AU.L2-3.3.5

Audit & Accountability

Audit Correlation

"Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity."

Objectives

[a]

Audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined.

[b]

Defined audit record review, analysis, and reporting processes are correlated.

Key Discussion Points

Not Silos:
Logs from different systems must be reviewed together — isolated review of each system in turn misses cross-system attack patterns.

Central Repository:
A SIEM or centralized log aggregator is the common solution — pulling logs to one place enables correlation.

Small Company Option:
Manual correlation with well-defined procedures is acceptable for small organizations — the guide specifically acknowledges this.

Extends 3.3.6:
3.3.5 defines the correlation process. 3.3.6 covers reduction and reporting. Both contribute to incident detection and response.

Assessment Methods

EXAMINE

Audit and accountability policy; procedures addressing audit record review, analysis, and reporting; system security plan; system configuration settings; procedures addressing investigation and response to suspicious activities; system audit logs across different repositories.

INTERVIEW

Personnel with audit record review, analysis, and reporting responsibilities; personnel with information security responsibilities.

TEST

Mechanisms supporting analysis and correlation of audit records; mechanisms integrating audit review, analysis, and reporting.

AU.L2-3.3.5

AUDIT & ACCOUNTABILITY — Audit Correlation

Plain English

What this control is really saying:

Reviewing each system's logs in isolation means you can miss an attack that spans multiple systems. An attacker who compromised the VPN, then a workstation, then the file server shows up across three separate logs — only correlation reveals the full picture.

How it is used:

- All log sources feed into a central SIEM — workstations, VPN gateway, file server, and email gateway logs are all collected in one place.
- The SIEM runs correlation rules that flag when the same source IP appears in VPN, workstation, and file server logs within a short time window.
- The IT admin reviews correlated alerts each morning — the procedure is documented and includes escalation to the security officer for anomalies.
- Small organizations without a SIEM use a weekly manual review process: all log exports are reviewed side-by-side against a defined checklist.

Real World Example

The Scenario

Acme Defense collects logs from five workstations and a file server. The IT admin reviews each system's Windows Event Viewer individually when something seems wrong. There is no SIEM and no documented review or correlation procedure.

What the assessor finds

No review or correlation process is documented. Logs are never looked at unless an incident is already known. The assessor pulls logs across three systems and identifies a pattern of failed logons on multiple machines on the same date — nobody had noticed.

SPRS Score Impact

3.3.5 carries a point value of 3. Siloed log review misses multi-system attack patterns — most sophisticated intrusions leave traces across multiple systems that only correlation reveals.

What Good Looks Like

Review, analysis, and reporting processes documented in SSP, logs from all CUI systems fed to central repository or SIEM, correlation rules defined, cross-system anomalies trigger investigation, findings documented and acted upon.

Common Gaps

What assessors actually find in the field:

✗ **Siloed log review**

Each system's logs are reviewed separately — nobody ever looks across systems simultaneously for related activity.

✗ **No process defined**

No documented procedure exists for how audit records should be reviewed, analyzed, and correlated.

✗ **No central repository**

Logs sit on individual systems — pulling them together for correlation requires manual effort that never happens.

✗ **SIEM deployed but unused**

A SIEM was deployed a year ago but no correlation rules are configured and nobody reviews its output.

✗ **Analysis not tied to response**

Logs are reviewed periodically but findings are never escalated or acted upon — analysis and response are disconnected.