DATASHEET

Sevco Exposure Assessment Platform for CMMC Compliance

Achieve and Maintain CMMC Certification with Continuous Visibility

Key Benefits

Asset Management

Maintain comprehensive inventory of all assets handling CUI with continuous discovery

Vulnerability Management

Identify, prioritize, and track remediation of vulnerabilities across your environment

Configuration Management

Monitor security control deployment and configuration baseline compliance

Audit Readiness

Continuous evidence collection and documentation for C3PAO assessments

Sevco Exposure Assessment Platform Use Cases

Built for Defense Industrial Base Contractors

Defense contractors and DIB organizations face a critical mandate: achieve CMMC compliance to maintain DoD contracts. Sevco's Exposure Assessment Platform directly addresses multiple CMMC domains including Asset Management, Configuration Management, Risk Management, and System and Information Integrity. With continuous asset discovery, vulnerability tracking, and verified remediation, Sevco helps you prepare for CMMC assessments and maintain compliance over time.

Continuous Monitoring & Assessment Readiness

Maintain audit-ready documentation with continuous evidence collection. Generate reports showing asset inventories, vulnerability remediation timelines, and security control effectiveness. Prepare for C3PAO assessments with confidence.

How Sevco Supports CMMC Domains

Asset Management (AM)

Comprehensive asset discovery and inventory management for CUI environments.

- AM.L2-3.4.1: Maintain current asset inventory
- AM.L2-3.4.2: Address unauthorized assets
- AM.L2-3.4.5: Implement least functionality

Risk Management (RM)

Vulnerability identification, prioritization, and remediation tracking.

- RM.L2-3.11.1: Periodically assess vulnerabilities
- RM.L2-3.11.2: Remediate vulnerabilities per risk
- RM.L2-3.11.3: Monitor threat intelligence

Configuration Management (CM)

Monitor security control deployment and baseline configurations.

- CM.L2-3.4.6: Employ least privilege
- CM.L2-3.4.7: Restrict software execution
- CM.L2-3.4.8: Control user-installed software

System & Information Integrity (SI)

Continuous monitoring and verification of security controls.

- SI.L2-3.14.1: Identify system flaws
- SI.L2-3.14.2: Deploy security updates timely
- SI.L2-3.14.6: Monitor security alerts

Sevco Security was founded on the premise that bad data creates bad outcomes. Sevco breaks down siloed tech tools to provide a system of record to support security programs. With Cyber Asset Attack Surface Management (CAASM) as the inventory foundation, Sevco has evolved to include vulnerability assessment, vulnerability prioritization, and threat intelligence—becoming a true Exposure Assessment Platform (EAP) that provides comprehensive data on devices, identities, applications, users and vulnerabilities.

Support for CMMC Levels

CMMC Level 2

Level 2 requires implementation of all 110 practices from NIST SP 800-171. Sevco directly supports practices across multiple domains:

- **Asset Management:** Maintain authoritative asset inventory with automated discovery and classification
- **Vulnerability Management:** Continuous vulnerability assessment and prioritized remediation tracking
- **Configuration Management:** Monitor security control deployment and baseline compliance
- **Evidence Collection:** Automated documentation for assessor review

CMMC Level 3

Level 3 adds advanced and progressive practices to protect against Advanced Persistent Threats (APTs). Sevco supports enhanced capabilities:

- **Advanced Threat Correlation:** Integrate threat intelligence with asset and vulnerability data
- **Continuous Monitoring:** Real-time visibility across the entire attack surface
- **Incident Response:** Rapid asset identification during security events
- **Verified Remediation:** Go beyond ticket closure to confirm fixes are implemented

The CMMC Imperative

CMMC certification is becoming mandatory for DoD contractors. Organizations that handle Controlled Unclassified Information (CUI) must achieve CMMC Level 2 certification by the DoD implementation deadline. Those supporting DoD programs involving advanced threats may require Level 3.

Without certification, contractors cannot:
Bid on new DoD contracts, renew existing contracts, or participate in the defense industrial base supply chain. Sevco helps you achieve and maintain certification by providing continuous evidence of compliance with CMMC requirements.

Prepare for C3PAO Assessment

Sevco helps you demonstrate compliance during certification assessments:

Evidence Collection

- Automated asset inventory reports
- Vulnerability assessment documentation
- Remediation timelines and verification
- Security control deployment status

Continuous Compliance

- Real-time monitoring of security posture
- Drift detection from approved baselines
- Automated compliance dashboards
- Historical trend analysis for assessors

Sevco Integrates With the Security Tools You Already Use

A few examples of the hundreds of integrations Sevco supports:

Vulnerability Scanning | Endpoint Protection | Cloud Security | Network Security | Applications

Contact Us

sevcosecurity.com | @sevcosecurity

1401 Lavaca Street
#857 Austin, TX 78701

Email: hello@sevcosecurity.com
Phone: 512.270.8949