Logs:  
  
1. Nov 18, 2024 @ 16:47:09.960

input.type:log agent.ip:192.168.1.8 agent.name:windows agent.id:001 manager.name:wazuh.manager data.win.eventdata.data:2124-10-25T11:17:10Z, RulesEngine data.win.system.eventID:16384 data.win.system.eventSourceName:Software Protection Platform Service data.win.system.keywords:0x80000000000000 data.win.system.providerGuid:{E23B33B0-C8C9-472C-A5F9-F2BDFEA0F156} data.win.system.level:4 data.win.system.channel:Application data.win.system.opcode:0 data.win.system.message:"Successfully scheduled Software Protection service for re-start at 2124-10-25T11:17:10Z. Reason: RulesEngine." data.win.system.version:0 data.win.system.systemTime:2024-11-18T11:17:10.2002730Z data.win.system.eventRecordID:4517 data.win.system.threadID:0 data.win.system.computer:CANUM20241025 data.win.system.task:0 data.win.system.processID:6228 data.win.system.severityValue:INFORMATION data.win.system.providerName:Microsoft-Windows-Security-SPP rule.firedtimes:5 rule.mail:false rule.level:3 rule.description:Software protection service scheduled successfully. rule.groups:windows, windows\_application rule.id:60642 location:EventChannel decoder.name:windows\_eventchannel id:1731928629.10932224 timestamp:Nov 18, 2024 @ 16:47:09.960 \_index:wazuh-alerts-4.x-2024.11.18

2. Nov 18, 2024 @ 16:46:35.396

input.type:log agent.ip:192.168.1.8 agent.name:windows agent.id:001 manager.name:wazuh.manager data.win.eventdata.subjectLogonId:0x3e7 data.win.eventdata.subjectDomainName:WORKGROUP data.win.eventdata.targetLinkedLogonId:0x0 data.win.eventdata.impersonationLevel:%%1833 data.win.eventdata.authenticationPackageName:Negotiate data.win.eventdata.targetLogonId:0x3e7 data.win.eventdata.logonProcessName:Advapi data.win.eventdata.logonGuid:{00000000-0000-0000-0000-000000000000}  
  
3. Nov 18, 2024 @ 16:41:11.368

input.type:log agent.ip:192.168.1.8 agent.name:windows agent.id:001 manager.name:wazuh.manager data.win.eventdata.param3:demand start data.win.eventdata.param4:BITS data.win.eventdata.param1:Background Intelligent Transfer Service data.win.eventdata.param2:auto start data.win.system.eventID:7040 data.win.system.eventSourceName:Service Control Manager data.win.system.keywords:0x8080000000000000 data.win.system.providerGuid:{555908d1-a6d7-4695-8e1e-26931d2012f4} data.win.system.level:4 data.win.system.channel:System data.win.system.opcode:0 data.win.system.message:"The start type of the Background Intelligent Transfer Service service was changed from auto start to demand start." data.win.system.version:0 data.win.system.systemTime:2024-11-18T11:11:10.5944319Z  
  
4. Nov 18, 2024 @ 16:33:11.521

input.type:log agent.ip:192.168.1.8 agent.name:windows agent.id:001 manager.name:wazuh.manager data.win.eventdata.subjectLogonId:0x3e7 data.win.eventdata.subjectDomainName:WORKGROUP data.win.eventdata.targetLinkedLogonId:0x0 data.win.eventdata.impersonationLevel:%%1833 data.win.eventdata.authenticationPackageName:Negotiate data.win.eventdata.targetLogonId:0x3e7 data.win.eventdata.logonProcessName:Advapi data.win.eventdata.logonGuid:{00000000-0000-0000-0000-000000000000} data.win.eventdata.targetUserName:SYSTEM data.win.eventdata.keyLength:0 data.win.eventdata.elevatedToken:%%1842 data.win.eventdata.subjectUserSid:S-1-5-18 data.win.eventdata.processId:0x434 data.win.eventdata.processName:C:\\Windows  
  
  
5. Nov 18, 2024 @ 16:31:05.863

input.type:log agent.ip:192.168.1.8 agent.name:windows agent.id:001 manager.name:wazuh.manager data.win.eventdata.param3:auto start data.win.eventdata.param4:BITS data.win.eventdata.param1:Background Intelligent Transfer Service data.win.eventdata.param2:demand start data.win.system.eventID:7040 data.win.system.eventSourceName:Service Control Manager data.win.system.keywords:0x8080000000000000 data.win.system.providerGuid:{555908d1-a6d7-4695-8e1e-26931d2012f4} data.win.system.level:4 data.win.system.channel:System data.win.system.opcode:0 data.win.system.message:"The start type of the Background Intelligent Transfer Service service was changed from demand start to auto start." data.win.system.version:0 data.win.system.systemTime:2024-11-18T11:01:05.4284814Z  
  
6. Nov 18, 2024 @ 17:24:48.391

input.type:log agent.ip:192.168.1.7 agent.name:Raman-windows agent.id:003 manager.name:wazuh.manager data.win.eventdata.subjectLogonId:0x3e7 data.win.eventdata.subjectDomainName:WORKGROUP data.win.eventdata.targetLinkedLogonId:0x0 data.win.eventdata.impersonationLevel:%%1833 data.win.eventdata.authenticationPackageName:Negotiate data.win.eventdata.targetLogonId:0x3e7 data.win.eventdata.logonProcessName:Advapi data.win.eventdata.logonGuid:{00000000-0000-0000-0000-000000000000} data.win.eventdata.targetUserName:SYSTEM data.win.eventdata.keyLength:0 data.win.eventdata.elevatedToken:%%1842 data.win.eventdata.subjectUserSid:S-1-5-18 data.win.eventdata.processId:0x36c data.win.eventdata.processName:C:\\Windows\\System32\\services.exe data.win.eventdata.targetDomainName:NT AUTHORITY data.win.eventdata.targetUserSid:S-1-5-18 data.win.eventdata.virtualAccount:%%1843 data.win.eventdata.logonType:5 data.win.eventdata.subjectUserName:DESKTOP-SCHL4P4$ data.win.system.eventID:4624 data.win.system.keywords:0x8020000000000000 data.win.system.providerGuid:{54849625-5478-4994-a5ba-3e3b0328c30d} data.win.system.level:0 data.win.system.channel:Security data.win.system.opcode:0 data.win.system.message:"An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: DESKTOP-SCHL4P4$ Account Domain: WORKGROUP Logon ID: 0x3E7 Logon Information: Logon Type: 5 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x36c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested." data.win.system.version:2 data.win.system.systemTime:2024-11-18T11:54:46.4056559Z data.win.system.eventRecordID:449968 data.win.system.threadID:13004 data.win.system.computer:DESKTOP-SCHL4P4 data.win.system.task:12544 data.win.system.processID:884 data.win.system.severityValue:AUDIT\_SUCCESS data.win.system.providerName:Microsoft-Windows-Security-Auditing rule.mail:false rule.level:3 rule.pci\_dss:10.2.5 rule.hipaa:164.312.b rule.tsc:CC6.8, CC7.2, CC7.3 rule.description:Windows Logon Success rule.groups:windows, windows\_security, authentication\_success rule.nist\_800\_53:AU.14, AC.7 rule.gdpr:IV\_32.2 rule.firedtimes:82 rule.mitre.technique:Valid Accounts rule.mitre.id:T1078 rule.mitre.tactic:Defense Evasion, Persistence, Privilege Escalation, Initial Access rule.id:60106 rule.gpg13:7.1, 7.2 location:EventChannel decoder.name:windows\_eventchannel id:1731930888.11446462 timestamp:Nov 18, 2024 @ 17:24:48.391 \_index:wazuh-alerts-4.x-2024.11.18

7. Nov 18, 2024 @ 17:24:46.430

input.type:log agent.ip:192.168.1.7 agent.name:Raman-windows agent.id:003 manager.name:wazuh.manager data.win.eventdata.subjectLogonId:0x3e7 data.win.eventdata.subjectDomainName:WORKGROUP data.win.eventdata.targetLinkedLogonId:0x0 data.win.eventdata.impersonationLevel:%%1833 data.win.eventdata.authenticationPackageName:Negotiate data.win.eventdata.targetLogonId:0x3e7 data.win.eventdata.logonProcessName:Advapi data.win.eventdata.logonGuid:{00000000-0000-0000-0000-000000000000} data.win.eventdata.targetUserName:SYSTEM data.win.eventdata.keyLength:0 data.win.eventdata.elevatedToken:%%1842 data.win.eventdata.subjectUserSid:S-1-5-18 data.win.eventdata.processId:0x36c data.win.eventdata.processName:C:\\Windows\\System32\\services.exe data.win.eventdata.targetDomainName:NT AUTHORITY data.win.eventdata.targetUserSid:S-1-5-18 data.win.eventdata.virtualAccount:%%1843 data.win.eventdata.logonType:5 data.win.eventdata.subjectUserName:DESKTOP-SCHL4P4$ data.win.system.eventID:4624 data.win.system.keywords:0x8020000000000000 data.win.system.providerGuid:{54849625-5478-4994-a5ba-3e3b0328c30d} data.win.system.level:0 data.win.system.channel:Security data.win.system.opcode:0 data.win.system.message:"An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: DESKTOP-SCHL4P4$ Account Domain: WORKGROUP Logon ID: 0x3E7 Logon Information: Logon Type: 5 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x36c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested." data.win.system.version:2 data.win.system.systemTime:2024-11-18T11:54:44.4442450Z data.win.system.eventRecordID:449966 data.win.system.threadID:13004 data.win.system.computer:DESKTOP-SCHL4P4 data.win.system.task:12544 data.win.system.processID:884 data.win.system.severityValue:AUDIT\_SUCCESS data.win.system.providerName:Microsoft-Windows-Security-Auditing rule.mail:false rule.level:3 rule.pci\_dss:10.2.5 rule.hipaa:164.312.b rule.tsc:CC6.8, CC7.2, CC7.3 rule.description:Windows Logon Success rule.groups:windows, windows\_security, authentication\_success rule.nist\_800\_53:AU.14, AC.7 rule.gdpr:IV\_32.2 rule.firedtimes:81 rule.mitre.technique:Valid Accounts rule.mitre.id:T1078 rule.mitre.tactic:Defense Evasion, Persistence, Privilege Escalation, Initial Access rule.id:60106 rule.gpg13:7.1, 7.2 location:EventChannel decoder.name:windows\_eventchannel id:1731930886.11439136 timestamp:Nov 18, 2024 @ 17:24:46.430 \_index:wazuh-alerts-4.x-2024.11.18

8. Nov 18, 2024 @ 17:20:08.181

input.type:log agent.ip:192.168.1.7 agent.name:Raman-windows agent.id:003 manager.name:wazuh.manager data.win.eventdata.binary:2D20436F64653A2020434F525356434330303030303737342D2043616C6C3A2020434F525356434330303030303735362D205049443A202030303031313733322D205449443A202030303031323434382D20434D443A2020433A5C57696E646F77735C73797374656D33325C76737376632E6578652020202D20557365723A204E616D653A204E5420415554484F524954595C53595354454D2C205349443A532D312D352D313820 data.win.system.eventID:8224 data.win.system.keywords:0x80000000000000 data.win.system.level:4 data.win.system.channel:Application  
  
  
9. Nov 18, 2024 @ 17:28:03.313

input.type:log agent.ip:192.168.1.7 agent.name:Raman-windows agent.id:003 manager.name:wazuh.manager data.win.eventdata.subjectLogonId:0x3e7 data.win.eventdata.subjectDomainName:WORKGROUP data.win.eventdata.targetLinkedLogonId:0x0 data.win.eventdata.impersonationLevel:%%1833 data.win.eventdata.authenticationPackageName:Negotiate data.win.eventdata.targetLogonId:0x3e7 data.win.eventdata.logonProcessName:Advapi data.win.eventdata.logonGuid:{00000000-0000-0000-0000-000000000000} data.win.eventdata.targetUserName:SYSTEM data.win.eventdata.keyLength:0 data.win.eventdata.elevatedToken:%%1842 data.win.eventdata.subjectUserSid:S-1-5-18 data.win.eventdata.processId:0x36c data.win.eventdata.processName:C:\\Windows\\System32\\services.exe data.win.eventdata.targetDomainName:NT AUTHORITY data.win.eventdata.targetUserSid:S-1-5-18 data.win.eventdata.virtualAccount:%%1843 data.win.eventdata.logonType:5 data.win.eventdata.subjectUserName:DESKTOP-SCHL4P4$ data.win.system.eventID:4624 data.win.system.keywords:0x8020000000000000 data.win.system.providerGuid:{54849625-5478-4994-a5ba-3e3b0328c30d} data.win.system.level:0 data.win.system.channel:Security data.win.system.opcode:0 data.win.system.message:"An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: DESKTOP-SCHL4P4$ Account Domain: WORKGROUP Logon ID: 0x3E7 Logon Information: Logon Type: 5 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x36c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested." data.win.system.version:2 data.win.system.systemTime:2024-11-18T11:58:01.2999711Z data.win.system.eventRecordID:449999 data.win.system.threadID:18396 data.win.system.computer:DESKTOP-SCHL4P4 data.win.system.task:12544 data.win.system.processID:884 data.win.system.severityValue:AUDIT\_SUCCESS data.win.system.providerName:Microsoft-Windows-Security-Auditing rule.mail:false rule.level:3 rule.pci\_dss:10.2.5 rule.hipaa:164.312.b rule.tsc:CC6.8, CC7.2, CC7.3 rule.description:Windows Logon Success rule.groups:windows, windows\_security, authentication\_success rule.nist\_800\_53:AU.14, AC.7 rule.gdpr:IV\_32.2 rule.firedtimes:88 rule.mitre.technique:Valid Accounts rule.mitre.id:T1078 rule.mitre.tactic:Defense Evasion, Persistence, Privilege Escalation, Initial Access rule.id:60106 rule.gpg13:7.1, 7.2 location:EventChannel decoder.name:windows\_eventchannel id:1731931083.11490576 timestamp:Nov 18, 2024 @ 17:28:03.313 \_index:wazuh-alerts-4.x-2024.11.18

10. Nov 18, 2024 @ 17:26:46.247

input.type:log agent.ip:192.168.1.7 agent.name:Raman-windows agent.id:003 manager.name:wazuh.manager data.win.eventdata.subjectLogonId:0x3e7 data.win.eventdata.subjectDomainName:WORKGROUP data.win.eventdata.targetLinkedLogonId:0x0 data.win.eventdata.impersonationLevel:%%1833 data.win.eventdata.authenticationPackageName:Negotiate data.win.eventdata.targetLogonId:0x3e7 data.win.eventdata.logonProcessName:Advapi data.win.eventdata.logonGuid:{00000000-0000-0000-0000-000000000000} data.win.eventdata.targetUserName:SYSTEM data.win.eventdata.keyLength:0 data.win.eventdata.elevatedToken:%%1842 data.win.eventdata.subjectUserSid:S-1-5-18 data.win.eventdata.processId:0x36c data.win.eventdata.processName:C:\\Windows\\System32\\services.exe data.win.eventdata.targetDomainName:NT AUTHORITY data.win.eventdata.targetUserSid:S-1-5-18 data.win.eventdata.virtualAccount:%%1843 data.win.eventdata.logonType:5 data.win.eventdata.subjectUserName:DESKTOP-SCHL4P4$ data.win.system.eventID:4624 data.win.system.keywords:0x8020000000000000 data.win.system.providerGuid:{54849625-5478-4994-a5ba-3e3b0328c30d} data.win.system.level:0 data.win.system.channel:Security data.win.system.opcode:0 data.win.system.message:"An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: DESKTOP-SCHL4P4$ Account Domain: WORKGROUP Logon ID: 0x3E7 Logon Information: Logon Type: 5 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x36c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested." data.win.system.version:2 data.win.system.systemTime:2024-11-18T11:56:44.2619455Z data.win.system.eventRecordID:449988 data.win.system.threadID:18396 data.win.system.computer:DESKTOP-SCHL4P4 data.win.system.task:12544 data.win.system.processID:884 data.win.system.severityValue:AUDIT\_SUCCESS data.win.system.providerName:Microsoft-Windows-Security-Auditing rule.mail:false rule.level:3 rule.pci\_dss:10.2.5 rule.hipaa:164.312.b rule.tsc:CC6.8, CC7.2, CC7.3 rule.description:Windows Logon Success rule.groups:windows, windows\_security, authentication\_success rule.nist\_800\_53:AU.14, AC.7 rule.gdpr:IV\_32.2 rule.firedtimes:87 rule.mitre.technique:Valid Accounts rule.mitre.id:T1078 rule.mitre.tactic:Defense Evasion, Persistence, Privilege Escalation, Initial Access rule.id:60106 rule.gpg13:7.1, 7.2 location:EventChannel decoder.name:windows\_eventchannel id:1731931006.11483250 timestamp:Nov 18, 2024 @ 17:26:46.247 \_index:wazuh-alerts-4.x-2024.11.18

11. Nov 18, 2024 @ 17:26:24.288

input.type:log agent.ip:192.168.1.7 agent.name:Raman-windows agent.id:003 manager.name:wazuh.manager data.win.eventdata.subjectLogonId:0x3e7 data.win.eventdata.subjectDomainName:WORKGROUP data.win.eventdata.targetLinkedLogonId:0x0 data.win.eventdata.impersonationLevel:%%1833 data.win.eventdata.authenticationPackageName:Negotiate data.win.eventdata.targetLogonId:0x3e7 data.win.eventdata.logonProcessName:Advapi data.win.eventdata.logonGuid:{00000000-0000-0000-0000-000000000000}  
  
  
12. Nov 18, 2024 @ 17:28:36.491

input.type:log agent.ip:192.168.1.7 agent.name:Raman-windows agent.id:003 manager.name:wazuh.manager data.win.eventdata.data:2124-10-25T11:58:35Z, RulesEngine data.win.system.eventID:16384 data.win.system.eventSourceName:Software Protection Platform Service data.win.system.keywords:0x80000000000000 data.win.system.providerGuid:{E23B33B0-C8C9-472C-A5F9-F2BDFEA0F156} data.win.system.level:4 data.win.system.channel:Application data.win.system.opcode:0 data.win.system.message:"Successfully scheduled Software Protection service for re-start at 2124-10-25T11:58:35Z. Reason: RulesEngine." data.win.system.version:0

13. Nov 18, 2024 @ 17:34:21.944

input.type:log agent.ip:192.168.1.7 agent.name:Raman-windows agent.id:003 manager.name:wazuh.manager data.win.eventdata.subjectLogonId:0x3e7 data.win.eventdata.subjectDomainName:WORKGROUP data.win.eventdata.targetLinkedLogonId:0x0 data.win.eventdata.impersonationLevel:%%1833 data.win.eventdata.authenticationPackageName:Negotiate data.win.eventdata.targetLogonId:0x3e7 data.win.eventdata.logonProcessName:Advapi data.win.eventdata.logonGuid:{00000000-0000-0000-0000-000000000000}

14. Nov 18, 2024 @ 17:42:34.163

input.type:log agent.ip:192.168.1.2 agent.name:sanskriti agent.id:002 manager.name:wazuh.manager data.win.eventdata.subjectLogonId:0x3e7 data.win.eventdata.subjectDomainName:WORKGROUP data.win.eventdata.targetLinkedLogonId:0x0 data.win.eventdata.impersonationLevel:%%1833 data.win.eventdata.authenticationPackageName:Negotiate data.win.eventdata.targetLogonId:0x3e7 data.win.eventdata.logonProcessName:Advapi data.win.eventdata.logonGuid:{00000000-0000-0000-0000-000000000000} data.win.eventdata.targetUserName:SYSTEM data.win.eventdata.keyLength:0 data.win.eventdata.elevatedToken:%%1842 data.win.eventdata.subjectUserSid:S-1-5-18 data.win.eventdata.processId:0x1ec data.win.eventdata.processName:C:\\Windows\\System32\\services.exe data.win.eventdata.targetDomainName:NT AUTHORITY

15. Nov 18, 2024 @ 17:41:09.400

input.type:log agent.ip:192.168.1.8 agent.name:windows agent.id:001 manager.name:wazuh.manager data.win.eventdata.param3:demand start data.win.eventdata.param4:BITS data.win.eventdata.param1:Background Intelligent Transfer Service data.win.eventdata.param2:auto start data.win.system.eventID:7040 data.win.system.eventSourceName:Service Control Manager data.win.system.keywords:0x8080000000000000 data.win.system.providerGuid:{555908d1-a6d7-4695-8e1e-26931d2012f4} data.win.system.level:4 data.win.system.channel:System data.win.system.opcode:0 data.win.system.message:"The start type of the Background Intelligent Transfer Service service was changed from auto start to demand start." data.win.system.version:0 data.win.system.systemTime:2024-11-18T12:11:08.7382048Z data.win.system.eventRecordID:5877 data.win.system.threadID:6456 data.win.system.computer:CANUM20241025 data.win.system.task:0 data.win.system.processID:1076 data.win.system.severityValue:INFORMATION data.win.system.providerName:Service Control Manager rule.firedtimes:4 rule.mail:false rule.level:3 rule.pci\_dss:10.6  
  
  
16. Nov 18, 2024 @ 17:50:34.809

input.type:log agent.ip:192.168.1.7 agent.name:Raman-windows agent.id:003 manager.name:wazuh.manager data.win.eventdata.data:2124-10-25T12:20:33Z, RulesEngine data.win.system.eventID:16384 data.win.system.eventSourceName:Software Protection Platform Service data.win.system.keywords:0x80000000000000 data.win.system.providerGuid:{E23B33B0-C8C9-472C-A5F9-F2BDFEA0F156} data.win.system.level:4 data.win.system.channel:Application data.win.system.opcode:0 data.win.system.message:"Successfully scheduled Software Protection service for re-start at 2124-10-25T12:20:33Z. Reason: RulesEngine." data.win.system.version:0 data.win.system.systemTime:2024-11-18T12:20:33.8225648Z data.win.system.eventRecordID:16201 data.win.system.threadID:0 data.win.system.computer:DESKTOP-SCHL4P4 data.win.system.task:0 data.win.system.processID:0 data.win.system.severityValue:INFORMATION

17. Nov 18, 2024 @ 17:52:10.261

input.type:log agent.ip:192.168.1.8 agent.name:windows agent.id:001 manager.name:wazuh.manager data.win.eventdata.subjectLogonId:0x3e7 data.win.eventdata.subjectDomainName:WORKGROUP data.win.eventdata.targetLinkedLogonId:0x0 data.win.eventdata.impersonationLevel:%%1833 data.win.eventdata.authenticationPackageName:Negotiate data.win.eventdata.targetLogonId:0x3e7 data.win.eventdata.logonProcessName:Advapi data.win.eventdata.logonGuid:{00000000-0000-0000-0000-000000000000} data.win.eventdata.targetUserName:SYSTEM data.win.eventdata.keyLength:0 data.win.eventdata.elevatedToken:%%1842 data.win.eventdata.subjectUserSid:S-1-5-18 data.win.eventdata.processId:0x434 data.win.eventdata.processName:C:\\Windows\\System32\\services.exe data.win.eventdata.targetDomainName:NT AUTHORITY  
  
18. Nov 18, 2024 @ 17:59:20.492

input.type:log agent.ip:192.168.1.13 agent.name:Megha agent.id:005 manager.name:wazuh.manager data.win.eventdata.subjectLogonId:0x3e7 data.win.eventdata.subjectDomainName:WORKGROUP data.win.eventdata.targetLinkedLogonId:0x0 data.win.eventdata.impersonationLevel:%%1833 data.win.eventdata.authenticationPackageName:Negotiate data.win.eventdata.targetLogonId:0x3e7 data.win.eventdata.logonProcessName:Advapi data.win.eventdata.logonGuid:{00000000-0000-0000-0000-000000000000} data.win.eventdata.targetUserName:SYSTEM data.win.eventdata.keyLength:0 data.win.eventdata.elevatedToken:%%1842 data.win.eventdata.subjectUserSid:S-1-5-18 data.win.eventdata.processId:0x3c4 data.win.eventdata.processName:C:\\Windows\\System32\\services.exe data.win.eventdata.targetDomainName:NT AUTHORITY data.win.eventdata.targetUserSid:S-1-5-18 data.win.eventdata.virtualAccount:%%1843 data.win.eventdata.logonType:5 data.win.eventdata.subjectUserName:LAPTOP-EQ5EDSEM$ data.win.system.eventID:4624 data.win.system.keywords:0x8020000000000000 data.win.system.providerGuid:{54849625-5478-4994-a5ba-3e3b0328c30d} data.win.system.level:0  
  
19. Nov 18, 2024 @ 18:06:00.285

input.type:log agent.name:nagappa-ubuntu agent.id:006 manager.name:wazuh.manager data.file:/usr/bin/diff data.title:Trojaned version of file detected. rule.firedtimes:4 rule.mail:false rule.level:7 rule.pci\_dss:10.6.1 rule.description:Host-based anomaly detection event (rootcheck). rule.groups:ossec, rootcheck rule.id:510 rule.gdpr:IV\_35.7.d location:rootcheck decoder.name:rootcheck id:1731933360.11882309 full\_log:Trojaned version of file '/usr/bin/diff' detected. Signature used: 'bash|^/bin/sh|file\.h|proc\.h|/dev/[^n]|^/bin/.\*sh' (Generic). timestamp:Nov 18, 2024 @ 18:06:00.285 \_index:wazuh-alerts-4.x-2024.11.18

20. Nov 18, 2024 @ 18:06:00.267

input.type:log agent.name:nagappa-ubuntu agent.id:006 manager.name:wazuh.manager data.file:/bin/diff data.title:Trojaned version of file detected. rule.firedtimes:3 rule.mail:false rule.level:7 rule.pci\_dss:10.6.1 rule.description:Host-based anomaly detection event (rootcheck). rule.groups:ossec, rootcheck rule.id:510 rule.gdpr:IV\_35.7.d location:rootcheck decoder.name:rootcheck id:1731933360.11881918 full\_log:Trojaned version of file '/bin/diff' detected. Signature used: 'bash|^/bin/sh|file\.h|proc\.h|/dev/[^n]|^/bin/.\*sh' (Generic). timestamp:Nov 18, 2024 @ 18:06:00.267 \_index:wazuh-alerts-4.x-2024.11.18

21. Nov 18, 2024 @ 18:05:58.444

input.type:log agent.name:nagappa-ubuntu agent.id:006 manager.name:wazuh.manager data.extra\_data:nagappa-ubuntu->any rule.firedtimes:1 rule.mail:false rule.level:3 rule.pci\_dss:10.6.1, 10.2.6 rule.hipaa:164.312.b rule.tsc:CC7.2, CC7.3, CC6.8 rule.description:Wazuh agent started. rule.groups:ossec rule.id:503 rule.nist\_800\_53:AU.6, AU.14, AU.5 rule.gpg13:10.1 rule.gdpr:IV\_35.7.d location:wazuh-agent decoder.parent:ossec decoder.name:ossec id:1731933358.11881578 full\_log:ossec: Agent started: 'nagappa-ubuntu->any'. timestamp:Nov 18, 2024 @ 18:05:58.444 \_index:wazuh-alerts-4.x-2024.11.18

22. Nov 18, 2024 @ 18:05:56.192

input.type:log agent.name:nagappa-ubuntu agent.id:006 manager.name:wazuh.manager data.extra\_data:nagappa-ubuntu->any rule.mail:false rule.level:3 rule.pci\_dss:10.6.1, 10.2.6 rule.hipaa:164.312.b rule.tsc:CC7.2, CC7.3, CC6.8 rule.description:Wazuh agent stopped. rule.groups:ossec rule.nist\_800\_53:AU.6, AU.14, AU.5 rule.gdpr:IV\_35.7.d rule.firedtimes:1 rule.mitre.technique:Disable or Modify Tools rule.mitre.id:T1562.001 rule.mitre.tactic:Defense Evasion rule.id:506 rule.gpg13:10.1 location:wazuh-remoted decoder.parent:ossec decoder.name:ossec id:1731933356.11881236 full\_log:ossec: Agent stopped: 'nagappa-ubuntu->any'. timestamp:Nov 18, 2024 @ 18:05:56.192 \_index:wazuh-alerts-4.x-2024.11.18

23. Nov 18, 2024 @ 18:05:54.068

input.type:log agent.name:nagappa-ubuntu agent.id:006 manager.name:wazuh.manager data.file:/usr/bin/diff data.title:Trojaned version of file detected. rule.firedtimes:2 rule.mail:false rule.level:7 rule.pci\_dss:10.6.1 rule.description:Host-based anomaly detection event (rootcheck). rule.groups:ossec, rootcheck rule.id:510 rule.gdpr:IV\_35.7.d location:rootcheck decoder.name:rootcheck id:1731933354.11880837 full\_log:Trojaned version of file '/usr/bin/diff' detected. Signature used: 'bash|^/bin/sh|file\.h|proc\.h|/dev/[^n]|^/bin/.\*sh' (Generic). timestamp:Nov 18, 2024 @ 18:05:54.068 \_index:wazuh-alerts-4.x-2024.11.18

24. Nov 18, 2024 @ 18:05:54.059

input.type:log agent.name:nagappa-ubuntu agent.id:006 manager.name:wazuh.manager data.file:/bin/diff data.title:Trojaned version of file detected. rule.firedtimes:1 rule.mail:false rule.level:7 rule.pci\_dss:10.6.1 rule.description:Host-based anomaly detection event (rootcheck). rule.groups:ossec, rootcheck rule.id:510 rule.gdpr:IV\_35.7.d location:rootcheck decoder.name:rootcheck id:1731933354.11880446 full\_log:Trojaned version of file '/bin/diff' detected. Signature used: 'bash|^/bin/sh|file\.h|proc\.h|/dev/[^n]|^/bin/.\*sh' (Generic). timestamp:Nov 18, 2024 @ 18:05:54.059 \_index:wazuh-alerts-4.x-2024.11.18

25. Nov 18, 2024 @ 18:05:52.533

input.type:log agent.name:nagappa-ubuntu agent.id:006 manager.name:wazuh.manager data.extra\_data:nagappa-ubuntu->any rule.firedtimes:1 rule.mail:false rule.level:3 rule.pci\_dss:10.6.1 rule.hipaa:164.312.b rule.tsc:CC7.2, CC7.3 rule.description:New wazuh agent connected. rule.groups:ossec rule.id:501 rule.nist\_800\_53:AU.6 rule.gpg13:10.1 rule.gdpr:IV\_35.7.d location:wazuh-agent decoder.parent:ossec decoder.name:ossec id:1731933352.11880160 full\_log:ossec: Agent started: 'nagappa-ubuntu->any'. timestamp:Nov 18, 2024 @ 18:05:52.533 \_index:wazuh-alerts-4.x-2024.11.18