DATASHEET

Sevco Exposure Assessment Platform for NIST Cybersecurity Framework

Align Your Security Program with Industry Standards

Key Benefits

Identify

Comprehensive asset management and risk assessment capabilities

Protect

Monitor security controls and vulnerability management programs

Detect

Continuous monitoring for anomalies and security events

Respond & Recover

Rapid asset identification and verified remediation tracking

Built to Support the NIST Cybersecurity Framework

The NIST Cybersecurity Framework provides a common language and systematic methodology for managing cybersecurity risk. Sevco's Exposure Assessment Platform directly supports the Framework's five core functions—Identify, Protect, Detect, Respond, and Recover—by providing continuous visibility into your attack surface, real-time risk assessment, and verified remediation capabilities. Whether you're implementing NIST CSF for regulatory compliance, customer requirements, or security program maturity, Sevco accelerates your journey.

NIST CSF Use Cases

- **Asset Management (ID.AM)**

  Maintain comprehensive inventory of all organizational assets including hardware, software, systems, data, and services. Automatically discover and classify assets with continuous updates as your environment changes.

- **Vulnerability Management (ID.RA, PR.IP)**

  Identify and prioritize vulnerabilities based on business context and threat intelligence. Track remediation activities and verify that fixes are implemented, supporting both risk assessment and protective technology functions

- **Continuous Monitoring (DE.CM)**

  Monitor security posture continuously across your environment. Detect configuration drift, missing security controls, and new exposures in real-time to support detection processes.

- **Incident Response & Recovery (RS.AN, RC.RP)**

  Rapidly identify affected assets during security incidents. Track remediation progress and verify recovery activities to ensure systems return to secure operational state.

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.

How Sevco Supports NIST CSF Core Functions

IDENTIFY (ID): Develop organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

ID.AM – Asset Management
Automated discovery and inventory of all organizational assets with continuous updates

ID.RA – Risk Assessment
Continuous vulnerability identification and risk prioritization based on business context

PROTECT (PR): Develop and implement appropriate safeguards to ensure delivery of critical services.

PR.IP – Information Protection
Track security control deployment and configuration management across environment

PR.PT – Protective Technology
Monitor endpoint protection, encryption, and security tool effectiveness

DETECT (DE): Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

DE.CM – Continuous Monitoring
Real-time monitoring for configuration drift, new exposures, and missing controls

DE.AE – Anomalies and Events
Detect unauthorized assets, software changes, and security control gaps

RESPOND (RS): Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

RS.AN – Analysis
Rapidly identify affected assets and their exposures during incident investigation

RS.MI – Mitigation
Track containment and mitigation actions across impacted systems

RECOVER (RC): Develop and implement appropriate activities to maintain plans for resilience and restore capabilities or services.

RC.RP – Recovery Planning
Verify restoration of systems and security controls to operational state

RC.IM – Improvements
Track lessons learned and remediation improvements over time

Progress Through Implementation Tiers

Sevco helps organizations advance their cybersecurity maturity across NIST CSF Implementation Tiers:

Tier 1: Partial

Move from manual,reactive processes to automated asset discovery and basic visibility

Tier 2: Risk Informed

Implement risk-based prioritization and continuous monitoring capabilities

Tier 3: Repeatable

Establish consistent processes with verified remediation and metrics

Tier 4: Adaptive

Achieve continuous improvement with predictive capabilities and automation

Sevco Integrates with Tools Across All NIST CSF Categories

A few examples of the hundreds of integrations Sevco supports:

Identify & Protect
Asset Management, CMDB, Vulnerability Scanners, Endpoint Protection

Detect
SIEM, EDR, Network Monitoring, Cloud Security Tools

Respond & Recover
Ticketing Systems, SOAR, Patch Management, Backup Solutions

Contact Us

sevcosecurity.com
@sevcosecurity

1401 Lavaca Street
#857 Austin, TX 78701

Email: hello@sevcosecurity.com
Phone: 512.270.8949