SOC Use Case Report

UC-010: Suspicious Arguments

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

1. Use Case Summary

Use Case ID	UC-010
Use Case Name	Suspicious Arguments
Category	Execution / Defense Evasion
SOC Tier	L1 (Triage + Investigation)
Severity Guideline	Medium → High

Suspicious arguments are command-line parameters commonly abused to hide execution, bypass controls, or load malicious content. SOC L1 must evaluate argument intent rather than the binary alone.

2. Scenario

- Endpoint: Windows 10 (`192.168.56.110`)
- User account: `clair`
- Process observed: `powershell.exe`
- Execution context: Interactive user session

SOC risk point: Many attacks rely on trusted binaries with malicious arguments rather than custom malware.

3. Telemetry and Evidence

Primary logs

- Windows Security Event Logs

Key Event IDs

4688	Process creation (arguments captured)
4624	Associated logon session

4. Detection Logic

Trigger when:

- suspicious arguments are passed to trusted binaries
- arguments indicate obfuscation, download, or bypass behavior

High-risk arguments include:

- `-EncodedCommand`
- `-NoProfile`
- `-ExecutionPolicy Bypass`
- `/c` chained commands
- hidden or window suppression flags

5. SOC L1 Playbook

Phase A: Triage

1. Identify binary and full argument list
2. Identify user and host context
3. Determine whether arguments are expected for the role

Phase B: Investigation

1. Review argument purpose and intent
2. Decode or expand encoded parameters if present
3. Validate execution intent with user/IT
4. Review spawned child processes
5. Review network activity following execution

6. Evidence Timeline

Time	Event ID	Entity	Observation
18:11:24	4688	powershell.exe	Executed with -EncodedCommand argument
18:11:26	4688	rundll32.exe	Child process spawned
18:12:02	4624	clair	Active user session confirmed

Outcome: Trusted binary executed with suspicious arguments and follow-on behavior. Escalation required.

7. False Positive Checks

- approved automation scripts
- enterprise deployment tools
- known administrative workflows

8. Verdict Criteria

True Positive if:

- arguments clearly indicate obfuscation or bypass
- no legitimate operational justification exists
- follow-on suspicious activity observed

Suspicious arguments on trusted binaries should be escalated when intent cannot be validated.

9. SOC Response Actions

- isolate endpoint if malicious intent confirmed
- block associated scripts or hashes
- reset credentials if compromise suspected
- tune detections to reduce benign noise

10. Ticket Notes

Ticket: UC-010 Suspicious Arguments Detected
Severity: High
Verdict: Escalation required

Analyst Notes

- Detected execution of trusted binary with suspicious arguments indicating possible obfuscation.
- Follow-on child process activity observed.
- Activity classified as suspicious execution and escalated for further analysis.