SI.L2-3.14.6

System & Information Integrity

Monitor Communications for Attacks

"Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks."

Objectives

[a]
The system is monitored to detect attacks and indicators of potential attacks.

[b]
Inbound communications traffic is monitored to detect attacks and indicators of potential attacks.

[c]
Outbound communications traffic is monitored to detect attacks and indicators of potential attacks.

Key Discussion Points

System + Inbound + Outbound:
All three must be monitored — [a] covers system-level events, [b] covers what enters the network, and [c] covers what leaves. Outbound is the most commonly missed.

Strategic Placement:
Monitoring devices belong at boundary points and near critical systems — a sensor that only covers part of the network leaves blind spots.

Indicators of Attack:
The guide specifies looking for attack indicators — unusual access patterns, after-hours activity, internal malware propagation, and data leaving the organization.

Feeds Incident Response:
Monitoring without a review process satisfies no objective — alerts must be reviewed, triaged, and escalated per the incident response plan.

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.L2-3.14.6

SYSTEM & INFO INTEGRITY — Monitor Communications for Attacks

Plain English

What this control is really saying:

An attacker leaves footprints. Unusual inbound connection patterns, after-hours file access, data leaving the network at odd times, traffic to known-bad IP addresses — all of these are indicators. This control requires that you watch for them: monitoring the system itself, monitoring what comes in, and monitoring what goes out. All three are required.

How it is used:

- IDS/IPS is deployed at the network boundary — it monitors inbound and outbound traffic, generates alerts on known attack signatures, and logs anomalous traffic patterns.
- SIEM aggregates logs from the firewall, VPN gateway, and CUI file server — correlation rules detect unusual access patterns and generate security alerts.
- Outbound traffic is monitored for data exfiltration indicators — large transfers to unknown destinations after hours trigger automatic alerts.
- System monitoring outputs are reviewed on a defined schedule — alerts are triaged, investigated, and escalated per the incident response plan.

Real World Example

The Scenario

Acme Defense has a perimeter firewall with logging enabled. No IDS or SIEM is deployed. Firewall logs are stored but never reviewed. Outbound traffic monitoring does not exist.

What the assessor finds

An attacker with compromised credentials accessed the CUI file server over 23 days, exfiltrating 4,200 design files in small batches via HTTPS to a cloud storage account. The firewall logged all 23 outbound sessions. No one reviewed the logs. The breach was discovered when a contracting officer noticed a competitor had identical design specifications.

SPRS Score Impact

3.14.6 carries a point value of 5. Unmonitored outbound traffic is the primary path for data exfiltration — an attacker can spend weeks quietly moving CUI outside the network while firewall logs accumulate unread.

What Good Looks Like

IDS/IPS deployed at network boundary, SIEM aggregates logs from key systems, inbound and outbound traffic both monitored, alerts reviewed on defined schedule, after-hours anomalies captured, monitoring outputs feed incident response process.

Common Gaps

What assessors actually find in the field:

✗ No IDS/IPS deployed

No intrusion detection system monitors network traffic — attacks in progress generate no alerts and are only discovered after damage occurs.

✗ Inbound only, outbound ignored

Inbound traffic is monitored by the firewall but outbound traffic is unrestricted and unmonitored — data exfiltration is invisible.

✗ Logs generated but not reviewed

Firewall and system logs are generated but nobody reviews them — attack indicators accumulate in log files that no one reads.

✗ No SIEM or log correlation

Logs exist on individual systems but are not centrally aggregated — a multi-step attack touching multiple systems cannot be correlated.

✗ No after-hours monitoring

Monitoring occurs during business hours only — attacks conducted outside working hours are not detected until the next business day.