SI.L2-3.14.4

System & Information Integrity

Update Malicious Code Protection [CUI Data]

"Update malicious code protection mechanisms when new releases are available."

Objectives

[a]
Malicious code protection mechanisms are updated when new releases are available.

Key Discussion Points

Definitions + Engine:
Both signature definitions AND the protection engine itself must be updated — an outdated engine may have known vulnerabilities that undermine its own protection.

Automated = Daily:
Malware evolves daily — the practical standard is automatic definition updates at least once per day, not weekly or monthly manual updates.

Verify Success:
Configuring automatic updates is not sufficient — failed updates must be detected. The last successful update date should be monitored per system.

Users Cannot Disable:
Update configurations must be locked via MDM or group policy — user-initiated disablement of automatic updates creates undetected definition drift.

Assessment Methods

EXAMINE

System and information integrity policy; configuration management policy; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; system security plan; system configuration settings; scan results from malicious code protection mechanisms; system audit logs.

INTERVIEW

System or network administrators; personnel with information security responsibilities; personnel installing and maintaining the system; personnel with responsibility for malicious code protection.

TEST

Organizational processes for employing, updating, and configuring malicious code protection mechanisms; mechanisms supporting malicious code protection including updates and configurations; mechanisms supporting malicious code scanning.

SI.L2-3.14.4

SYSTEM & INFO INTEGRITY — Update Malicious Code Protection [CUI Data]

Plain English

What this control is really saying:

Malware evolves on an hourly basis. An anti-malware tool with last week's definitions may not recognize today's ransomware variant. This control requires that malicious code protection mechanisms — signature databases, reputation engines, and the software itself — be updated when new releases are available, which in practice means automated daily or more frequent updates.

How it is used:

- Endpoint protection software is configured for automatic definition updates — the update check runs at least daily and logs each successful update.
- The IT admin verifies definition currency monthly — the most recent update date for each protected system is confirmed and logged.
- Anti-malware software engine versions are updated when the vendor releases new versions — the update process is part of the standard patch management cycle.
- The SSP documents the anti-malware product in use, the definition update frequency, and the process for verifying updates completed successfully.

Real World Example

The Scenario

Acme Defense installed endpoint protection two years ago. The product was configured to update definitions automatically, but the update server license expired six months ago. Definitions on all CUI workstations are 180+ days old.

What the assessor finds

Ransomware deployed against the company used a variant first identified 90 days ago. The anti-malware tool with current definitions would have detected and blocked it. With 180-day-old definitions, the tool had no signature for the variant — it executed without detection.

SPRS Score Impact

3.14.4 carries a point value of 5. Anti-malware with outdated definitions provides false assurance — the tool reports clean scans on infected systems because it cannot detect variants it has never seen.

What Good Looks Like

Anti-malware definitions updated at least daily via automatic update, update success verified and logged, engine version current, update configuration locked to prevent user disablement, last update date monitored as part of security operations.

Common Gaps

What assessors actually find in the field:

✗ Definitions not updated

Anti-malware definitions have not been updated in 60+ days — malware variants released after the last update are not detectable.

✗ Manual updates, inconsistently applied

Updates require manual initiation — some systems were last updated three months ago while others are current.

✗ No update verification

Automatic updates are configured but nobody verifies they succeed — failed updates go undetected and endpoints may be running stale definitions.

✗ Engine version outdated

Definitions are current but the anti-malware engine itself has not been updated in years — known engine vulnerabilities remain unpatched.

✗ Updates disabled by users

Users on CUI workstations have disabled automatic updates to avoid performance impact — IT has no visibility into which systems are running outdated definitions.