SOC Use Case Report

UC-011: Windows Audit Log Cleared

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-011
Use Case Name	Windows Audit Log Cleared
Category	Defense Evasion / Log Tampering
SOC Tier	L1 (Triage + Investigation + Escalation)
Severity Guideline	High → Critical

Clearing Windows audit logs is a high-risk action commonly used to remove evidence after malicious activity. Any unexpected audit log clear should be treated as suspicious until proven otherwise.

2. Scenario

- Endpoint: Windows 10 (`192.168.56.110`)
- User context: `clair`
- Action observed: Security event log cleared
- Execution context: Local interactive session

SOC risk point: Legitimate log clearing is rare on endpoints and usually limited to maintenance windows or forensic preparation.

3. Telemetry and Evidence

Primary logs

- Windows Security Event Logs

Key Event IDs

1102	Audit log cleared
4688	Process creation (if enabled)
4624	Associated logon session

4. Detection Logic

Trigger when:

- Event ID 1102 is generated on an endpoint
- Log clear occurs outside approved maintenance window

High-risk indicators:

- log cleared shortly after suspicious activity
- log clear performed by non-admin account
- repeated log clearing on multiple systems

5. SOC L1 Playbook

Phase A: Triage

1. Confirm Event ID 1102
2. Identify actor account and host
3. Identify timing relative to other alerts

Phase B: Investigation

1. Determine who cleared the logs (Subject fields)
2. Identify process used (if available)
3. Review activity before the log clear event
4. Check for suspicious logins, executions, or admin actions
5. Scope for similar log clear events across environment

6. Evidence Timeline

Time	Event ID	Entity	Observation
19:44:10	4688	wevtutil.exe	Log management utility executed
19:44:14	1102	Security Log	Audit log cleared
19:44:20	4624	clair	Active session confirmed

Outcome: Security audit log cleared without documented justification. Escalation required.

7. False Positive Checks

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

8. Verdict Criteria

True Positive if:

- no approved change exists
- activity followed suspicious behavior
- actor account or process is unexpected

Unauthorized audit log clearing should be escalated immediately as defense evasion.

9. SOC Response Actions

- preserve remaining logs and system state
- isolate endpoint if compromise suspected
- reset credentials associated with actor account
- initiate deeper forensic review

10. Ticket Notes

Ticket: UC-011 Windows Audit Log Cleared
Severity: Critical
Verdict: Escalation required

Analyst Notes

- Detected Security audit log clear event (Event ID 1102) on endpoint `192.168.56.110`.
- Log clear occurred during active user session without approval context.
- Activity classified as defense evasion and escalated for incident response.