

## 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\PowerS
                    hell\ModuleLogging
PSParentPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerS
                    hell
PSChildName         : ModuleLogging
PSDrive             : HKLM
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)**

The screenshot shows the Splunk search results interface. At the top, the search criteria are 'EventCode=4103' and 'EventCode=4104'. The results show 11 events. The first event is for EventCode=4104, occurring on 6/12/25 at 3:35:57 PM. The details for this event are: LogName=Application, EventCode=4104, EventType=4, ComputerName=DESKTOP-PERTPN8. The second event is for EventCode=4103, occurring on 6/12/25 at 3:27:23 PM. The details for this event are: LogName=Application, EventCode=4103, EventType=4, ComputerName=DESKTOP-PERTPN8.

- **Event ID 4103 (Module Logging)**

The screenshot shows the Splunk search results interface. The first event is for EventCode=4104, occurring on 6/12/25 at 3:26:54 PM. The details for this event are: LogName=Application, EventCode=4104, EventType=4, ComputerName=DESKTOP-PERTPN8. The second event is for EventCode=4625, occurring on 6/12/25 at 8:30:04 AM. The details for this event are: LogName=Security, EventCode=4625, EventType=0, ComputerName=DESKTOP-PERTPN8.

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

The screenshot shows the Splunk Enterprise interface for configuring a detection alert. The alert is titled 'Detection suspicious activity alert'. It is enabled and has a trigger condition of 'Number of Results is > 5'. The alert is scheduled weekly on Monday at 6:00. The alert type is 'Scheduled, Weekly, Monday at 6:00'. The alert is owned by 'splunk\_admin' and has permissions set to 'Private'.