**Usecase 3: PowerShell Usage**

Objective: Detect usage of PowerShell

Log Source: Windows Sysmon

Event ID: Sysmon ID 1: Process Creation

Example Target Log From Event Viewer:

Process Create:

RuleName: technique\_id=T1204,technique\_name=User Execution

UtcTime: 2025-06-30 22:13:58.574

ProcessGuid: {0430377a-0c26-6863-fd10-000000001d00}

ProcessId: 22660

Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

FileVersion: 10.0.26100.3323 (WinBuild.160101.0800)

Description: Windows PowerShell

Product: Microsoft® Windows® Operating System

Company: Microsoft Corporation

OriginalFileName: PowerShell.EXE

CommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"

CurrentDirectory: C:\Users\<username>\

User: <system name>\<username>

LogonGuid: {0430377a-884e-685d-13c1-620300000000}

LogonId: 0x362C113

TerminalSessionId: 2

IntegrityLevel: Medium

Hashes: SHA1= <hash string>

ParentProcessGuid: {0430377a-8850-685d-4a06-000000001d00}

ParentProcessId: 17992

ParentImage: C:\Windows\explorer.exe

ParentCommandLine: C:\WINDOWS\Explorer.EXE

Pre-configuration: Sysmon set up, after installation run these commands as admin in powershell: cd ‘C:\Sysmon\’ (or wherever Sysmon is installed) > wget https://wazuh.com/resources/blog/emulation-of-attack-techniques-and-detection-with-wazuh/sysmonconfig.xml -Outfile sysmonconfig.xml > then .\Sysmon.exe (or wherever Sysmon.exe is installed) -accepteula -I .\sysmonconfig.xml (or wherever sysmonconfig.xml is installed)

Then need to configure agent log collection for Sysmon by adding this to the local agent configuration

A black background with white text

Description automatically generated

Custom Wazuh Rule:

A computer code on a black background

AI-generated content may be incorrect.

Filters the default 61603 for powershell occurrences using eventdata.image contains powershell.exe

A screen shot of a computer code

AI-generated content may be incorrect.

Because 61603 already filters for event ID 1 events, no further filtering is required other than for the image

Example Alerts:

A black background with white text

AI-generated content may be incorrect.

Verification of fields:

A screenshot of a computer

AI-generated content may be incorrect.

While it seems the image filtering is unsuccessful on first glance we can see both are different paths to powershell so both are successful.