AU.L2-3.3.6

Audit & Accountability

Reduction & Reporting

"Provide audit record reduction and report generation to support on-demand analysis and reporting."

Objectives

[a]

An audit record reduction capability that supports on-demand analysis is provided.

[b]

A report generation capability that supports on-demand reporting is provided.

Key Discussion Points

Raw Logs Are Unusable:
Raw audit logs are massive and noisy — reduction extracts meaningful security-relevant events without altering the originals.

On-Demand Capability:
The key word is 'on-demand' — personnel must be able to pull reduced data and reports immediately during an incident, not days later.

Reduction Tools:
SIEM dashboards, log management platforms, and data mining tools all satisfy this — even open-source solutions count.

Separate From Logging:
The reduction and reporting capability does not have to come from the same system that collects the logs.

Assessment Methods

EXAMINE

Audit and accountability policy; procedures addressing audit record reduction and report generation; system design documentation; system security plan; system configuration settings; audit record reduction, review, analysis, and reporting tools; system audit logs and records.

INTERVIEW

Personnel with audit record reduction and report generation responsibilities; personnel with information security responsibilities.

TEST

Audit record reduction and report generation capability.

AU.L2-3.3.6

AUDIT & ACCOUNTABILITY — Reduction & Reporting

Plain English

What this control is really saying:

Raw logs are thousands of lines of noise. Nobody can read them in real time during an incident. This control requires tools that can filter, summarize, and report on audit data on demand — so when the phone rings at 2 AM you can pull a useful report in minutes, not days.

How it is used:

- The SIEM provides pre-built and custom dashboards that reduce raw logs to security-relevant events — failed logons, privilege escalations, and large file transfers.
- The IT admin can generate an on-demand report of all CUI file access activity for any date range within minutes using the SIEM's report builder.
- Nightly backup events are filtered out of daily review reports — reducing noise so anomalies stand out.
- During incident response, the security officer can pull a reduced log report covering specific systems and timeframes within minutes.

Real World Example

The Scenario

Acme Defense uses a Windows Event Collector that aggregates logs from all workstations. The only way to query the logs is to open the Event Viewer directly on the collector. There is no search, filter, or report capability. Generating any useful output requires hours of manual work.

What the assessor finds

There is no reduction or reporting capability. Producing a report of all failed logons over the past 30 days would take an estimated 4 hours manually. During a live incident, actionable data cannot be produced in time to be useful.

SPRS Score Impact

3.3.6 carries a point value of 3. Without on-demand reduction and reporting, incident response is slowed to a crawl — attackers rely on defenders being unable to analyze data quickly enough to act.

What Good Looks Like

SIEM or log management tool deployed with pre-built security dashboards, on-demand report generation for any date range or system, routine events filtered out, reports available to security personnel during incidents within minutes.

Common Gaps

What assessors actually find in the field:

✗ **No reduction capability**

Raw logs are the only output — there is no mechanism to filter, summarize, or extract meaningful security events.

✗ **No on-demand reporting**

Reports require days of manual effort — during an incident, actionable data cannot be produced quickly enough.

✗ **SIEM with no reports**

A SIEM exists but no dashboards or reports have been configured — the data is collected but not accessible in usable form.

✗ **Logs not filtered for noise**

Routine events like backups and scheduled tasks flood the logs, burying actual security events.

✗ **Reports only for compliance**

Report generation exists but is only used for periodic compliance reviews — not available for on-demand incident response.