VectorUSA Security Operations Center (SOC)

Capabilities & Operations Overview

VectorUSA's Security Operations Center (SOC) delivers human-led, technology-enabled security operations that help organizations quickly detect, respond to, and reduce cybersecurity risk.

EXECUTIVE OVERVIEW

VectorUSA has established a dedicated Security Operations Center (SOC) to help organizations detect, respond to, and recover from cybersecurity threats with greater speed, clarity, and confidence.

The VectorUSA SOC delivers structured, human-led security operations supported by automation and proven technologies. Rather than focusing solely on alerts or tools, the SOC is designed to reduce real-world risk by aligning people, process, and technology to identify threats early, respond effectively, and drive issues to resolution.

This overview outlines how the VectorUSA SOC operates, what capabilities are included, and how customers benefit from a disciplined and transparent security operations model.

IN-SCOPE SERVICES

- Continuous security monitoring and alert triage
- Threat investigation and incident response
- Vulnerability identification, prioritization, and remediation
- Security automation and response orchestration
- Governance, reporting, and performance measurement

MISSION

Deliver trusted, efficient, and adaptive security operations through 16×5 SOC coverage, vulnerability management, and automated response using Microsoft and Fortinet technologies.

Connecting People and Information to the World – Securely.

CONTACT

800.929.4516

www.vectorusa.com

HOW THE VECTOR USA SOC OPERATES

The VectorUSA SOC operates on a 16×5 coverage model, providing active monitoring and response during peak operational hours when most cyber risk occurs. The SOC works directly with customer environments and IT teams, enabling coordinated action and faster remediation.

TIERED SOC OPERATIONS

Tier 1 – Core Monitoring

Foundational 16×5 security visibility with monitoring and reporting.
Included Services: Endpoint & server monitoring, monthly reporting

Tier 2 – Monitoring + Response

Adds active incident response, remediation, and vulnerability management to reduce risk faster.
Adds: Incident remediation, vulnerability management, and root cause analysis.

Tier 3 – Full SOC Service

Delivers expanded SOC operations with automation, compliance mapping, and advanced reporting.
Adds: Compliance mapping, automation, SOAR tuning

Tier 4 – Enterprise 24×7 SOC

Provides after-hours escalation, proactive threat hunting, and an incident response (IR) retainer.

Technology and Automation

The VectorUSA SOC is built on an integrated security platform that provides broad visibility without vendor lock-in. Core technologies include Microsoft Sentinel, Microsoft Defender XDR, FortiSOAR, Fortinet security platforms, and vulnerability management tools.

Automation improves speed and consistency for common, high-volume alerts, while engineers maintain oversight and final decision authority for investigations and response.

Vulnerability Management and Remediation

The SOC goes beyond alerting by owning the vulnerability lifecycle. Identified risks are prioritized, remediated within defined service levels, and validated to confirm closure. This approach helps customers reduce exposure rather than accumulate unresolved findings.

Governance, Reporting, and Transparency

SOC performance is measured using clear operational metrics such as Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), automation utilization, and resolution timelines.

Customers receive regular reporting that provides visibility into security activity, outcomes, and trends. Operational practices align with recognized security frameworks, supporting audit readiness and governance needs.

WHAT SETS THE VECTOR USA SOC APART

- ✓ Human-led investigations supported by automation
- ✓ End-to-end ownership from detection through remediation
- ✓ Open, multi-vendor security architecture
- ✓ Operates within customer environments
- ✓ SLA-backed operational accountability

SCAN THE QR CODE TO LEARN MORE

1072026me