

# 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.



*Connecting People and Information to the World – Securely.*

### CONTACT

800.929.4516

### 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 24x7 SOC coverage, vulnerability management, and automated response .

# HOW THE VECTOR USA SOC OPERATES

The VectorUSA SOC operates on a 24x7 model 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 – Monitoring & Triage

Provides continuous security event monitoring and initial triage. Alerts are validated for accuracy and severity, with meaningful activity identified and prioritized. This tier establishes clear visibility into security events and ensures potential issues are accurately surfaced.

### Tier 2 – Investigation & Escalation

Tier 2 expands monitoring with in-depth investigation of validated security events. Activity is analyzed in context and correlated across multiple data sources to determine risk and impact. Confirmed incidents are escalated with clear, actionable findings to support timely response.

### Tier 3 – Remediation & Engineering

Delivers full operational SOC coverage, including investigation, containment, and remediation. Hands-on actions include indicator removal, configuration hardening, identity cleanup, patch validation, and vulnerability remediation support. This tier represents end-to-end ownership from detection through resolution.

### Tier 4 – Extended Coverage & 24x7 Operations

Extends SOC operations with after-hours monitoring and enhanced response availability. This level provides continuous security coverage and accelerated response timelines to support always-on operational requirements.

## Technology and Automation

The VectorUSA SOC is built on an integrated security platform that provides broad visibility without vendor lock-in.

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.

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



1202026me