CMMC

SYSTEM & INFO INTEGRITY

Catch Problems Before They Catch You.

The System and Information Integrity family is about spotting and stopping trouble early before small issues turn into full-blown incidents. It covers patching, anti-malware, alerts, and watching for weird activity on your systems. You're giving your environment a regular health check so you're not surprised by preventable attacks.

Proof of Practice

Examples

☑ **Antivirus/EDR deployment report**
Inventory or console view listing protected devices, last check-in, and recent detections. Proves coverage is broad, active, and monitored, not just "installed once."

☑ **Email notifications from AV/EDR or SIEM**
Alert emails (or digests) about malware detections, blocked activity, or policy violations, along with ticket IDs or actions taken. Shows continuous monitoring and response.

☑ **Security advisory & alert emails**
A shared mailbox or mail folder where CISA alerts, vendor advisories, and KEV notices are auto-routed.

The Business Impact

A small shop delays updates and ignores antivirus alerts "until things slow down." One day, a known vulnerability gets exploited, production halts, and their customer asks why basic hygiene was skipped. Strong controls prove you're actively watching, patching, and protecting the systems that keep DoD missions moving.

Available Resources

CISA Cybersecurity Alerts & Advisories
https://www.cisa.gov/news-events/cybersecurity-advisories

NSA Cybersecurity Advisories & Guidance
lhttps://www.nsa.gov/press-room/cybersecurity-advisories-guidance/

NIST SP 800-137: Info Security Continuous Monitoring
https://csrc.nist.gov/pubs/sp/800/137/final

Microsoft Defender for Endpoint
https://www.microsoft.com/en-us/security/business/endpoint-security/microsoft-defender-endpoint

Crowdstrike
https://www.crowdstrike.com/en-us/platform/endpoint-security/

Quick Wins

1. Subscribe security/IT leads to CISA alerts & vendor security advisories

2. Build a simple "patch this week" list.

3. Turn on automatic updates where safe.

4. Standardize and tune antivirus/EDR alerts.

5. Create a "see something, say something" channel.

CYBERNEX TECHNOLOGY

www.CyberNEX.io