SI.L2-3.14.5

System & Information Integrity

System & File Scanning [CUI Data]

"Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed."

Objectives

[a]
The frequency for malicious code scans is defined.

[b]
Malicious code scans are performed with the defined frequency.

[c]
Real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.

Key Discussion Points

Two Scan Types:
[a,b] periodic scheduled scans catch dormant malware already on disk; [c] real-time scans catch malware as it enters from email, downloads, and removable media.

Define the Frequency:
[a] requires the scan frequency to be defined — 'when convenient' is not a defined frequency. Daily or weekly scheduled scans with a documented policy satisfy [a].

External Sources Defined:
External sources include web downloads, email attachments, and removable media (USB drives) — all must be covered by real-time scanning, not just internet downloads.

Quarantine + Notify:
Detected malicious files should be quarantined automatically — and the security team notified. Silent detection with no action does not meet the intent of the control.

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.L2-3.14.5

SYSTEM & INFO INTEGRITY — System & File Scanning [CUI Data]

Plain English

What this control is really saying:

Having anti-malware installed is not the same as having it actively scan. This control requires two scanning modes: periodic full-system scans on a defined schedule (catching dormant malware already on the system), and real-time scanning of every file coming from outside — email attachments, web downloads, USB drives — before they execute.

How it is used:

- Anti-malware is configured for daily full-system scans — the scan frequency is documented in the SSP and scan logs confirm the schedule is maintained.
- Real-time protection is enabled on all CUI workstations — any file downloaded, opened, or copied from external media is scanned before execution.
- Email attachments are scanned at the gateway before delivery — suspicious attachments are quarantined and the IT admin is notified.
- USB drive access on CUI workstations triggers an automatic scan before files can be accessed — removable media is treated as an external source.

Real World Example

The Scenario

Acme Defense has anti-malware installed. Real-time protection was disabled by the IT admin six months ago because users complained it slowed down their machines. Weekly scheduled scans are configured but the last scan log entry is 11 weeks old.

What the assessor finds

An engineer downloads a malicious PDF from a phishing email. With real-time scanning disabled, the file downloads and executes without inspection. The payload installs a keylogger on the CUI workstation — the next scheduled scan would have caught it, but the scan hasn't run in 11 weeks.

SPRS Score Impact

3.14.5 carries a point value of 5. Real-time scanning is the primary defense against phishing and download-based attacks — the tool reports clean scans on infected systems because it cannot detect variants it has never seen.

What Good Looks Like

Periodic scan frequency defined in SSP and in anti-malware configuration, scans running on schedule with logs maintained, real-time protection enabled on all CUI endpoints, external sources include email, web downloads, and removable media, scan results reviewed and acted on.

Common Gaps

What assessors actually find in the field:

✗ No scan frequency defined

Anti-malware is installed but no policy defines how often periodic scans must run — [a] is not met and scan consistency cannot be verified.

✗ Scans not running on schedule

Policy requires weekly scans but scan logs show the last scan ran three months ago — [b] is not met.

✗ Real-time protection disabled

Periodic scans run on schedule but real-time protection is disabled to improve performance — files from email and USB execute without scanning.

✗ USB drives not scanned

Real-time protection covers downloads but not removable media — USB drives can introduce malware that is not scanned before execution.

✗ Scan results not reviewed

Scans run on schedule but results are never reviewed — detections are logged but no action is taken until a user reports a problem.