

SOC Use Case Report

UC-012: Clearing Windows Logs using wevtutil

Author	Abishek V
Date	29 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-012
Use Case Name	Clearing Windows Logs using wevtutil
Category	Defense Evasion / Log Tampering
SOC Tier	L1 (Triage + Investigation + Escalation)
Severity Guideline	High → Critical

Attackers commonly use the built-in utility `wevtutil.exe` to clear Windows logs and remove evidence of malicious activity. This activity is rarely legitimate on endpoints.

2. Scenario

- Endpoint: Windows 10 (192.168.56.110)
- User context: `clair`
- Utility used: `wevtutil.exe`
- Action: Security log cleared

SOC risk point: Use of `wevtutil` to clear logs strongly indicates intentional log tampering.

3. Telemetry and Evidence

Primary logs

- Windows Security Event Logs

Key Event IDs

4688	Process creation (<code>wevtutil.exe</code>)
1102	Audit log cleared
4624	Associated logon session

4. Detection Logic

Trigger when:

- `wevtutil.exe` is executed with clear arguments
- Event ID 1102 is observed shortly after execution

High-risk indicators:

- execution by non-administrative user
- log clear following suspicious activity
- repeated use across endpoints

5. SOC L1 Playbook

Phase A: Triage

1. Confirm execution of `wevtutil.exe`

2. Confirm Event ID 1102
3. Identify actor account and endpoint

Phase B: Investigation

1. Review command-line arguments used
2. Identify activity prior to log clear
3. Check for suspicious login or execution events
4. Scope for similar activity across environment

6. Evidence Timeline

Time	Event ID	Entity	Observation
20:12:55	4688	wevtutil.exe	Executed with clear-log argument
20:12:58	1102	Security Log	Audit log cleared
20:13:04	4624	clair	Active user session confirmed

Outcome: Windows Security log cleared using wevtutil without justification. Escalation required.

7. False Positive Checks

- approved maintenance or troubleshooting
- endpoint rebuild or imaging process
- forensic preparation with documented approval

8. Verdict Criteria

True Positive if:

- no approved change exists
- wevtutil used to clear logs
- activity aligns with other suspicious behavior

Use of `wevtutil` to clear logs should be escalated immediately as defense evasion.

9. SOC Response Actions

- preserve remaining system artifacts
- isolate endpoint if compromise suspected
- reset credentials for involved accounts
- initiate incident response procedures

10. Ticket Notes

Ticket: UC-012 wevtutil Log Clearing
Severity: Critical
Verdict: Escalation required

Analyst Notes

- Detected execution of `wevtutil.exe` followed by audit log clear (Event ID 1102).
- Activity occurred during active user session without authorization context.
- Classified as log tampering and escalated for incident response.