RULE WIZARD RULE1:-

|  |  |
| --- | --- |
| Rule Description | |
|  | Apply sysmon Encoded PowerShell Detection on events which are detected by the Local system and when the event matches UTF8(payload) ILIKE '%Sysmon%' AND ( UTF8(payload) ILIKE '%powershell%' AND (UTF8(payload) ILIKE '%-enc%' OR UTF8(payload) ILIKE '%EncodedCommand%') ) AQL filter query |
|  | |
| Rule Responses | |
|  | * Dispatch New Event   + Event Name: Encoded PowerShell detected on endpoint   + Event Description: Description -----Encoded PowerShell detected on endpoint   + Severity: 6 Credibility: 10 Relevance: 10   + High-Level Category: Access   + Low-Level Category: Access Denied   + Annotate the offense with MITRE\_TACTICS: Execution, Defense Evasion MITRE\_TECHNIQUES: T1059.001, T1027   + Force the dispatched event to create a NEW offense, select the offense using Event Name * Add Source IP to Reference Set: suspicious Endpoints |
| This Rule will be: Enabled | |

TO TRIGGER THIS OFFENSE ON POWERSHELL:-

PS C:\WINDOWS\system32> $command = "Write-Host 'Hello from Encoded PowerShell'"

PS C:\WINDOWS\system32> $bytes = [System.Text.Encoding]::Unicode.GetBytes($command)

PS C:\WINDOWS\system32> $encoded = [Convert]::ToBase64String($bytes)

PS C:\WINDOWS\system32> $encoded

VwByAGkAdABlAC0ASABvAHMAdAAgACcASABlAGwAbABvACAAZgByAG8AbQAgAEUAbgBjAG8AZABlAGQAIABQAG8AdwBlAHIAUwBoAGUAbABsACcA

PS C:\WINDOWS\system32>

PS C:\WINDOWS\system32>

PS C:\WINDOWS\system32> powershell -enc VwByAGkAdABlAC0ASABvAHMAdAAgACcASABlAGwAbABvACAARgByAG8AbQAgAEUAbgBjAG8AZABlAGQAIABQAG8AdwBlAHIAUwBoAGUAbABsACcA

RULE WIZARD RULE2

|  |  |
| --- | --- |
| Rule Description | |
|  | Apply Sysmon Process Create event on events which are detected by the Local system and when the event matches UTF8(payload) ILIKE '%sysmon%' AND (UTF8(payload) ILIKE '%downloads%' OR UTF8(payload) ILIKE '%Temp%') AQL filter query |
|  | |
| Rule Responses | |
|  | * Dispatch New Event   + Event Name: Suspicious execution from download/Temp folder   + Event Description: Description----Suspicious execution from Temp/folder   + Severity: 5 Credibility: 10 Relevance: 10   + High-Level Category: Access   + Low-Level Category: Access Denied   + Annotate the offense with MITRE\_TACTICS: Execution, Initial Access MITRE\_TECHNIQUES: T1204.002, T1105   + Force the dispatched event to create a NEW offense, select the offense using Event Name * Add Source IP to Reference Set: Suspicious\_Behavior |
| This Rule will be: Enabled | |

TO TRIGGER THIS OFFENSE ON POWERSHELL:-

PS C:\WINDOWS\system32>

>> .\notepad.exe

>> copy C:\Windows\System32\notepad.exe .

>> cd $env:USERPROFILE\Downloads

RULE WIZARD RULE3

|  |  |
| --- | --- |
| Rule Description | |
|  | Apply sysmon event Network Connect on events which are detected by the Local system and when the destination port is one of the following 80, 443, 53 and when the event matches UTF8(payload) ILIKE '%Network connection detected%' AND (UTF8(payload) ILIKE '%powershell.exe%' or UTF8(payload) ILIKE '%cmd.exe%') AQL filter query |
|  | |
| Rule Responses | |
|  | * Dispatch New Event   + Event Name: Unexpected network connection from CLI process.   + Event Description: description-----Unexpected network connection from CLI process.   + Severity: 1 Credibility: 0 Relevance: 0   + High-Level Category: Access   + Low-Level Category: Access Denied   + Annotate the offense with MITRE\_TACTICS: Command and Control MITRE\_TECHNIQUES: T1071.001, T1059   + Force the dispatched event to create a NEW offense, select the offense using Event Name |
| This Rule will be: Enabled | |

TO TRIGGER THIS OFFENSE ON POWERSHELL:-

PS C:\Users\saman\Downloads> powershell.exe -NoProfile -Command "Invoke-WebRequest google.com"