SI.L2-3.14.3

System & Information Integrity

Security Alerts & Advisories

"Monitor system security alerts and advisories and take action in response."

Objectives

[a]
Response actions to system security alerts and advisories are identified.

[b]
System security alerts and advisories are monitored.

[c]
Actions in response to system security alerts and advisories are taken.

Key Discussion Points

Three Requirements:
[a] define responses, [b] monitor sources, [c] act — all three are required. Monitoring without defined responses, or responses never taken, fails this control.

Reputable Sources:
CISA, US-CERT, vendor security mailing lists, and sector ISACs are the expected sources — subscribing to at least CISA is a baseline expectation.

Applicability Review:
Not every advisory applies to every organization — the review process must assess whether the alert is relevant to CUI systems before action is required.

Evidence of Response:
Assessors will ask to see records — the POAM entry, the change record, or the communication to staff that demonstrates the advisory triggered a real response.

Assessment Methods

EXAMINE

System and information integrity policy; procedures addressing security alerts, advisories, and directives; system security plan; records of security alerts and advisories.

INTERVIEW

Personnel with security alert and advisory responsibilities; system or network administrators; personnel with information security responsibilities; external organizations to whom alerts are disseminated.

TEST

Organizational processes for receiving, reviewing, and responding to security alerts and advisories; mechanisms supporting receipt, generation, and dissemination of security directives.

SI.L2-3.14.3

SYSTEM & INFO INTEGRITY — Security Alerts & Advisories

Plain English

What this control is really saying:

US-CERT, vendor security advisories, and CISA KEV entries are published constantly. This control requires that you receive them, review them for applicability to your systems, define what actions to take when relevant alerts arrive, and actually take those actions. A subscription that nobody reads satisfies none of the three objectives.

How it is used:

- The IT admin subscribes to CISA alerts, US-CERT advisories, and vendor security mailing lists — new alerts are reviewed weekly or immediately for critical advisories.
- Each alert is assessed for applicability — if a vulnerability affects a CUI system, it is entered into the POAM and assigned to the patch management schedule.
- The SSP documents the alert sources monitored, the review frequency, and the defined response actions for different severity levels.
- When a CISA emergency directive is issued, the IT admin reviews within 24 hours and initiates the required remediation action with documented evidence.

Real World Example

The Scenario

Acme Defense subscribed to CISA email alerts two years ago. The IT admin's inbox shows 312 unread CISA advisory emails. A CISA Known Exploited Vulnerability affecting the company's VPN was flagged in an advisory six weeks ago.

What the assessor finds

The VPN vulnerability identified in the CISA advisory was never patched — the advisory was never read. An assessor confirms the vulnerability is actively being exploited and the VPN is the entry point used in a recent unauthorized access event.

SPRS Score Impact

3.14.3 carries a point value of 1. CISA KEV entries represent vulnerabilities with confirmed active exploitation — an organization that monitors alerts but takes no action has no meaningful security benefit from the monitoring.

What Good Looks Like

Alert subscriptions active from CISA, US-CERT, and vendors, alerts reviewed on defined frequency, response actions documented for each severity level, applicable alerts trigger POAM entries and patch actions, evidence of review and response maintained.

Common Gaps

What assessors actually find in the field:

✗ **No alert subscriptions**

The organization does not subscribe to any security alert service — CISA KEV entries, vendor advisories, and emergency directives go unmonitored.

✗ **Subscribed but not reviewed**

The IT admin receives CISA email alerts but the inbox folder holds 400 unread messages — monitoring exists in form only, not in practice.

✗ **No response actions defined**

Alerts are received but no documented process defines what to do — [a] requires response actions to be identified before they are needed.

✗ **Alerts not acted on**

A CISA KEV entry affecting a CUI server was issued three months ago and is still unpatched — the alert was received but no action was taken.

✗ **Internal dissemination missing**

External alerts are reviewed by IT but never shared with affected system owners or management — relevant parties are not informed.