SOC Use Case Report

UC-014: Clear PowerShell Console Command History

Author	Abishek V
Date	30 January 2026
Environment	Home SOC Lab (VirtualBox)
Primary Logs	Windows Security Logs / PowerShell Logs
Target OS	Windows 10

1. Use Case Summary

Use Case ID	UC-014
Use Case Name	Clear PowerShell Console Command History
Category	Defense Evasion / Anti-Forensics
SOC Tier	L1 (Triage + Investigation + Escalation)
Severity Guideline	Medium → High

Clearing PowerShell command history is a common anti-forensic technique used to remove evidence of executed commands. This behavior is unusual for normal users and should be validated.

2. Scenario

- Endpoint: Windows 10 (`192.168.56.110`)
- User account: `clair`
- Tool used: PowerShell console
- Action observed: Command history cleared

SOC risk point: Clearing command history often occurs after suspicious PowerShell activity and may indicate an attempt to hide execution.

3. Telemetry and Evidence

Primary logs

- PowerShell Operational Logs
- Windows Security Event Logs

Key Event Sources

PowerShell Operational	Script block and engine activity
4688	Process creation (PowerShell)
4624	Associated logon session

4. Detection Logic

Trigger when:

- PowerShell history file is cleared or truncated
- Commands associated with history removal are executed

Common methods:

- `Clear-History`
- Deletion of `ConsoleHost_history.txt`
- Profile modification disabling history logging

5. SOC L1 Playbook

Phase A: Triage

1. Confirm PowerShell usage prior to history clearing
2. Identify user and host context
3. Determine timing relative to other alerts

Phase B: Investigation

1. Identify how history was cleared (command vs file deletion)
2. Review PowerShell activity prior to clearing
3. Check for encoded or suspicious commands earlier in session
4. Correlate with process creation or network activity
5. Scope for similar behavior on other endpoints

6. Evidence Timeline

Time	Event ID / Source	Entity	Observation
22:18:41	4688	powershell.exe	Interactive PowerShell session started
22:19:12	PS Operational	ScriptBlock	Suspicious commands executed
22:20:05	File System	ConsoleHost_history.txt	History file cleared
22:20:14	4624	clair	Active user session confirmed

Outcome: PowerShell command history cleared following suspicious activity. Escalation required.

7. False Positive Checks

- user intentionally clearing history for privacy (rare)
- troubleshooting or testing activity (must be confirmed)
- script execution during development work

8. Verdict Criteria

True Positive if:

- history cleared after suspicious PowerShell usage
- no legitimate explanation provided
- behavior aligns with other defense evasion indicators

Clearing PowerShell command history without justification should be escalated as anti-forensic behavior.

9. SOC Response Actions

- preserve remaining PowerShell and system logs
- review historical telemetry prior to clearing
- reset credentials if compromise suspected
- monitor endpoint for further suspicious behavior

10. Ticket Notes

Ticket: UC-014 PowerShell History Cleared
Severity: High
Verdict: Escalation required

Analyst Notes

- Observed PowerShell command history cleared during active user session.
- History clearing followed suspicious PowerShell activity.
- Classified as potential anti-forensic behavior and escalated for further investigation.