Scenario 5: Detecting Suspicious PowerShell Activity

Step 1: Update Sysmon Configuration to Log PowerShell Activity

```
PS C:\users\windows\Downloads> Get-ItemProperty -Path "HKLM:\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging"

>> Get-ItemProperty -Path "HKLM:\Software\Policies\Microsoft\Windows\PowerShell\ModuleLogging"

EnableModuleLogging : 1

ModuleNames : *

PSPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ModuleLogging

PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell

PSChildName : ModuleLogging

PSDrive : MKLM

PSProvider : Microsoft.PowerShell.Core\Registry
```

Step 2: Simulate Suspicious PowerShell Execution

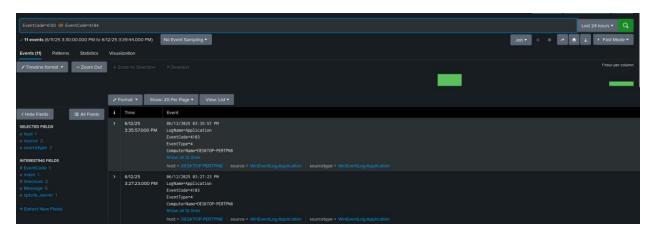
- Run this PowerShell script:
- Invoke-Expression -Command "Get-Process | Where-Object { \$_.CPU -gt 100 }"

Step 3: What should happen:

If logging is correctly set:

- You should see logs for this command in:
- index=winlogs EventCode=4103 OR EventCode=4104

Event ID 4104 (Script Block Logging)



Event ID 4103 (Module Logging)



Step 4 : Analyze PowerShell Logs in Splunk & Create Detection Alerts

