SOC Use Case Report

UC-007: Suspicious PowerShell Commands

Author	Abishek V
Date	22 January 2026
Environment	Home SOC Lab (VirtualBox)
Primary Logs	Windows Security Event Logs / PowerShell Logs
Target OS	Windows 10

1. Use Case Summary

Use Case ID	UC-007
Use Case Name	Suspicious PowerShell Commands
Category	Execution / Defense Evasion
SOC Tier	L1 (Triage + Investigation + Escalation)
Severity Guideline	Medium → High

PowerShell is frequently abused for payload execution, download, and in-memory activity. SOC L1 must quickly determine whether PowerShell usage is administrative or malicious.

2. Scenario

- Endpoint: Windows 10 (`192.168.56.110`)
- User context: `clair`
- Source system: Kali Linux (`192.168.56.120`)
- Execution type: Interactive PowerShell session

> **SOC risk point:** Encoded commands, hidden windows, and download/execution patterns are strong indicators of malicious PowerShell activity.

3. Telemetry and Evidence

Primary logs

- Windows Security Event Logs
- PowerShell Operational Logs

Key Event IDs

4688	Process creation (`powershell.exe`)
4104	PowerShell script block logging
4103	PowerShell module logging
4624	Associated logon session

4. Detection Logic

Trigger when:

- PowerShell executed with suspicious arguments
- Encoded or obfuscated commands detected
- PowerShell used to download or execute remote content

High-risk indicators:

- `-EncodedCommand`
- `IEX` / `Invoke-Expression`
- `DownloadString` / `WebClient`
- Hidden or non-interactive execution

5. SOC L1 Playbook

Phase A: Triage

1. Confirm PowerShell execution event
2. Identify command-line arguments
3. Identify user and host context

Phase B: Investigation

1. Review full command line and script block content
2. Decode encoded commands if present
3. Validate user intent (admin task vs suspicious)
4. Check for network activity or follow-on processes
5. Scope for similar PowerShell usage on other hosts

6. Evidence Timeline

Time	Event ID	Entity	Observation
11:04:18	4688	powershell.exe	PowerShell launched with encoded command
11:04:19	4104	ScriptBlock	Encoded payload decoded in memory
11:04:22	4688	cmd.exe	Child process spawned
11:05:10	4624	clair	Active user session confirmed

Outcome: PowerShell executed with encoded command and suspicious follow-on activity. Escalation required.

7. False Positive Checks

- legitimate admin script using encoded command
- enterprise automation task
- known management tooling

8. Verdict Criteria

True Positive if:

- obfuscation or encoded execution observed
- download or in-memory execution detected
- user cannot justify command usage

Suspicious PowerShell execution should be escalated when intent cannot be validated.

9. SOC Response Actions

- isolate endpoint if malicious behavior confirmed
- block malicious script or hash

- reset credentials if compromise suspected
- review PowerShell usage across environment

10. Ticket Notes

Ticket: UC-007 Suspicious PowerShell Execution
Severity: High
Verdict: Escalation required

Analyst Notes

- Detected PowerShell execution with encoded command under user `clair`.
- Script block logging confirmed obfuscated content and child process execution.
- Activity classified as suspicious execution. Escalated for deeper analysis.