SOC Use Case Report

UC-009: Unusually Long Command Line Strings

Author	Abishek V
Date	28 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-009
Use Case Name	Unusually Long Command Line Strings
Category	Execution / Obfuscation
SOC Tier	L1 (Triage + Investigation)
Severity Guideline	Medium → High

Attackers often use very long command lines to hide payloads, encoded content, or chained commands. SOC L1 must determine whether the command length is justified or indicative of obfuscation.

2. Scenario

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

SOC risk point: Excessively long command lines are commonly used to conceal encoded payloads or multiple execution stages.

3. Telemetry and Evidence

Primary logs

- Windows Security Event Logs

Key Event IDs

4688	Process creation (command line captured)
4624	Associated logon session

4. Detection Logic

Trigger when:

- command-line length exceeds defined baseline threshold
- command contains multiple chained arguments or obfuscated content

Common risk indicators:

- base64-encoded strings
- repeated use of escape characters
- excessive flags and nested commands

5. SOC L1 Playbook

Phase A: Triage

1. Identify process name and command-line length

2. Identify user and host context
3. Determine if the command is typical for the role

Phase B: Investigation

1. Review full command line content
2. Extract and decode encoded segments if present
3. Validate execution intent with user/IT if needed
4. Review child processes and network activity
5. Search for similar executions across environment

6. Evidence Timeline

Time	Event ID	Entity	Observation
17:22:41	4688	powershell.exe	PowerShell launched with long encoded command
17:22:42	4688	cmd.exe	Child process spawned
17:23:05	4624	clair	Active user session confirmed

Outcome: Command-line length exceeded baseline and contained encoded content. Escalation required.

7. False Positive Checks

- complex but legitimate automation scripts
- software installation commands
- enterprise deployment tooling

8. Verdict Criteria

True Positive if:

- command is obfuscated without clear justification
- encoded payloads or hidden execution identified
- suspicious follow-on activity observed

Unusually long command lines without clear operational purpose should be escalated.

9. SOC Response Actions

- isolate endpoint if malicious execution confirmed
- block associated hashes or scripts
- reset credentials if compromise suspected
- tune detection thresholds if false positives observed

10. Ticket Notes

Ticket: UC-009 Unusually Long Command Line
Severity: High
Verdict: Escalation required

Analyst Notes

- Detected PowerShell execution with command-line length exceeding baseline.
- Encoded segments identified within the command.
- Activity classified as suspicious execution and escalated for deeper analysis.