SOC Use Case Report

UC-013: Windows Audit Log Tampering

Author	Abishek V
Date	30 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-013
Use Case Name	Windows Audit Log Tampering
Category	Defense Evasion / Log Integrity
SOC Tier	L1 (Triage + Investigation + Escalation)
Severity Guideline	High → Critical

Audit log tampering includes attempts to disable logging, modify audit policies, or interfere with log collection. Such actions are commonly associated with efforts to hide malicious activity.

2. Scenario

- Endpoint: Windows 10 (`192.168.56.110`)
- User context: `clair`
- Activity observed: Audit policy modification
- Execution context: Local interactive session

SOC risk point: Any unauthorized modification to audit policy or logging configuration should be treated as suspected defense evasion.

3. Telemetry and Evidence

Primary logs

- Windows Security Event Logs

Key Event IDs

4719	System audit policy changed
4902	Per-user audit policy table created
4907	Auditing settings changed
4688	Process creation (if enabled)
4624	Associated logon session

4. Detection Logic

Trigger when:

- audit policy is modified outside approved change windows
- logging categories are disabled or reduced

High-risk indicators:

- audit changes performed by non-IT user
- audit policy changes shortly after suspicious activity
- repeated audit modifications across endpoints

5. SOC L1 Playbook

Phase A: Triage

1. Confirm audit policy change event
2. Identify actor account and target host
3. Determine timing relative to other alerts

Phase B: Investigation

1. Review audit policy before and after change
2. Identify process or tool used to modify policy
3. Check for suspicious activity prior to change
4. Scope for similar audit changes on other systems

6. Evidence Timeline

Time	Event ID	Entity	Observation
21:06:42	4688	auditpol.exe	Audit policy tool executed
21:06:45	4719	Audit Policy	System audit policy modified
21:06:50	4624	clair	Active user session confirmed

Outcome: Audit policy modified without authorization. Activity classified as log tampering. Escalation required.

7. False Positive Checks

- approved security hardening activity
- compliance or audit configuration updates
- endpoint provisioning or baseline enforcement

8. Verdict Criteria

True Positive if:

- no approved change exists
- audit categories reduced or disabled
- activity aligns with other suspicious indicators

Unauthorized audit policy modification should be escalated immediately as defense evasion.

9. SOC Response Actions

- restore audit policy to baseline
- preserve system state and remaining logs
- isolate endpoint if compromise suspected
- initiate incident response procedures

10. Ticket Notes

Ticket: UC-013 Audit Log Tampering
Severity: Critical
Verdict: Escalation required

Analyst Notes

- Detected unauthorized audit policy modification (Event ID 4719).
- Audit policy change occurred during active user session without approval context.
- Activity classified as defense evasion and escalated for incident response.