AU.L2-3.3.8

Audit & Accountability

Audit Protection

"Protect audit information and audit logging tools from unauthorized access, modification, and deletion."

Objectives

[a]
Audit information is protected from unauthorized access.

[b]
Audit information is protected from unauthorized modification.

[c]
Audit information is protected from unauthorized deletion.

[d]
Audit logging tools are protected from unauthorized access.

[e]
Audit logging tools are protected from unauthorized modification.

[f]
Audit logging tools are protected from unauthorized deletion.

Key Discussion Points

Two Things to Protect:
Both the audit information itself AND the tools used to collect it must be protected — attackers go after both.

Access Restriction:
Only authorized personnel should be able to read, modify, or delete logs or the logging infrastructure.

Immutability is the Goal:
Logs should be append-only — users should not be able to edit or delete records, even admins with elevated privileges.

Forward to Central Repo:
Forwarding logs to a central server that standard users cannot access is the most common technical control.

Assessment Methods

EXAMINE

Audit and accountability policy; access control policy; procedures addressing protection of audit information; system security plan; system configuration settings; system audit logs and records; audit logging tools.

INTERVIEW

Personnel with audit and accountability responsibilities; personnel with information security responsibilities; system or network administrators; system developers.

TEST

Mechanisms implementing audit information protection.

AU.L2-3.3.8

AUDIT & ACCOUNTABILITY — Audit Protection

Plain English

What this control is really saying:

An attacker who compromises a system will often try to cover their tracks by deleting or modifying the logs. This control makes that much harder by protecting the logs from the people they're meant to track. If a regular user or even a local admin can delete audit records, the logs are worthless.

How it is used:

- Audit logs are forwarded in real time to a central SIEM — standard users have no access to the SIEM and cannot delete forwarded logs.
- Local logs on workstations are ACL-restricted to Administrators only — non-admin users cannot read, modify, or clear event logs.
- The SIEM is deployed on a dedicated server — only the security officer and IT admin have accounts on the SIEM platform.
- Audit logging tools (the SIEM agents) are protected by application whitelisting — they cannot be uninstalled by standard users.

Real World Example

The Scenario

Acme Defense uses Windows Event Logging and a basic log aggregator. The IT admin has a domain admin account and is also the person responsible for reviewing logs. Any of the five users with domain admin rights can access and clear logs.

What the assessor finds

All five domain admins can clear the Security log on any system. The log aggregator is on a shared server with no access controls — any domain user can browse to the logs folder. Three months of audit data was overwritten last month with no alert.

SPRS Score Impact

3.3.8 carries a point value of 3. Logs that can be deleted or modified by the people they're designed to monitor are not reliable evidence — this control is what gives your audit program legal and forensic credibility.

What Good Looks Like

Logs forwarded to central SIEM with restricted access, local log ACLs prevent user modification, SIEM access limited to security personnel, logging agents protected from uninstall, audit data backed up and encrypted.

Common Gaps

What assessors actually find in the field:

✗ **Users can clear logs**

Standard users can open Event Viewer and clear the Security log — audit evidence can be destroyed by anyone.

✗ **Logs only stored locally**

Logs reside only on the system being audited — a compromised system can overwrite its own evidence.

✗ **SIEM accessible to all admins**

All domain admins can access and delete records in the SIEM — no separation between admin and audit roles.

✗ **Logging agents unprotected**

Users can disable or uninstall logging agents — the audit infrastructure itself can be taken offline.

✗ **No backup of audit data**

Logs are not backed up — a storage failure or attacker action results in permanent loss of audit history.