2023 15:50:59</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:07:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:07:33.044947400Z'/><EventRecordID>11</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Pub</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:07:33.031</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\sysmon64.exe|7dec52f2d2929003\Publisher</Data><Data Name='Details'>sysinternals - www.sysinternals.com</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>
2023-12-07T09:07:33+0100	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-12-07T08:07:33.043083000Z'/><EventRecordID>10</EventRecordID><Correlation/><Execution ProcessID='6380' ThreadID='7100'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>InvDB-Path</Data><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2023-12-07 08:07:33.031</Data><Data Name='ProcessGuid'>{3CBB8FBE-0215-656E-2800-000000001200}</Data><Data Name='ProcessId'>2668</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetObject'>\REGISTRY\A\{3d6eaaca-19df-6f24-a466-4da4ce39373e}\Root\InventoryApplicationFile\sysmon64.exe|7dec52f2d2929003\LowerCaseLongPath</Data><Data Name='Details'>c:\users\vagrant\downloads\sysmon\sysmon64.exe</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data></EventData></Event>