Invoke-Mimikatz (PowerSploit)

Table of Contents

Open all sections | Close all sections

Tool Overview

Category

Password and Hash Dump

Description

Loads Mimikatz into memory and starts it up.

Example of Presumed Tool Use During an Attack

This tool is used to acquire the user's password and use it for unauthorized login.

Tool Operation Overview

Item	Source Host	Destination Host
OS	Windows	
Belonging to Domain	Not required	
Rights	Administrator	
Communication Protocol	5985/tcp (HTTP), 5986/tcp (HTTPS)	
Service	Windows Remote Management	

Information Acquired from Log

Standard Settings

- Source host
  - Execution history (Prefetch)
  - Details of the script/command executed (Windows 10 only. They are recorded in "Microsoft-Windows-PowerShell/Operational" and C:\Users\[User Name]\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt)

Additional Settings

- Source host
  - Execution history (audit policy, Sysmon)
  - A record of communication using WinRM (5985/tcp) (audit policy, Sysmon)
  - Details of the script/command executed (when Windows Management Framework 5.0 is installed on Windows 7. They are recorded in "Microsoft-Windows-PowerShell/Operational" and C:\Users\[User Name]\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt)
- Destination Host
  - A record of communication using WinRM (5985/tcp) (audit policy, Sysmon)

- Evidence That Can Be Confirmed When Execution is Successful

- Source Host: The Event ID: 4104 is recorded in the event log "Microsoft-Windows-PowerShell/Operational", and its contents include a Invoke-Mimikatz script (Windows 10, or when Windows Management Framework 5.0 is installed on Windows 7).

- Main Information Recorded at Execution

- Source Host

Event log

#	Log	Event ID	Task Category	Event Details
1	Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	Process Create. • **CommandLine**: Command line of the execution command ("C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe") • **UtcTime**: Process execution date and time (UTC) • **ProcessGuid/ProcessId**: Process ID • **Image**: Path to the executable file (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **User**: Execute as user
2	Microsoft-Windows-WinRM/Operational	6	WSMan Session Initialize	Creating WSMan Session. The connect string is [Connect String]. • **Connect String**: Host name (source host)
3	Microsoft-Windows-PowerShell/Operational	4104	Execute a Remote Command.	Creating Scriptblock text. • **Message**: The content of the script executed. The content of the executed PowerShell script is recorded as is.
4	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. • **Protocol**: Protocol (tcp) • **Image**: Path to the executable file (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **SourceIp/SourceHostname/SourcePort**: Source IP address/Host name/Port number (source host) • **DestinationIp/DestinationHostname/DestinationPort**: Destination IP address/Host name/Port number (destination port: 5985)

USN journal

#	File Name	Process

1	ConsoleHost_history.txt	CLOSE+DATA_EXTEND

UserAssist

#	Registry	Data
1	HKEY_USERS\[User SID]\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\JvaqbjfCbjreFuryy\i1.0\cbjrefuryy.rkr	Date and time of the initial execution, Total number of executions

MFT

#	Path	Header Flag	Validity
1	[Drive Name]:\Users\[User Name]\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt	FILE	ALLOCATED

Prefetch

- C:\Windows\Prefetch\POWERSHELL.EXE-[RANDOM].pf

- Destination Host

Event log

#	Log	Event ID	Task Category	Event Details
1	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. • **Protocol**: Protocol (tcp) • **Image**: Path to the executable file (System) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **SourceIp/SourceHostname/SourcePort**: Source IP address/Host name/Port number (destination port: 5985) • **DestinationIp/DestinationHostname/DestinationPort**: Destination IP address/Host name/Port number (source host)
2	Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	Process Create. • **ParentImage**: Executable file of the parent process (C:\Windows\System32\svchost.exe) • **CommandLine**: Command line of the execution command (C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding) • **ParentCommandLine**: Command line of the parent process (C:\Windows\system32\svchost.exe -k DcomLaunch) • **UtcTime**: Process execution date and time (UTC) • **ProcessGuid/ProcessId**: Process ID • **Image**: Path to the executable file (C:\Windows\System32\wbem\WmiPrvSE.exe)
3	Microsoft-Windows-WinRM/Operational	81	Processing of Request	Processing client request for operation [Operation]. • **Operation**: Requested process (CreateShell)

Prefetch

- C:\Windows\Prefetch\WSMPROVHOST.EXE-[RANDOM].pf

- Details: Source Host

- USN Journal

#	File Name	Process	Attribut
1	POWERSHELL.EXE-[RANDOM].pf	FILE_CREATE	archive
	POWERSHELL.EXE-[RANDOM].pf	FILE_CREATE+SECURITY_CHANGE	archive
	POWERSHELL.EXE-[RANDOM].pf	DATA_EXTEND+FILE_CREATE+SECURITY_CHANGE	archive
	POWERSHELL.EXE-[RANDOM].pf	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+SECURITY_CHANGE	archive
	POWERSHELL.EXE-[RANDOM].pf	BASIC_INFO_CHANGE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+SECURITY_CHANGE	archive
	POWERSHELL.EXE-[RANDOM].pf	BASIC_INFO_CHANGE+CLOSE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+SECURITY_CHANGE	archive
2	POWERSHELL.EXE-[RANDOM].pf	DATA_TRUNCATION	archive
	POWERSHELL.EXE-[RANDOM].pf	DATA_EXTEND+DATA_TRUNCATION	archive
	POWERSHELL.EXE-[RANDOM].pf	CLOSE+DATA_EXTEND+DATA_TRUNCATION	archive
3	CustomDestinations	FILE_CREATE	directory
	CustomDestinations	CLOSE+FILE_CREATE	directory
4	[RANDOM].customDestinations-ms	FILE_CREATE	archive
	[RANDOM].customDestinations-ms	FILE_CREATE+SECURITY_CHANGE	archive
	[RANDOM].customDestinations-ms	DATA_EXTEND+FILE_CREATE+SECURITY_CHANGE	archive
	[RANDOM].customDestinations-ms	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+SECURITY_CHANGE	archive
	[RANDOM].customDestinations-ms	BASIC_INFO_CHANGE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+SECURITY_CHANGE	archive
	[RANDOM].customDestinations-ms	BASIC_INFO_CHANGE+CLOSE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE+SECURITY_CHANGE	archive
5	[RANDOM].customDestinations-ms~RF[RANDOM].TMP	FILE_CREATE	hidden+archive+
	[RANDOM].customDestinations-ms~RF[RANDOM].TMP	CLOSE+FILE_CREATE	hidden+archive+
	[RANDOM].customDestinations-ms~RF[RANDOM].TMP	CLOSE+FILE_DELETE	hidden+archive+
6	[RANDOM].ps1	FILE_CREATE	archive
	[RANDOM].ps1	DATA_EXTEND+FILE_CREATE	archive
	[RANDOM].ps1	CLOSE+DATA_EXTEND+FILE_CREATE	archive
	[RANDOM].ps1	CLOSE+FILE_DELETE	archive
7	[RANDOM].psm1	FILE_CREATE	archive
	[RANDOM].psm1	DATA_EXTEND+FILE_CREATE	archive
	[RANDOM].psm1	CLOSE+DATA_EXTEND+FILE_CREATE	archive
	[RANDOM].psm1	CLOSE+FILE_DELETE	archive
8	ConsoleHost_history.txt	DATA_EXTEND	archive
	ConsoleHost_history.txt	CLOSE+DATA_EXTEND	archive

- **Event Log**

#	Event Log	Event ID	Task Category	Event Details
1	Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	Process Create. • **LogonGuid/LogonId**: ID of the logon session • **ParentProcessGuid/ParentProcessId**: Process ID of the parent process • **ParentImage**: Executable file of the parent process • **CurrentDirectory**: Work directory • **CommandLine**: Command line of the execution command ("C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe") • **IntegrityLevel**: Privilege level • **ParentCommandLine**: Command line of the parent process • **UtcTime**: Process execution date and time (UTC) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user • **Hashes**: Hash value of the executable file (High) • **Image**: Path to the executable file (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe)
	Security	4688	Process Create	A new process has been created. • **Process Information > Required Label**: Necessity of privilege escalation • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Process Information > Source Process Name**: Path to parent process that created the new process • **Log Date and Time**: Process execution date and time (local time) • **Process Information > New Process Name**: Path to the executable file (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Process Information > Token Escalation Type**: Presence of privilege escalation (1) • **Process Information > New Process ID**: Process ID (hexadecimal) • **Process Information > Source Process ID**: Process ID of the parent process that created th new process. "Creator Process ID" in Windows 7 • **Subject > Logon ID**: Session ID of the user who executed the process
2	Microsoft-Windows-PowerShell/Operational	40961	PowerShell Console Startup	The PowerShell console is starting up.
	Microsoft-Windows-PowerShell/Operational	53504	PowerShell Named Pipe IPC	Windows PowerShell has started an IPC listening thread on process [Process ID] of the [Domain].
	Microsoft-Windows-PowerShell/Operational	40962	PowerShell Console Startup	PowerShell console is ready for user input
3	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (including WriteData or AddFile, and AppendData) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\[User Name]\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\[RANDOM].tem • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Type of the file (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4663	File System	An attempt was made to access an object. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (WriteData or AddFile, AppendData)

				• **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\[User Name]\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\[RANDOM].tem • **Audit Success**: Success or failure (access successful) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Category of the target (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the object (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Microsoft-Windows-Sysmon/Operational	11	File created (rule: FileCreate)	File created. • **Image**: Path to the executable file (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **ProcessGuid/ProcessId**: Process ID • **TargetFilename**: Created file (C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestination [RANDOM].temp) • **CreationUtcTime**: File creation date and time (UTC)
	Microsoft-Windows-Sysmon/Operational	2	File creation time changed (rule: FileCreateTime)	File creation time changed. • **UtcTime**: Date and time the change occurred (UTC) • **CreationUtcTime**: New timestamp (UTC) • **Image**: Path to the executable file (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **PreviousCreationUtcTime**: Old timestamp (UTC) • **TargetFilename**: Name of the file changed (C:\Users\[User Name]\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\[RANDOM].tem
4	Security	4670	Authorization Policy Change	Permissions on an object were changed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Audit Success**: Success or failure (change successful) • **Object > Object Name**: Target file name (C:\Users\[User Name]\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\[RANDOM].tem • **Subject > Account Name**: Name of the account that executed the tool • **Subject > Account Domain**: Domain to which the account belongs • **Change permissions > New security descriptor**: Security descriptor after the change (D:ARAI(A;;FA;;;SY)(A;;FA;;;BA)(A;;FA;;;[SID])(A;ID;FA;;;SY)(A;ID;FA;;;BA)(A;ID;FA;;;[SID])) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Change permissions > Original security descriptor**: Security descriptor before the chang (D:(A;;FA;;;SY)(A;;FA;;;BA)(A;;FA;;;[SID])) • **Subject > Security ID**: SID of the user who executed the tool • **Object > Object Type**: Category of the target (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
5	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (including WriteData or AddFile, and AppendData)

				• **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\[User Name]\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\ [RANDOM].customDestinations-ms) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Type of the file (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4663	File System	An attempt was made to access an object. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privilege • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestination [RANDOM].customDestinations-ms) • **Audit Success**: Success or failure (access successful) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Target category • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the object (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
6	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (including WriteData or AddFile) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\[User Name]\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\ [RANDOM].customDestinations-ms~[RANDOM].TMP) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Type of the file (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the object (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
7	Security	4656	File System/Other Object Access	A handle to an object was requested.

			Events	• **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (including SYNCHRONIZE, and WriteData or AddFile) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestination • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Type of the file (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4663	File System	An attempt was made to access an object. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (SYNCHRONIZE, WriteData or AddFile) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestination • **Audit Success**: Success or failure (access successful) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Target category • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the object (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
8	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privilege (including DELETE) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestination [ALPHANUM].customDestinations-ms~[ALPHANUM].TMP) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Type of the file (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4663	File System	An attempt was made to access an object. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privilege (DELETE) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestination [ALPHANUM].customDestinations-ms~[ALPHANUM].TMP) • **Audit Success**: Success or failure (access successful)

				• **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Category of the target (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4660	File System	An object was deleted. • **Process Information > Process ID**: Process ID (hexadecimal) • **Audit Success**: Success or failure (access successful) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name • **Access Request Information > Access**: Requested privilege • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the object (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
9	Microsoft-Windows-Sysmon/Operational	13	Registry value set (rule: RegistryEvent)	Registry value set. • **EventType**: Process type (SetValue) • **Image**: Path to the executable file (C:\Windows\Explorer.EXE) • **ProcessGuid/ProcessId**: Process ID • **Details**: Setting value written to the registry (Binary Data) • **TargetObject**: Registry value at the write destination (\REGISTRY\USER\[User SID]\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{[GUID]}\Count\{[GUID]}\JvaqbjfCbjreFuryy\i1.0\cbjrefuryy.rkr)
	Microsoft-Windows-Sysmon/Operational	13	Registry value set (rule: RegistryEvent)	Registry value set. • **EventType**: Process type (SetValue) • **Image**: Path to the executable file (C:Windows\Explorer.EXE) • **ProcessGuid/ProcessId**: Process ID • **Details**: Setting value written to the registry (QWORD) • **TargetObject**: Registry value at the write destination (\REGISTRY\USER\[User SID]\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData\{[GUID]}\WindowsPowerShell\v1.0\powershell.exe)
	Microsoft-Windows-Sysmon/Operational	10	Process accessed (rule: ProcessAccess)	Process accessed. • **SourceProcessGUID/SourceProcessId/SourceThreadId**: Process of the access source process/Thread ID • **TargetProcessGUID/TargetProcessId**: Process ID of the access destination process • **GrantedAccess**: Details of the granted access • **SourceImage**: Path to the access source process (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **TargetImage**: Path to the access destination process (C:\Windows\Explorer.EXE)
10	Security	4703	Token Right Adjusted Events	A token right was adjusted. • **Disabled Privileges**: Privileges that were disabled • **Target Account > Security ID/Account Name/Account Domain**: Target user SID/Accou name/Domain • **Target Account > Logon ID**: Session ID of the target user • **Enabled Privileges**: Enabled privileges (SeDebugPrivilege)

				• **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Process Information > Process ID**: ID of the executed process • **Process Information > Process Name**: Name of the executed process (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe)
	Security	4673	Sensitive Privilege Use	A privileged service was called. • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Process > Process ID**: ID of the process that used the privilege • **Subject > Logon ID**: Session ID of the user who executed the process • **Service Request Information > Privilege**: Privilege used (SeCreateGlobalPrivilege) • **Process > Process Name**: Process that used the privilege (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe)
11	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (including WriteData or AddFile) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\Administrator\AppData\Local\Temp\[RANDOM].ps1) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Type of the file (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4663	File System	An attempt was made to access an object. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (WriteData or AddFile) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\Administrator\AppData\Local\Temp\[RANDOM].ps1) • **Audit Success**: Success or failure (access successful) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Category of the target (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the object (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
12	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (including WriteData or AddFile) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool

				• **Object > Object Name**: Target file name (C:\Users\Administrator\AppData\Local\Temp\[RANDOM].psm1) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Type of the file (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4663	File System	An attempt was made to access an object. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (WriteData or AddFile) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\Administrator\AppData\Local\Temp\[RANDOM].psm1) • **Audit Success**: Success or failure (access successful) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Category of the target (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
13	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (including DELETE) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\Administrator\AppData\Local\Temp\[RANDOM].ps1) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Type of the file (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4663	File System	An attempt was made to access an object. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privilege (DELETE) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\Administrator\AppData\Local\Temp\[RANDOM].ps1) • **Audit Success**: Success or failure (access successful) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Category of the target (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4660	File System	An object was deleted. • **Process Information > Process ID**: Process ID (hexadecimal) • **Audit Success**: Success or failure (access successful) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name • **Access Request Information > Access**: Requested privilege • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Subject > Logon ID**: Session ID of the user who executed the process

				• **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the object (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
14	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privilege (DELETE) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\Administrator\AppData\Local\Temp\[RANDOM].psm1) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Type of the file (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4663	File System	An attempt was made to access an object. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privilege (DELETE) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\Administrator\AppData\Local\Temp\[RANDOM].psm1) • **Audit Success**: Success or failure (access successful) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Category of the target (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4660	File System	An object was deleted. • **Process Information > Process ID**: Process ID (hexadecimal) • **Audit Success**: Success or failure (access successful) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name • **Access Request Information > Access**: Requested privilege • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the object (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)

15	Microsoft-Windows-Sysmon/Operational	13	Registry value set (rule: RegistryEvent)	Registry value set. • **EventType**: Process type (SetValue) • **Image**: Path to the executable file (C:Windows\Explorer.EXE) • **ProcessGuid/ProcessId**: Process ID • **Details**: Setting value written to the registry (Binary Data) • **TargetObject**: Registry value at the write destination (\REGISTRY\USER\[SID]\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{[GUID]}\Count\{[GUID]}\JvaqbjfCbjreFuryy\i1.0\cbjrefuryy.rkr)
16	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (including WriteData or AddFile) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Windows\Prefetch\POWERSHELL.EXE-[RANDOM].pf) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\svchost.exe) • **Object > Object Type**: Type of the file (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4663	File System	An attempt was made to access an object. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privilege • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Windows\Prefetch\POWERSHELL.EXE-[RANDOM].pf) • **Audit Success**: Success or failure (access successful) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\svchost.exe) • **Object > Object Type**: Category of the target (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4658	File System	The handle to an object was closed. (The handle to an object was closed.) • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the object (C:\Windows\System32\svchost.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
17	Security	4656	File System/Other Object Access Events	A handle to an object was requested. (A handle to an object was requested.) • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (including WriteData or AddFile) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\[User Name]\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_histor • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Type of the file (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle

	Security	4663	File System	An attempt was made to access an object. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (WriteData or AddFile) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\[User Name]\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_histor • **Audit Success**: Success or failure (access successful) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Category of the target (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the object (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
18	Microsoft-Windows-PowerShell/Operational	4104	Execute a Remote Command.	Creating Scriptblock text. • **Message**: The content of the script executed. The content of the executed PowerShell script i recorded as is.
19	Microsoft-Windows-Sysmon/Operational	2	File creation time changed (rule: FileCreateTime)	File creation time changed. • **UtcTime**: Date and time the change occurred (UTC) • **CreationUtcTime**: New timestamp (UTC) • **Image**: Path to the executable file • **PreviousCreationUtcTime**: Old timestamp (UTC) • **TargetFilename**: Name of the file changed
	Microsoft-Windows-WinRM/Operational	29	WSMan API Initialize	Initializing the WSMan API completed successfully.
	Microsoft-Windows-WinRM/Operational	6	WSMan Session Initialize	Creating WSMan Session. The connect string is [Connect String]. • **Connect String**: Host name (source host)
	Microsoft-Windows-WinRM/Operational	31	WSMan Session Initialize	WSMan Create Session operation completed successfully
	Microsoft-Windows-WinRM/Operational	10	WSMan API Call	Setting WSMan Session Option ([Option Number]) with value ([Value]) completed successfully • **Option Number**: Option number for the setting target (34) • **Value**: Value set (WSMAN_OPTION_USE_INTEARACTIVE_TOKEN)
	Microsoft-Windows-WinRM/Operational	10	WSMan API Call	Setting WSMan Session Option ([Option Number]) with value ([Value]) completed successfully • **Option Number**: Option number for the setting target (26) • **Value**: Value set (WSMAN_OPTION_UI_LANGUAGE)
	Microsoft-Windows-WinRM/Operational	10	WSMan API Call	Setting WSMan Session Option ([Option Number]) with value ([Value]) completed successfully • **Option Number**: Option number for the setting target (25) • **Value**: Value set (WSMAN_OPTION_LOCALE)

Microsoft-Windows-WinRM/Operational	10	WSMan API Call	Setting WSMan Session Option ([Option Number]) with value ([Value]) completed successfully • **Option Number**: Option number for the setting target (1) • **Value**: Value set (WSMAN_OPTION_DEFAULT_OPERATION_TIMEOUTMS)
Microsoft-Windows-WinRM/Operational	10	WSMan API Call	Setting WSMan Session Option ([Option Number]) with value ([Value]) completed successfully • **Option Number**: Option number for the setting target (12) • **Value**: Value set (WSMAN_OPTION_TIMEOUTMS_CREATE_SHELL)
Microsoft-Windows-WinRM/Operational	10	WSMan API Call	Setting WSMan Session Option ([Option Number]) with value ([Value]) completed successfully • **Option Number**: Option number for the setting target (17) • **Value**: Value set (WSMAN_OPTION_TIMEOUTMS_CLOSE_SHELL)
Microsoft-Windows-WinRM/Operational	10	WSMan API Call	Setting WSMan Session Option ([Option Number]) with value ([Value]) completed successfully • **Option Number**: Option number for the setting target (16) • **Value**: Value set (WSMAN_OPTION_TIMEOUTMS_SIGNAL_SHELL)
Microsoft-Windows-WinRM/Operational	11	WSMan API Call	Creating a WSMan shell with the resource URI http://schemas.microsoft.com/wbem/wsman/1/windows/shell/cmd and ShellId Unspecified.
Microsoft-Windows-WinRM/Operational	10	WSMan API Call	Setting WSMan Session Option ([Option Number]) with value ([Value]) completed successfully • **Option Number**: Option number for the setting target (28) • **Value**: Value set (WSMAN_OPTION_MAX_ENVELOPE_SIZE_KB)
Microsoft-Windows-WinRM/Operational	13	WSMan API Call	Executing the WSMan command of CommandId Unspecified.
Microsoft-Windows-PowerShell/Operational	8193	Connect	Creating Runspace object. • **Instance ID**: Instance ID of the object
Microsoft-Windows-PowerShell/Operational	8194	Connect	Creating RunspacePool object. • **Instance ID**: Instance ID of the object
Microsoft-Windows-PowerShell/Operational	8195	Connect	Opening RunspacePool.
Microsoft-Windows-PowerShell/Operational	8197	Connect	Runspace state changed to [State]. • **State**: State of the runspace (Opening)
Microsoft-Windows-PowerShell/Operational	8196	PowerShell (Microsoft-Windows-PowerShell)	Modifying activity ID and correlating.
Microsoft-Windows-PowerShell/Operational	12039	PowerShell (Microsoft-Windows-PowerShell)	Modifying activity ID and correlating.
Microsoft-Windows-PowerShell/Operational	8196	PowerShell (Microsoft-Windows-PowerShell)	Modifying activity ID and correlating.
Microsoft-Windows-PowerShell/Operational	12039	PowerShell (Microsoft-Windows-PowerShell)	Modifying activity ID and correlating.
Microsoft-Windows-PowerShell/Operational	8196	PowerShell (Microsoft-Windows-PowerShell)	Modifying activity ID and correlating.

	Microsoft-Windows-PowerShell/Operational	12039	PowerShell (Microsoft-Windows-PowerShell)	Modifying activity ID and correlating.
	Microsoft-Windows-PowerShell/Operational	8197	Connect	Runspace state changed to [State]. • **State**: State of the runspace (Opened)
20	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (including WriteData or AddFile) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\[User Name]\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_histor • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Type of the file (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4663	File System	An attempt was made to access an object. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (WriteData or AddFile) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\[User Name]\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_histor • **Audit Success**: Success or failure (access successful) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Category of the target (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the object (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
21	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. • **Protocol**: Protocol (tcp) • **DestinationIp**: Destination IP address (Domain Controller IP address) • **Image**: Path to the executable file (C:\Windows\System32\lsass.exe) • **DestinationHostname**: Destination host name (Domain Controller host name) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **DestinationPort**: Destination port number (88) • **SourcePort**: Source port number (high port) • **SourceHostname**: Source host name (source host name) • **SourceIp**: Source IP address (source host IP address)
	Security	5158	Filtering Platform Connection	The Windows Filtering Platform has permitted a bind to a local port. • **Network Information > Protocol**: Protocol used (6=TCP) • **Network Information > Source Port**: Bind local port (high port)

				• **Application Information > Process ID**: Process ID • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\lsass.exe)
	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. • **Network Information > Destination Port**: Destination port number (88) • **Network Information > Source Port**: Source port number (high port) • **Network Information > Destination Address**: Destination IP address (Domain Controller • **Network Information > Protocol**: Protocol used (6=TCP) • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\lsass.exe) • **Network Information > Direction**: Communication direction (outbound) • **Network Information > Source Address**: Source IP address (source host) • **Application Information > Process ID**: Process ID
22	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. • **Protocol**: Protocol (tcp) • **DestinationIp**: Destination IP address (Domain Controller IP address) • **Image**: Path to the executable file (C:\Windows\System32\lsass.exe) • **DestinationHostname**: Destination host name (Domain Controller host name) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **DestinationPort**: Destination port number (88) • **SourcePort**: Source port number (high port) • **SourceHostname**: Source host name (source host name) • **SourceIp**: Source IP address (source host IP address)
	Security	5158	Filtering Platform Connection	The Windows Filtering Platform has permitted a bind to a local port. • **Network Information > Protocol**: Protocol used (6=TCP) • **Network Information > Source Port**: Bind local port (high port) • **Application Information > Process ID**: Process ID • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\lsass.exe)
	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. • **Network Information > Destination Port**: Destination port number (88) • **Network Information > Source Port**: Source port number (high port) • **Network Information > Destination Address**: Destination IP address (Domain Controller • **Network Information > Protocol**: Protocol used (6=TCP) • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\lsass.exe) • **Network Information > Direction**: Communication direction (outbound) • **Network Information > Source Address**: Source IP address (source host) • **Application Information > Process ID**: Process ID
23	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. • **Protocol**: Protocol (tcp) • **DestinationIp**: Destination IP address (Domain Controller IP address) • **Image**: Path to the executable file (C:\Windows\System32\lsass.exe) • **DestinationHostname**: Destination host name (Domain Controller host name) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **DestinationPort**: Destination port number (88) • **SourcePort**: Source port number (high port) • **SourceHostname**: Source host name (source host name) • **SourceIp**: Source IP address (source host IP address)
	Security	5158	Filtering Platform Connection	The Windows Filtering Platform has permitted a bind to a local port. • **Network Information > Protocol**: Protocol used (6=TCP) • **Network Information > Source Port**: Bind local port (high port)

				• **Application Information > Process ID**: Process ID • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\lsass.exe)
	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. • **Network Information > Destination Port**: Destination port number (88) • **Network Information > Source Port**: Source port number (high port) • **Network Information > Destination Address**: Destination IP address (Domain Controller • **Network Information > Protocol**: Protocol used (6=TCP) • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\lsass.exe) • **Network Information > Direction**: Communication direction (outbound) • **Network Information > Source Address**: Source IP address (source host) • **Application Information > Process ID**: Process ID
24	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. • **Protocol**: Protocol (tcp) • **DestinationIp**: Destination IP address (destination host IP address) • **Image**: Path to the executable file (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **DestinationHostname**: Destination host name (destination host name) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **DestinationPort**: Destination port number (5985) • **SourcePort**: Source port number (high port) • **SourceHostname**: Source host name (source host name) • **SourceIp**: Source IP address (source host IP address)
	Security	5158	Filtering Platform Connection	The Windows Filtering Platform has permitted a bind to a local port. • **Network Information > Protocol**: Protocol used (6=TCP) • **Network Information > Source Port**: Bind local port (high port) • **Application Information > Process ID**: Process ID • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\lsass.exe)
	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. • **Network Information > Destination Port**: Destination port number (5985) • **Network Information > Source Port**: Source port number (high port) • **Network Information > Destination Address**: Destination IP address (destination host) • **Network Information > Protocol**: Protocol used (6=TCP) • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\windowspowershell\v1.0\powershell.exe) • **Network Information > Direction**: Communication direction (outbound) • **Network Information > Source Address**: Source IP address (source host) • **Application Information > Process ID**: Process ID
25	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. • **Protocol**: Protocol (tcp) • **DestinationIp**: Destination IP address (destination host IP address) • **Image**: Path to the executable file (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **DestinationHostname**: Destination host name (destination host name) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **DestinationPort**: Destination port number (5985) • **SourcePort**: Source port number (high port) • **SourceHostname**: Source host name (source host name) • **SourceIp**: Source IP address (source host IP address)
	Security	5158	Filtering Platform Connection	The Windows Filtering Platform has permitted a bind to a local port.

				• **Network Information > Protocol**: Protocol used (6=TCP) • **Network Information > Source Port**: Bind local port (high port) • **Application Information > Process ID**: Process ID • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\windowspowershell\v1.0\powershell.exe)
	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. • **Network Information > Destination Port**: Destination port number (5985) • **Network Information > Source Port**: Source port number (high port) • **Network Information > Destination Address**: Destination IP address (destination host) • **Network Information > Protocol**: Protocol used (6=TCP) • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\windowspowershell\v1.0\powershell.exe) • **Network Information > Direction**: Communication direction (outbound) • **Network Information > Source Address**: Source IP address (source host) • **Application Information > Process ID**: Process ID
26	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. • **Protocol**: Protocol (tcp) • **DestinationIp**: Destination IP address (destination host IP address) • **Image**: Path to the executable file (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **DestinationHostname**: Destination host name (destination host name) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **DestinationPort**: Destination port number (5985) • **SourcePort**: Source port number (high port) • **SourceHostname**: Source host name (source host name) • **SourceIp**: Source IP address (source host IP address)
	Security	5158	Filtering Platform Connection	The Windows Filtering Platform has permitted a bind to a local port. • **Network Information > Protocol**: Protocol used (6=TCP) • **Network Information > Source Port**: Bind local port (high port) • **Application Information > Process ID**: Process ID • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\windowspowershell\v1.0\powershell.exe)
	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. • **Network Information > Destination Port**: Destination port number (5985) • **Network Information > Source Port**: Source port number (high port) • **Network Information > Destination Address**: Destination IP address (destination host) • **Network Information > Protocol**: Protocol used (6=TCP) • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\windowspowershell\v1.0\powershell.exe) • **Network Information > Direction**: Communication direction (outbound) • **Network Information > Source Address**: Source IP address (source host) • **Application Information > Process ID**: Process ID
27	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. • **Protocol**: Protocol (tcp) • **DestinationIp**: Destination IP address (destination host IP address) • **Image**: Path to the executable file (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **DestinationHostname**: Destination host name (destination host name) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **DestinationPort**: Destination port number (5985) • **SourcePort**: Source port number (high port) • **SourceHostname**: Source host name (source host name) • **SourceIp**: Source IP address (source host IP address)

	Security	5158	Filtering Platform Connection	The Windows Filtering Platform has permitted a bind to a local port. • **Network Information > Protocol**: Protocol used (6=TCP) • **Network Information > Source Port**: Bind local port (high port) • **Application Information > Process ID**: Process ID • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\windowspowershell\v1.0\powershell.exe)
	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. • **Network Information > Destination Port**: Destination port number (5985) • **Network Information > Source Port**: Source port number (high port) • **Network Information > Destination Address**: Destination IP address (destination host) • **Network Information > Protocol**: Protocol used (6=TCP) • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\windowspowershell\v1.0\powershell.exe) • **Network Information > Direction**: Communication direction (outbound) • **Network Information > Source Address**: Source IP address (source host) • **Application Information > Process ID**: Process ID
28	Microsoft-Windows-Sysmon/Operational	12	Registry object added or deleted (rule: RegistryEvent)	Registry object added or deleted. • **EventType**: Process type (CreateKey) • **Image**: Path to the executable file (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **ProcessGuid/ProcessId**: Process ID • **TargetObject**: Created/deleted registry key/value (\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters)
29	Microsoft-Windows-WinRM/Operational	15	WSMan API Call	Closing WSMan command
	Microsoft-Windows-WinRM/Operational	16	WSMan API Call	Closing WSMan shell
	Microsoft-Windows-WinRM/Operational	8	WSMan Session Uninitialize	Closing WSMan session
	Microsoft-Windows-WinRM/Operational	4	WSMan API Uninitialize	Uninitializing WSMan API
	Microsoft-Windows-WinRM/Operational	30	WSMan API Uninitialize	Uninitializing WSMan API completed successfully
	Microsoft-Windows-WinRM/Operational	33	WSMan Session Initialize	The operation for closing the WSMan session completed successfully.
	Microsoft-Windows-PowerShell/Operational	8196	PowerShell (Microsoft-Windows-PowerShell)	Modifying activity ID and correlating.
	Microsoft-Windows-PowerShell/Operational	12039	PowerShell (Microsoft-Windows-PowerShell)	Modifying activity ID and correlating.
	Microsoft-Windows-PowerShell/Operational	8197	Connect	Runspace state changed to [State].
	Microsoft-Windows-PowerShell/Operational	8197	Connect	Runspace state changed to [State].
30	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (including WriteData or AddFile) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\[User Name]\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive)

				• **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Type of the file (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4663	File System	An attempt was made to access an object. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (including WriteData or AddFile) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Object > Object Name**: Target file name (C:\Users\[User Name]\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive) • **Audit Success**: Success or failure (access successful) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Object > Object Type**: Category of the target (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the object (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
31	Microsoft-Windows-Sysmon/Operational	5	Process terminated (rule: ProcessTerminate)	Process terminated. • **UtcTime**: Process terminated date and time (UTC) • **ProcessGuid/ProcessId**: Process ID • **Image**: Path to the executable file (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe)
	Security	4689	Process Termination	A process has exited. • **Process Information > Process ID**: Process ID (hexadecimal) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of user who executed the tool • **Process Information > Exit Status**: Process return value (0xc000013a) • **Subject > Account Name**: Name of the account that executed the tool • **Log Date and Time**: Process terminated date and time (local time) • **Subject > Account Domain**: Domain to which the account belongs • **Process Information > Process Name**: Path to the executable file (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe) • **Subject > Security ID**: SID of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process

- **UserAssist**

#	Registry entry	Information That Can Be Confirmed
1	HKEY_USERS\[User SID]\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\JvaqbjfCbjreFuryy\i1.0\cbjrefuryy.rkr	Date and time of the initial execution, Total number of executions

- MFT

#	Path	Header Flag	Validity
1	[Drive Name]:\Windows\Prefetch\POWERSHELL.EXE-[RANDOM].pf	FILE	ALLOCATED
2	[Drive Name]:\Users\[User Name]\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations	FOLDER	ALLOCATED
3	[Drive Name]:\Users\[User Name]\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\[RANDOM].customDestinations-ms	FILE	ALLOCATED
4	[Drive Name]:\Users\[User Name]\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt	FILE	ALLOCATED

- Prefetch

#	Prefetch File	Process Name	Process Path	Information That Can Be Confirmed
1	POWERSHELL.EXE-[RANDOM].pf	POWERSHELL.EXE	\VOLUME{[GUID]}\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE	Last Run Time (last execution date and time)

- Registry Entry

#	Path	Type	Value
1	HKEY_USERS\[User SID]\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\JvaqbjfCbjreFuryy\i1.0\cbjrefuryy.rkr	Binary	[Binary Value]
2	HKEY_USERS\[User SID]\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\WindowsPowerShell\v1.0\powershell.exe	Binary	[Binary Value]

- Details: Destination Host

- Event Log

#	Event log	Event ID	Task Category	Event Details
1	Microsoft-Windows-WinRM/Operational	169	User Authentication	User [User Name] authenticated successfully using [Authentication Method] authentication • **User Name**: User name used • **Authentication Method**: Authentication method used (Kerberos)
	Security	4624	Logon	An account was successfully logged on. • **Process Information > Process ID**: Process ID (hexadecimal) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **New Logon > Logon ID/Logon GUID**: Session ID of the user who was logged on • **Detailed Authentication Information > Package Name (NTLM only)**: NTLM version • **Detailed Authentication Information > Logon Process**: Process used for logon (Kerberos)

				• **Network Information > Source Port**: Source port number • **New Logon > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who was logged on • **Logon Type**: Logon path, method, etc. (3=Network) • **Network Information > Workstation Name**: Name of the host that requested the logon • **Detailed Authentication Information > Key Length**: Length of the key used for the authentication (0) • **Process Information > Process Name**: Path to the executable file • **Detailed Authentication Information > Authentication Package**: Authentication package used (Kerberos) • **Network Information > Source Network Address**: IP address that requested the logon • **Subject > Logon ID**: Session ID of the user who executed the authentication
	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privilege • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\svchost.exe) • **Object > Object Type**: File type (Unknown) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
2	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. • **Protocol**: Protocol (tcp) • **DestinationIp**: Destination IP address (source host IP address) • **Image**: Path to the executable file (System) • **DestinationHostname**: Destination host name (source host name) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **DestinationPort**: Destination port number (high port) • **SourcePort**: Source port number (5985) • **SourceHostname**: Source host name (destination host name) • **SourceIp**: Source IP address (destination host IP address)
	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. • **Network Information > Destination Port**: Destination port number (high port) • **Network Information > Source Port**: Source port number (5985) • **Network Information > Destination Address**: Destination IP address (source host) • **Network Information > Protocol**: Protocol used (6=TCP) • **Application Information > Application Name**: Execution process (System) • **Network Information > Direction**: Communication direction (inbound) • **Network Information > Source Address**: Source IP address (destination host) • **Application Information > Process ID**: Process ID
	Security	4672	Special Logon	Privileges assigned to a new logon. • **Privileges**: Assigned privileges (SeSecurityPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeTakeOwnershipPrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeLoadDriverPrivilege, SeImpersonatePrivilege) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process

	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. (Network connection detected) • **Protocol**: Protocol (tcp) • **DestinationIp**: Destination IP address (Domain Controller IP address) • **Image**: Path to the executable file (System) • **DestinationHostname**: Destination host name (Domain Controller host name) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **DestinationPort**: Destination port number (88) • **SourcePort**: Source port number (high port) • **SourceHostname**: Source host name (destination host) • **SourceIp**: Source IP address (destination host IP address)
3	Security	5158	Filtering Platform Connection	The Windows Filtering Platform has permitted a bind to a local port. • **Network Information > Protocol**: Protocol used (6=TCP) • **Network Information > Source Port**: Bind local port (high port) • **Application Information > Process ID**: Process ID • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\lsass.exe)
	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. • **Network Information > Destination Port**: Destination port number (88) • **Network Information > Source Port**: Source port number (high port) • **Network Information > Destination Address**: Destination IP address (Domain Controller) • **Network Information > Protocol**: Protocol used (6=TCP) • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\lsass.exe) • **Network Information > Direction**: Communication direction (outbound) • **Network Information > Source Address**: Source IP address (destination host) • **Application Information > Process ID**: Process ID
4	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. (Network connection detected) • **Protocol**: Protocol (tcp) • **DestinationIp**: Destination IP address (Domain Controller IP address) • **Image**: Path to the executable file (System) • **DestinationHostname**: Destination host name (Domain Controller host name) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **DestinationPort**: Destination port number (88) • **SourcePort**: Source port number (high port) • **SourceHostname**: Source host name (destination host) • **SourceIp**: Source IP address (destination host IP address)
	Security	5158	Filtering Platform Connection	The Windows Filtering Platform has permitted a bind to a local port. • **Network Information > Protocol**: Protocol used (6=TCP) • **Network Information > Source Port**: Bind local port (high port) • **Application Information > Process ID**: Process ID • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\lsass.exe)
	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. • **Network Information > Destination Port**: Destination port number (88) • **Network Information > Source Port**: Source port number (high port) • **Network Information > Destination Address**: Destination IP address (Domain Controller) • **Network Information > Protocol**: Protocol used (6=TCP) • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\lsass.exe) • **Network Information > Direction**: Communication direction (outbound) • **Network Information > Source Address**: Source IP address (destination host)

				• **Application Information > Process ID**: Process ID
5	Security	4688	Process Create	A new process has been created. • **Process Information > Required Label**: Necessity of privilege escalation • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Process Information > Source Process Name**: Path to parent process that created the new process • **Log Date and Time**: Process execution date and time (local time) • **Process Information > New Process Name**: Path to the executable file (C:\Windows\System32\wsmprovhost.exe) • **Process Information > Token Escalation Type**: Presence of privilege escalation (1) • **Process Information > New Process ID**: Process ID (hexadecimal) • **Process Information > Source Process ID**: Process ID of the parent process that created the new process. "Creator Process ID" in Windows 7 • **Subject > Logon ID**: Session ID of the user who executed the process
6	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. • **Protocol**: Protocol (tcp) • **DestinationIp**: Destination IP address (source host IP address) • **Image**: Path to the executable file (System) • **DestinationHostname**: Destination host name (source host name) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **DestinationPort**: Destination port number (high port) • **SourcePort**: Source port number (5985) • **SourceHostname**: Source host name (destination host name) • **SourceIp**: Source IP address (destination host IP address)
	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. • **Network Information > Destination Port**: Destination port number (high port) • **Network Information > Source Port**: Source port number (5985) • **Network Information > Destination Address**: Destination IP address (source host) • **Network Information > Protocol**: Protocol used (6=TCP) • **Application Information > Application Name**: Execution process (System) • **Network Information > Direction**: Communication direction (inbound) • **Network Information > Source Address**: Source IP address (destination host) • **Application Information > Process ID**: Process ID
7	Security	4672	Special Logon	Privileges assigned to a new logon. • **Privileges**: Assigned privileges (SeSecurityPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeTakeOwnershipPrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeLoadDriverPrivilege, SeImpersonatePrivilege) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process
	Security	4624	Logon	An account was successfully logged on. • **Process Information > Process ID**: Process ID (hexadecimal) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **New Logon > Logon ID/Logon GUID**: Session ID of the user who was logged on • **Detailed Authentication Information > Package Name (NTLM only)**: NTLM version • **Detailed Authentication Information > Logon Process**: Process used for logon (Kerberos) • **Network Information > Source Port**: Source port number • **New Logon > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who was logged on

				• **Logon Type**: Logon path, method, etc. • **Network Information > Workstation Name**: Name of the host that requested the logon • **Detailed Authentication Information > Key Length**: Length of the key used for the authentication (0) • **Process Information > Process Name**: Path to the executable file • **Detailed Authentication Information > Authentication Package**: Authentication package used (Kerberos) • **Network Information > Source Network Address**: IP address that requested the logon • **Subject > Logon ID**: Session ID of the user who executed the authentication
	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privilege • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\svchost.exe) • **Object > Object Type**: File type (Unknown) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
8	Microsoft-Windows-WinRM/Operational	192	User Approval	Authorizing the user • **Error**: Error code
	Microsoft-Windows-WinRM/Operational	193	User Approval	A request for the user is made using a WinRM virtual account. • **User Information**: Information of the user • **Virtual Account**: WinRM virtual account to be used
	Microsoft-Windows-WinRM/Operational	192	User Approval	Authorizing the user • **Error**: Error code
	Microsoft-Windows-WinRM/Operational	81	Processing of Request	Processing client request for operation [Operation]. • **Operation**: Requested process (CreateShell)
	Microsoft-Windows-WinRM/Operational	82	Processing of Request	Entering the plug-in for executing the operation [Operation]. ResourceURI <[URL]> is used. • **URL**: URL of the resource (http://schemas.microsoft.com/powershell/Microsoft.PowerShell) • **Operation**: Requested process (Shell)
	Microsoft-Windows-WinRM/Operational	134	Response Processing	Sending response for operation [Operation] • **Operation**: Process performed (CreateShell)
9	Microsoft-Windows-WinRM/Operational	169	User Authentication	User [User Name] authenticated successfully using [Authentication Method] authentication • **User Name**: User name used • **Authentication Method**: Authentication method used (Kerberos)
	Microsoft-Windows-WinRM/Operational	192	User Approval	Authorizing the user • **Error**: Error code
	Microsoft-Windows-WinRM/Operational	193	User Approval	A request for the user is made using a WinRM virtual account. • **User Information**: Information of the user

			• **Virtual Account**: WinRM virtual account to be used
Microsoft-Windows-WinRM/Operational	192	User Approval	Authorizing the user • **Error**: Error code
Microsoft-Windows-WinRM/Operational	81	Processing of Request	Processing client request for operation [Operation]. • **Operation**: Requested process (Receive)
Microsoft-Windows-WinRM/Operational	82	Processing of Request	Entering the plug-in for executing the operation [Operation]. ResourceURI <[URL]> is used. • **URL**: URL of the resource (http://schemas.microsoft.com/powershell/Microsoft.PowerShell) • **Operation**: Requested process (Receive)
Microsoft-Windows-WinRM/Operational	83	Processing of Request	Coming out of the plug-in for executing the operation [Operation]. • **Operation**: Requested process (Receive)
Microsoft-Windows-WinRM/Operational	134	Response Processing	Sending response for operation [Operation] • **Operation**: Process performed (Receive)
Microsoft-Windows-WinRM/Operational	83	Processing of Request	Coming out of the plug-in for executing the operation [Operation]. • **Operation**: Requested process (Shell)
Microsoft-Windows-WinRM/Operational	192	User Approval	Authorizing the user • **Error**: Error code
Microsoft-Windows-WinRM/Operational	81	Processing of Request	Processing client request for operation [Operation]. • **Operation**: Requested process (Receive)
Microsoft-Windows-WinRM/Operational	82	Processing of Request	Entering the plug-in for executing the operation [Operation]. ResourceURI <[URL]> is used. • **URL**: URL of the resource (http://schemas.microsoft.com/powershell/Microsoft.PowerShell) • **Operation**: Requested process (Receive)
Microsoft-Windows-WinRM/Operational	83	Processing of Request	Coming out of the plug-in for executing the operation [Operation]. • **Operation**: Requested process (Receive)
Microsoft-Windows-WinRM/Operational	134	Response Processing	Sending response for operation [Operation] • **Operation**: Process performed (Receive)
Microsoft-Windows-WinRM/Operational	192	User Approval	Authorizing the user • **Error**: Error code
Microsoft-Windows-WinRM/Operational	81	Processing of Request	Processing client request for operation [Operation]. • **Operation**: Requested process (Receive)
Microsoft-Windows-WinRM/Operational	82	Processing of Request	Entering the plug-in for executing the operation [Operation]. ResourceURI <[URL]> is used. • **URL**: URL of the resource (http://schemas.microsoft.com/powershell/Microsoft.PowerShell) • **Operation**: Requested process (Receive)

	Microsoft-Windows-WinRM/Operational	83	Processing of Request	Coming out of the plug-in for executing the operation [Operation]. • **Operation**: Requested process (Receive)
	Microsoft-Windows-WinRM/Operational	192	User Approval	Authorizing the user • **Error**: Error code
10	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. • **Network Information > Destination Port**: Destination port number (high port) • **Network Information > Source Port**: Source port number (5985) • **Network Information > Destination Address**: Destination IP address (source host) • **Network Information > Protocol**: Protocol used (6=TCP) • **Application Information > Application Name**: Execution process (System) • **Network Information > Direction**: Communication direction (inbound) • **Network Information > Source Address**: Source IP address (destination host) • **Application Information > Process ID**: Process ID
11	Security	4672	Special Logon	Privileges assigned to a new logon. • **Privileges**: Assigned privileges (SeSecurityPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeTakeOwnershipPrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeLoadDriverPrivilege, SeImpersonatePrivilege) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process
	Security	4624	Logon	An account was successfully logged on. (An account successfully logged on.) • **Process Information > Process ID**: Process ID (hexadecimal) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **New Logon > Logon ID/Logon GUID**: Session ID of the user who was logged on • **Detailed Authentication Information > Package Name (NTLM only)**: NTLM version • **Detailed Authentication Information > Logon Process**: Process used for logon (Kerberos) • **Network Information > Source Port**: Source port number • **New Logon > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who was logged on • **Logon Type**: Logon path, method, etc. • **Network Information > Workstation Name**: Name of the host that requested the logon • **Detailed Authentication Information > Key Length**: Length of the key used for the authentication (0) • **Process Information > Process Name**: Path to the executable file • **Detailed Authentication Information > Authentication Package**: Authentication package used (Kerberos) • **Network Information > Source Network Address**: IP address that requested the logon • **Subject > Logon ID**: Session ID of the user who executed the authentication
	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privilege • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\svchost.exe) • **Object > Object Type**: File type (Unknown) • **Subject > Logon ID**: Session ID of the user who executed the process

				• **Object > Handle ID**: ID of the relevant handle
12	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. • **Network Information > Destination Port**: Destination port number (high port) • **Network Information > Source Port**: Source port number (5985) • **Network Information > Destination Address**: Destination IP address (source host) • **Network Information > Protocol**: Protocol used (6=TCP) • **Application Information > Application Name**: Execution process (System) • **Network Information > Direction**: Communication direction (inbound) • **Network Information > Source Address**: Source IP address (destination host) • **Application Information > Process ID**: Process ID
13	Security	4624	Logon	An account was successfully logged on. (An account successfully logged on.) • **Process Information > Process ID**: Process ID (hexadecimal) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **New Logon > Logon ID/Logon GUID**: Session ID of the user who was logged on • **Detailed Authentication Information > Package Name (NTLM only)**: NTLM version • **Detailed Authentication Information > Logon Process**: Process used for logon (Kerberos) • **Network Information > Source Port**: Source port number • **New Logon > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who was logged on • **Logon Type**: Logon path, method, etc. (3=Network) • **Network Information > Workstation Name**: Name of the host that requested the logon • **Detailed Authentication Information > Key Length**: Length of the key used for the authentication (0) • **Process Information > Process Name**: Path to the executable file • **Detailed Authentication Information > Authentication Package**: Authentication package used (Kerberos) • **Network Information > Source Network Address**: IP address that requested the logon • **Subject > Logon ID**: Session ID of the user who executed the authentication
	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privilege • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\svchost.exe) • **Object > Object Type**: File type (Unknown) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
14	Microsoft-Windows-WinRM/Operational	81	Processing of Request	Processing client request for operation [Operation]. • **Operation**: Requested process (Command)
	Microsoft-Windows-WinRM/Operational	82	Processing of Request	Entering the plug-in for executing the operation [Operation]. ResourceURI <[URL]> is used. • **URL**: URL of the resource (http://schemas.microsoft.com/powershell/Microsoft.PowerShell) • **Operation**: Requested process (Command)
	Microsoft-Windows-WinRM/Operational	83	Processing of Request	Coming out of the plug-in for executing the operation [Operation].

			• **Operation**: Requested process (Command)
Microsoft-Windows-WinRM/Operational	134	Response Processing	Sending response for operation [Operation] • **Operation**: Process performed (Command)
Microsoft-Windows-WinRM/Operational	169	User Authentication	User [User Name] authenticated successfully using [Authentication Method] authentication • **User Name**: User name used • **Authentication Method**: Authentication method used (Kerberos)
Microsoft-Windows-WinRM/Operational	192	User Approval	Authorizing the user • **Error**: Error code
Microsoft-Windows-WinRM/Operational	193	User Approval	A request for the user is made using a WinRM virtual account. • **User Information**: Information of the user • **Virtual Account**: WinRM virtual account to be used
Microsoft-Windows-WinRM/Operational	192	User Approval	Authorizing the user • **Error**: Error code
Microsoft-Windows-WinRM/Operational	81	Processing of Request	Processing client request for operation [Operation]. • **Operation**: Requested process (Send)
Microsoft-Windows-WinRM/Operational	82	Processing of Request	Entering the plug-in for executing the operation [Operation]. ResourceURI <[URL]> is used. • **URL**: URL of the resource (http://schemas.microsoft.com/powershell/Microsoft.PowerShell) • **Operation**: Requested process (Send)
Microsoft-Windows-WinRM/Operational	83	Processing of Request	Coming out of the plug-in for executing the operation [Operation]. • **Operation**: Requested process (Send)
Microsoft-Windows-WinRM/Operational	134	Response Processing	Sending response for operation [Operation] • **Operation**: Process performed (Send)
Microsoft-Windows-WinRM/Operational	169	User Authentication	User [User Name] authenticated successfully using [Authentication Method] authentication • **User Name**: User name used • **Authentication Method**: Authentication method used (Kerberos)
Microsoft-Windows-WinRM/Operational	192	User Approval	Authorizing the user • **Error**: Error code
Microsoft-Windows-WinRM/Operational	193	User Approval	A request for the user is made using a WinRM virtual account. • **User Information**: Information of the user • **Virtual Account**: WinRM virtual account to be used
Microsoft-Windows-WinRM/Operational	192	User Approval	Authorizing the user • **Error**: Error code
Microsoft-Windows-WinRM/Operational	81	Processing of Request	Processing client request for operation [Operation]. • **Operation**: Requested process (Receive)

	Microsoft-Windows-WinRM/Operational	82	Processing of Request	Entering the plug-in for executing the operation [Operation]. ResourceURI <[URL]> is used. • **URL**: URL of the resource (http://schemas.microsoft.com/powershell/Microsoft.PowerShell) • **Operation**: Requested process (Receive)
	Microsoft-Windows-WinRM/Operational	83	Processing of Request	Coming out of the plug-in for executing the operation [Operation]. • **Operation**: Requested process (Receive)
	Microsoft-Windows-WinRM/Operational	134	Response Processing	Sending response for operation [Operation] • **Operation**: Process performed (Send)
15	Security	4624	Logon	An account was successfully logged on. • **Process Information > Process ID**: Process ID (hexadecimal) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **New Logon > Logon ID/Logon GUID**: Session ID of the user who was logged on • **Detailed Authentication Information > Package Name (NTLM only)**: NTLM version • **Detailed Authentication Information > Logon Process**: Process used for logon (Advapi) • **Network Information > Source Port**: Source port number • **New Logon > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who was logged on • **Logon Type**: Logon path, method, etc. (5) • **Network Information > Workstation Name**: Name of the host that requested the logon • **Detailed Authentication Information > Key Length**: Length of the key used for the authentication (0) • **Process Information > Process Name**: Path to the executable file • **Detailed Authentication Information > Authentication Package**: Authentication package used (Negotiate) • **Network Information > Source Network Address**: IP address that requested the logon • **Subject > Logon ID**: Session ID of the user who executed the authentication
	Security	4672	Special Logon	Privileges assigned to a new logon. • **Privileges**: Assigned privileges (SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process
16	Security	4688	Process Create	A new process has been created. • **Process Information > Required Label**: Necessity of privilege escalation • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Process Information > Source Process Name**: Path to parent process that created the new process • **Log Date and Time**: Process execution date and time (local time) • **Process Information > New Process Name**: Path to the executable file (C:\Windows\System32\wbem\WmiPrvSE.exe) • **Process Information > Token Escalation Type**: Presence of privilege escalation (1) • **Process Information > New Process ID**: Process ID (hexadecimal) • **Process Information > Source Process ID**: Process ID of the parent process that created the new process. "Creator Process ID" in Windows 7 • **Subject > Logon ID**: Session ID of the user who executed the process

	Security	4674	Sensitive Privilege Use	An operation was attempted on a privileged object. • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Name of the object to be processed (\BaseNamedObjects\LOADPERF_MUTEX) • **Object > Object Server**: Service that executed the process • **Requested operation > Privileges**: Requested privileges (SeTakeOwnershipPrivilege) • **Process Information > Process Name**: Path to the executable file (C:\Windows\System32\wbem\WmiPrvSE.exe) • **Object > Object Type**: Type of the object to be processed (Mutant) • **Subject > Logon ID**: Session ID of the user who executed the process
	Security	4674	Sensitive Privilege Use	An operation was attempted on a privileged object. • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Name of the object to be processed • **Object > Object Server**: Service that executed the process • **Requested operation > Privileges**: Requested privileges (SeTakeOwnershipPrivilege) • **Process Information > Process Name**: Path to the executable file (C:\Windows\System32\wbem\WmiPrvSE.exe) • **Object > Object Type**: Type of the object to be processed • **Subject > Logon ID**: Session ID of the user who executed the process
17	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. • **Protocol**: Protocol (tcp) • **DestinationIp**: Destination IP address (source host IP address) • **Image**: Path to the executable file (System) • **DestinationHostname**: Destination host name (source host name) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **DestinationPort**: Destination port number (high port) • **SourcePort**: Source port number (5985) • **SourceHostname**: Source host name (destination host name) • **SourceIp**: Source IP address (destination host IP address)
18	Microsoft-Windows-Sysmon/Operational	12	Registry object added or deleted (rule: RegistryEvent)	Registry object added or deleted. • **EventType**: Process type (CreateKey) • **Image**: Path to the executable file (C:\Windows\system32\wsmprovhost.exe) • **ProcessGuid/ProcessId**: Process ID • **TargetObject**: Created/deleted registry key/value (\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters)
19	Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	Process Create. • **LogonGuid/LogonId**: ID of the logon session • **ParentProcessGuid/ParentProcessId**: Process ID of the parent process • **ParentImage**: Executable file of the parent process (C:\Windows\System32\svchost.exe) • **CurrentDirectory**: Work directory (C:\Windows\system32\) • **CommandLine**: Command line of the execution command (C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding) • **IntegrityLevel**: Privilege level (System) • **ParentCommandLine**: Command line of the parent process (C:\Windows\system32\svchost.exe -k DcomLaunch) • **UtcTime**: Process execution date and time (UTC) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\NETWORK SERVICE) • **Hashes**: Hash value of the executable file • **Image**: Path to the executable file (C:\Windows\System32\wbem\WmiPrvSE.exe)

20	Microsoft-Windows-Sysmon/Operational	12	Registry object added or deleted (rule: RegistryEvent)	Registry object added or deleted. • **EventType**: Process type (CreateKey) • **Image**: Path to the executable file (C:\Windows\system32\wsmprovhost.exe) • **ProcessGuid/ProcessId**: Process ID • **TargetObject**: Created/deleted registry key/value (\REGISTRY\MACHINE\SOFTWARE\Microsoft\WBEM)
21	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. • **Protocol**: Protocol (tcp) • **DestinationIp**: Destination IP address (source host IP address) • **Image**: Path to the executable file (System) • **DestinationHostname**: Destination host name (source host name) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **DestinationPort**: Destination port number (high port) • **SourcePort**: Source port number (5985) • **SourceHostname**: Source host name (destination host name) • **SourceIp**: Source IP address (destination host IP address)
22	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (including WriteData or AddFile, and AppendData) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name (C:\Windows\Prefetch\WSMPROVHOST.EXE-[RANDOM].pf) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\svchost.exe) • **Object > Object Type**: Type of the file (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4663	File System	An attempt was made to access an object. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (WriteData or AddFile, AppendData) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name (C:\Windows\Prefetch\WSMPROVHOST.EXE-[RANDOM].pf) • **Audit Success**: Success or failure (access successful) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\svchost.exe) • **Object > Object Type**: Category of the target (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4673	Sensitive Privilege Use	A privileged service was called. • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Process > Process ID**: ID of the process that used the privilege • **Subject > Logon ID**: Session ID of the user who executed the process • **Service Request Information > Privilege**: Privileges used (SeTcbPrivilege) • **Process > Process Name**: Process that used the privileges (C:\Windows\System32\wsmprovhost.exe)
	Security	4673	Sensitive Privilege Use	A privileged service was called.

				• **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Process > Process ID**: ID of the process that used the privilege • **Subject > Logon ID**: Session ID of the user who executed the process • **Service Request Information > Privilege**: Privileges used (SeTcbPrivilege) • **Process > Process Name**: Process that used the privileges (C:\Windows\System32\wsmprovhost.exe)
23	Security	4634	Logoff	An account was logged off. • **Logon Type**: Logon path, method, etc. (3=Network) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the authentication
	Security	4634	Logoff	An account was logged off. • **Logon Type**: Logon path, method, etc. (3=Network) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the authentication
	Security	4634	Logoff	An account was logged off. (An account was logged off.) • **Logon Type**: Logon path, method, etc. (3=Network) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the authentication
24	Microsoft-Windows-WinRM/Operational	83	Processing of Request	Coming out of the plug-in for executing the operation [Operation]. • **Operation**: Requested process (Send)
	Microsoft-Windows-WinRM/Operational	134	Response Processing	Sending response for operation [Operation] • **Operation**: Process performed (Receive)
	Microsoft-Windows-WinRM/Operational	192	User Approval	Authorizing the user • **Error**: Error code
	Microsoft-Windows-WinRM/Operational	81	Processing of Request	Processing client request for operation [Operation]. • **Operation**: Requested process (Signal)
	Microsoft-Windows-WinRM/Operational	82	Processing of Request	Entering the plug-in for executing the operation [Operation]. ResourceURI <[URL]> is used (entering the plug-in for executing the Signal operation. ResourceURI schemas.microsoft.com/powershell/Microsoft.PowerShell> is used.) • **URL**: URL of the resource (http://schemas.microsoft.com/powershell/Microsoft.PowerShell) • **Operation**: Requested process (Signal)
	Microsoft-Windows-WinRM/Operational	134	Response Processing	Sending response for operation [Operation] • **Operation**: Process performed (Signal)
	Microsoft-Windows-WinRM/Operational	83	Processing of Request	Coming out of the plug-in for executing the operation [Operation]. • **Operation**: Requested process (Signal)
	Microsoft-Windows-WinRM/Operational	192	User Approval	Authorizing the user • **Error**: Error code
	Microsoft-Windows-WinRM/Operational	81	Processing of Request	Processing client request for operation [Operation].

				• **Operation**: Requested process (DeleteShell)
	Microsoft-Windows-WinRM/Operational	82	Processing of Request	Entering the plug-in for executing the operation [Operation]. ResourceURI <[URL]> is used. • **URL**: URL of the resource (http://schemas.microsoft.com/powershell/Microsoft.PowerShell) • **Operation**: Requested process (DeleteShell)
	Microsoft-Windows-WinRM/Operational	141	Response Processing	Sending the operation timeout response: [Operation] • **Operation**: Process performed (Receive)
	Microsoft-Windows-WinRM/Operational	83	Processing of Request	Coming out of the plug-in for executing the operation [Operation]. • **Operation**: Requested process (DeleteShell)
	Microsoft-Windows-WinRM/Operational	134	Response Processing	Sending response for operation [Operation] • **Operation**: Process performed (Receive)
	Microsoft-Windows-WinRM/Operational	134	Response Processing	Sending response for operation [Operation] • **Operation**: Process performed (DeleteShell)
25	Security	4689	Process Termination	A process has exited. • **Process Information > Process ID**: Process ID (hexadecimal) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Process Information > Exit Status**: Process return value (0x0) • **Log Date and Time**: Process terminated date and time (local time) • **Process Information > Process Name**: Path to the executable file (C:\Windows\System32\wsmprovhost.exe) • **Subject > Logon ID**: Session ID of the user who executed the process
	Microsoft-Windows-Sysmon/Operational	5	Process terminated (rule: ProcessTerminate)	Process terminated. • **UtcTime**: Process terminated date and time (UTC) • **ProcessGuid/ProcessId**: Process ID • **Image**: Path to the executable file (C:\Windows\System32\wsmprovhost.exe)
26	Security	4689	Process Termination	A process has exited. • **Process Information > Process ID**: Process ID (hexadecimal) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Process Information > Exit Status**: Process return value (0x0) • **Log Date and Time**: Process terminated date and time (local time) • **Process Information > Process Name**: Path to the executable file (C:\Windows\System32\wbem\WmiPrvSE.exe) • **Subject > Logon ID**: Session ID of the user who executed the process
	Microsoft-Windows-Sysmon/Operational	5	Process terminated (rule: ProcessTerminate)	Process terminated. • **UtcTime**: Process terminated date and time (UTC) • **ProcessGuid/ProcessId**: Process ID • **Image**: Path to the executable file (C:\Windows\System32\wbem\WmiPrvSE.exe)

- **USN Journal**

#	File Name	Process	Attribute

1	WSMPROVHOST.EXE-[RANDOM].pf	FILE_CREATE	archive+not_indexed

- **MFT**

#	Path	Header Flag	Validity
1	[Drive Name]:\Windows\Prefetch\WSMPROVHOST.EXE-[RANDOM].pf	FILE	ALLOCATED

- **Prefetch**

#	Prefetch File	Process Name	Process Path	Information That Can Be Confirmed
1	WSMPROVHOST.EXE-[RANDOM].pf	WSMPROVHOST.EXE	C:\WINDOWS\SYSTEM32\WSMPROVHOST.EXE	Last Run Time (last execution date and time)

- Details: Domain Controller

- **Event Log**

#	Event Log	Event ID	Task Category	Event Details
1	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. • **Protocol**: Protocol (tcp) • **DestinationIp**: Destination IP address (destination host IP address) • **Image**: Path to the executable file (C:\Windows\System32\lsass.exe) • **DestinationHostname**: Destination host name (destination host name) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **DestinationPort**: Destination port number (high port) • **SourcePort**: Source port number (88) • **SourceHostname**: Source host name (Domain Controller host name) • **SourceIp**: Source IP address (Domain Controller IP address)
	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. • **Network Information > Destination Port**: Destination port number (high port) • **Network Information > Source Port**: Source port number (88) • **Network Information > Destination Address**: Destination IP address (destination host) • **Network Information > Protocol**: Protocol used (6=TCP) • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\lsass.exe) • **Network Information > Direction**: Communication direction (inbound) • **Network Information > Source Address**: Source IP address (Domain Controller) • **Application Information > Process ID**: Process ID
2	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. • **Protocol**: Protocol (tcp) • **DestinationIp**: Destination IP address (destination host IP address) • **Image**: Path to the executable file (C:\Windows\System32\lsass.exe) • **DestinationHostname**: Destination host name (destination host name)

				• **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **DestinationPort**: Destination port number (high port) • **SourcePort**: Source port number (88) • **SourceHostname**: Source host name (Domain Controller host name) • **SourceIp**: Source IP address (Domain Controller IP address)
	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. • **Network Information > Destination Port**: Destination port number (high port) • **Network Information > Source Port**: Source port number (88) • **Network Information > Destination Address**: Destination IP address (destination host) • **Network Information > Protocol**: Protocol used (6=TCP) • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\lsass.exe) • **Network Information > Direction**: Communication direction (inbound) • **Network Information > Source Address**: Source IP address (Domain Controller) • **Application Information > Process ID**: Process ID
3	Security	4768	Kerberos Authentication Service	A Kerberos authentication ticket (TGT) was requested. • **Network Information > Client Address**: Source IP address that requested the ticket (destination host IP address) • **Account Information > Supplied Realm Name**: Domain of the account • **Additional Information > Ticket Option**: Ticket settings (0x40810010) • **Account Information > Account Name**: Name of the account from which the ticket was requested • **Additional Information > Result Code**: Ticket processing result (0x0) • **Network Information > Client Port**: Source port number of the ticket request (high port) • **Account Information > User ID**: SID of the account
4	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. • **Protocol**: Protocol (tcp) • **DestinationIp**: Destination IP address (destination host IP address) • **Image**: Path to the executable file (C:\Windows\System32\lsass.exe) • **DestinationHostname**: Destination host name (destination host name) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **DestinationPort**: Destination port number (high port) • **SourcePort**: Source port number (88) • **SourceHostname**: Source host name (Domain Controller host name) • **SourceIp**: Source IP address (Domain Controller IP address)
	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. • **Network Information > Destination Port**: Destination port number (high port) • **Network Information > Source Port**: Source port number (88) • **Network Information > Destination Address**: Destination IP address (destination host) • **Network Information > Protocol**: Protocol used (6=TCP) • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\lsass.exe) • **Network Information > Direction**: Communication direction (inbound) • **Network Information > Source Address**: Source IP address (Domain Controller) • **Application Information > Process ID**: Process ID
5	Security	4769	A Kerberos service ticket was requested	A Kerberos service ticket was requested.

				• **Network Information > Client Address**: Source IP address that requested the ticket (source host) • **Account Information > Account Domain**: Domain of the account • **Account Information > Account Name**: Name of the account from which the ticket was requested • **Additional Information > Ticket Option**: Ticket settings (0x40810010) • **Additional Information > Error Code**: Ticket processing result (0x0) • **Service Information > Service Name**: Service name of the ticket • **Account Information > Logon GUID**: Session ID of the logon • **Service Information > Service ID**: SID of the service • **Network Information > Client Port**: Source port number of the ticket request (high port)
6	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. • **Protocol**: Protocol (tcp) • **DestinationIp**: Destination IP address (destination host IP address) • **Image**: Path to the executable file (C:\Windows\System32\lsass.exe) • **DestinationHostname**: Destination host name (destination host name) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **DestinationPort**: Destination port number (high port) • **SourcePort**: Source port number (88) • **SourceHostname**: Source host name (Domain Controller host name) • **SourceIp**: Source IP address (Domain Controller IP address)
	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. • **Network Information > Destination Port**: Destination port number (high port) • **Network Information > Source Port**: Source port number (88) • **Network Information > Destination Address**: Destination IP address (destination host) • **Network Information > Protocol**: Protocol used (6=TCP) • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\lsass.exe) • **Network Information > Direction**: Communication direction (inbound) • **Network Information > Source Address**: Source IP address (Domain Controller) • **Application Information > Process ID**: Process ID
7	Security	4769	A Kerberos service ticket was requested	A Kerberos service ticket was requested. • **Network Information > Client Address**: Source IP address that requested the ticket (source host) • **Account Information > Account Domain**: Domain of the account • **Account Information > Account Name**: Name of the account from which the ticket was requested • **Additional Information > Ticket Option**: Ticket settings (0x40810010) • **Additional Information > Error Code**: Ticket processing result (0x0) • **Service Information > Service Name**: Service name of the ticket • **Account Information > Logon GUID**: Session ID of the logon • **Service Information > Service ID**: SID of the service • **Network Information > Client Port**: Source port number of the ticket request (high port)
8	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. • **Protocol**: Protocol (tcp) • **DestinationIp**: Destination IP address (destination host IP address) • **Image**: Path to the executable file (C:\Windows\System32\lsass.exe) • **DestinationHostname**: Destination host name (destination host name) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **DestinationPort**: Destination port number (high port) • **SourcePort**: Source port number (88)

				• **SourceHostname**: Source host name (Domain Controller host name) • **SourceIp**: Source IP address (Domain Controller IP address)
	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. • **Network Information > Destination Port**: Destination port number (high port) • **Network Information > Source Port**: Source port number (88) • **Network Information > Destination Address**: Destination IP address (destination host) • **Network Information > Protocol**: Protocol used (6=TCP) • **Application Information > Application Name**: Execution process • **Network Information > Direction**: Communication direction (inbound) • **Network Information > Source Address**: Source IP address (Domain Controller) • **Application Information > Process ID**: Process ID