VERTEX TECHNOLOGIES GROUP
Security Operations Practice

MONITORING GUIDE

Traffic Analysis · Anomaly Detection · Protocol Monitoring Threat Intelligence Integration · Alert Tuning · Sensor Management

Document No.	VTG-NSM-GDE-2026-02
Classification	RESTRICTED — INTERNAL USE ONLY
Version	1.4
Effective Date	March 10, 2026
Review Cycle	Quarterly
Document Owner	Network Security Operations Manager
Prepared By	Bradley Documentation & Learning

NON-PROPRIETARY PORTFOLIO SAMPLE — No live network data, sensor configurations, or client infrastructure details included.

Table of Contents

1. Document Authority and Purpose

1.1 Purpose and Scope

This Network Security Monitoring (NSM) Guide establishes the operational standards, detection methodology, sensor management requirements, and analyst procedures for the Vertex Technologies Group network security monitoring program. It governs all activities related to traffic analysis, anomaly detection, protocol inspection, alert triage, and threat intelligence integration across the enterprise network environment.

Effective NSM provides the visibility layer that enables early detection of threats, lateral movement, data exfiltration, and policy violations. It supports incident response, compliance validation, and network operations through continuous monitoring, structured baselining, and disciplined alert management.

1.2 Governing Standards and Frameworks

- ◆ NIST SP 800-137 — Information Security Continuous Monitoring (ISCM): Primary NSM framework reference.
- ◆ NIST SP 800-94 — Guide to Intrusion Detection and Prevention Systems: Detection architecture guidance.
- ◆ CIS Control 13 — Network Monitoring and Defense: Implementation benchmark.
- ◆ Vertex Enterprise Information Security Policy (EISP-VTG-2026): Internal governing policy.
- ◆ Vertex Network Architecture Standards (NAS-VTG-2026): Network topology and segmentation reference.
- ◆ MITRE ATT&CK; Framework — Network-based technique detection mapping.

1.3 Document Control

Field	Value
Document Owner	Network Security Operations Manager
Technical Authority	Chief Information Security Officer (CISO)
Primary Audience	NSM analysts, SOC leads, network security engineers, threat hunters
Review Trigger	Quarterly cycle, or after significant network architecture change or major detection gap identified
Related Documents	NAS-VTG-2026 (Architecture), IR Playbook MHS-IR-PLY, SIEM Tuning Guide VTG-SIEM-2026
Storage	Vertex Secure Documentation Repository (VTG-DOC-SECURE)

2. NSM Architecture and Sensor Deployment

2.1 Monitoring Architecture Overview

The Vertex NSM architecture uses a defense-in-depth sensor model with monitoring points at the network perimeter, internal segmentation boundaries, cloud egress, and critical asset subnets. No single sensor provides complete visibility; the layered model ensures coverage continuity when individual sensors experience degraded performance or maintenance windows.

2.2 Sensor Deployment Zones

Zone	Location / Description	Sensor Type(s)	Coverage Priority
Internet Perimeter	North-south traffic at primary and secondary internet ingress/egress points.	NGFW, IDS/IPS, NetFlow collector	Critical
DMZ Boundary	Traffic between DMZ-hosted services and internal networks; external-facing application servers.	IDS/IPS, packet capture, NGFW	Critical
Internal Core	East-west traffic on core switching fabric; inter-VLAN routing points.	NetFlow/IPFIX collector, IDS tap	High
Remote Access / VPN	VPN gateway ingress; remote employee and vendor access sessions.	VPN log aggregation, NetFlow, authentication monitor	High
Cloud Egress	Traffic leaving on-premises environment to cloud providers (AWS, Azure, SaaS).	CASB, cloud-native flow logs, NGFW	High
Critical Asset Subnet	Subnets containing regulated data systems, privileged infrastructure, or OT/IoT systems.	Dedicated IDS sensor, full packet capture	Critical
Guest / BYOD Network	Isolated guest Wi-Fi and BYOD segments with internet-only access.	NGFW, basic flow logging	Standard
Out-of-Band Management	Network management plane; switch/router management interfaces; IPMI/iDRAC segments.	Access control monitoring, authentication logging	High

2.3 Sensor Tap and SPAN Configuration Standards

All passive monitoring sensors must receive traffic via hardware TAPs or dedicated SPAN ports configured per the Network Architecture Standards. Analysts must understand the following constraints when interpreting sensor data:

- ◆ SPAN ports may drop packets under high load — hardware TAPs are required for critical asset subnet monitoring.
- ◆ Encrypted traffic (TLS 1.3) will appear as opaque flows unless SSL/TLS inspection is enabled at the designated inspection points.
- ◆ IPv6 traffic must have equivalent monitoring coverage to IPv4 — confirm sensor dual-stack capability during deployment.
- ◆ Asymmetric routing can cause incomplete flow records — document known asymmetric paths in the network topology register.

◆ Out-of-band management traffic should be monitored separately from production traffic to avoid alert noise.

NOTE	Sensor placement diagrams and current tap/SPAN configurations are maintained in the Network Architecture Standards document (NAS-VTG-2026). Analysts should not modify sensor configurations without Change Management approval. See Section 8 for sensor health monitoring procedures.

3. Traffic Baseline and Anomaly Detection

3.1 Baselining Methodology

Effective anomaly detection depends on accurate network traffic baselines. Baselines must capture normal patterns across multiple dimensions: volume, protocol distribution, connection patterns, timing, geographic distribution, and behavior by system role. Baselines that do not account for business cycles (daily peaks, weekly patterns, quarterly activity) will generate excessive false positives or miss genuine anomalies.

The NSM team maintains rolling 90-day baselines updated weekly. Significant business events (acquisitions, new application deployments, major infrastructure changes) require an explicit baseline reset with documentation of the change and the expected new normal.

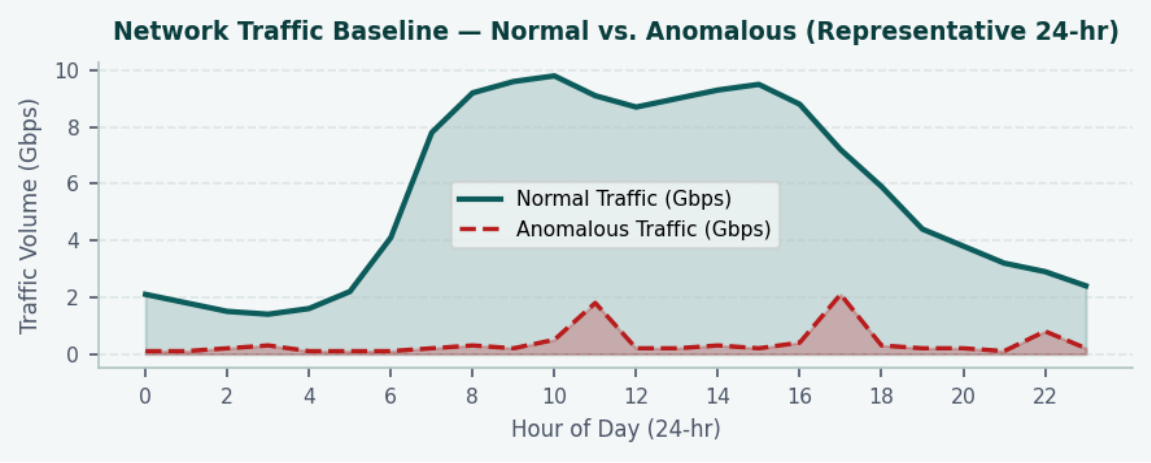


Figure 1 — Representative 24-hour traffic baseline showing normal (teal) vs. anomalous (red dashed) traffic volume. Spikes at hours 11–12 and 17 warrant investigation.

3.2 Baseline Dimensions and Collection Requirements

Baseline Dimension	Measurement	Collection Interval	Alerting Threshold
Traffic Volume	Gbps by segment; packets per second at key inspection points	Per 5-minute interval	>2 std dev from 4-week rolling avg
Top Talkers	Top 20 internal hosts by inbound and outbound byte count	Hourly	New host in top 5; >300% volume increase
Protocol Distribution	Percentage share of each protocol by segment	Daily	>5% shift in any protocol share
External Connections	Unique external IP count; new external ASN connections	Per session	Connection to new high-risk country or ASN
DNS Query Volume	Queries per host per hour; unique domains per host per day	Per 15-minute interval	>500 queries/hr or >200 unique domains/day
Authentication Events	Login count, failure rate, time-of-day pattern	Per event	Failure rate >10% or off-hours admin login
Data Transfer Volume	Bytes transferred to external destinations by host and department	Hourly	>500% of daily average in single hour

Baseline Dimension	Measurement	Collection Interval	Alerting Threshold
Connection Duration	Average session length by protocol and destination type	Per session	Sessions >4 hours to external IP

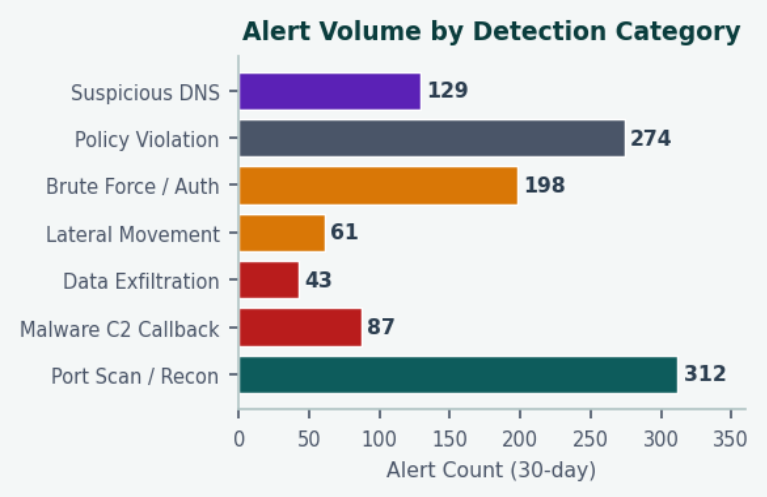
3.3 Anomaly Detection Categories

Anomalies are classified into three operational tiers based on detection confidence and required response urgency. All anomalies generate a detection record regardless of tier.

◆ **Tier 1 — High Confidence Anomaly:** Statistical deviation exceeds threshold AND matches known attacker TTP or threat intelligence indicator. Requires immediate analyst review.

◆ **Tier 2 — Behavioral Anomaly:** Unusual pattern detected but no corroborating threat intelligence match. Analyst review required within current shift.

◆ **Tier 3 — Low-Confidence Signal:** Minor deviation from baseline, single data point, or first-occurrence event. Log and monitor for pattern development.



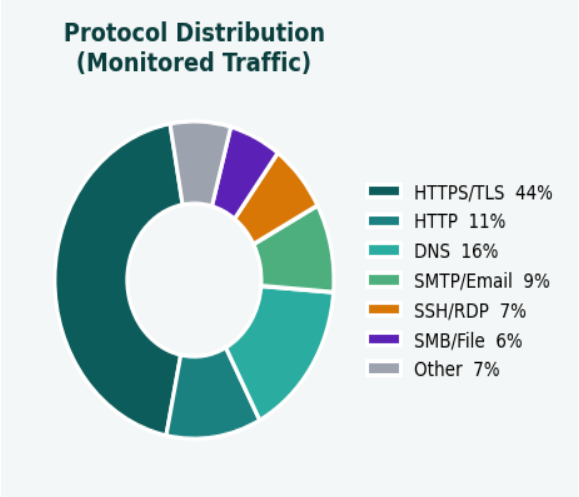


Figure 2 (left) — Alert volume by detection category, 30-day period. Figure 3 (right) — Monitored traffic protocol distribution by percentage.

4. Protocol Analysis and Inspection Standards

4.1 Priority Protocols for Deep Inspection

Not all traffic warrants deep packet inspection. The following protocols are designated for full deep inspection based on their abuse potential and relevance to known attacker TTPs. Inspection scope and depth are documented in the NSM Tool Configuration Guide (VTG-NSM-CONFIG).

Protocol	Inspection Focus	Key Indicators of Compromise	Inspection Level
DNS	Query volume, domain age, entropy, NX-domain ratio, tunneling patterns.	High NX-domain rate; DGA-pattern domains; unusually long query strings; TXT record abuse.	Full inspection + ML scoring
HTTP/HTTPS	User-agent strings, URI patterns, POST body anomalies, C2 callback patterns.	Beaconing regularity; encoded POST data; unusual user-agent; connection to new external IP.	Full inspection; TLS decryption at designated points
SMB	Lateral movement patterns, named pipe usage, admin share access.	Admin share access from non-admin hosts; EternalBlue-pattern connections; after-hours access.	Header + metadata inspection
RDP / SSH	Authentication failure patterns, source IP geography, session duration.	Brute force attempt sequences; access from unexpected source; unusual session length.	Flow analysis + authentication event correlation
SMTP / Email	Attachment types, external relay usage, volume spikes, spoofed headers.	Mass outbound; attachment type anomaly; relay misconfiguration abuse.	Header + attachment metadata
ICMP	Tunnel detection, volume anomalies, non-standard type/code combinations.	ICMP payloads exceeding standard sizes; regular ICMP beaconing; ICMP tunneling patterns.	Full inspection
PowerShell / WMI Remoting	Encoded commands, WINRM traffic, remote execution patterns.	Base64-encoded command strings; WMI lateral movement; PSRemoting from unusual sources.	Payload inspection where available

4.2 Encrypted Traffic Analysis

The widespread adoption of TLS 1.3 and certificate pinning limits traditional deep packet inspection. Analysts must use metadata-based analysis methods for encrypted traffic where full decryption is not available.

◆ **JA3/JA3S fingerprinting:** TLS client and server hello fingerprints identify known malware families and unusual TLS implementations without decryption.

◆ **Certificate analysis:** Self-signed certificates, recently-issued certificates (< 30 days), and certificates with unusual subject fields are elevated indicators.

◆ **Flow pattern analysis:** Connection timing, packet interval regularity, and byte count patterns can identify C2 beaconing even in encrypted streams.

◆ **SNI / ESNI inspection:** Server Name Indication fields provide destination context for encrypted HTTPS without decryption.

◆ **DNS-over-HTTPS (DoH) detection:** DoH bypasses standard DNS monitoring; identify DoH usage and route through enterprise DNS resolver.

IMPORTANT	SSL/TLS inspection of encrypted traffic requires legal and compliance review before deployment. Decryption of personal communications may have legal implications in some jurisdictions. Consult Legal and Privacy before expanding decryption scope.

5. Alert Management and Triage Procedures

5.1 Alert Lifecycle

Every NSM alert follows a defined lifecycle from generation through final disposition. Analysts must complete all lifecycle stages and document each transition. Alerts that cannot be resolved within the current shift must be formally handed off per Section 10.

Stage	Analyst Action	Documentation	Time Limit
Generated	Alert appears in queue. System assigns case ID and priority.	Case ID auto-created; source logged.	Automatic
Acknowledged	Analyst opens and acknowledges the alert to stop SLA clock from lapsing.	Analyst name, acknowledgment time.	Per priority SLA
Under Review	Active investigation: source confirmed, context gathered, related alerts reviewed.	Evidence gathered; related case IDs noted.	Per priority SLA
Escalated	Alert meets escalation criteria; handed to SOC Lead or IR team per Section 10.	Escalation notice completed; recipient confirmed.	Immediately on criteria met
Closed — Action Taken	Analyst completed containment or remediation action. Evidence documented.	Action record; outcome confirmed.	Before shift end
Closed — False Positive	Alert confirmed benign. Root cause of false positive documented for tuning.	False positive rationale; tuning recommendation submitted.	Before shift end
Closed — Informational	Alert reviewed; no action required. Expected behavior confirmed.	Evidence reviewed; expected behavior noted.	Before shift end

5.2 NSM Alert Priority Definitions

Priority	Definition	Response SLA	Escalation
P1 — Critical	Active confirmed threat: C2 communication, data exfiltration in progress, ransomware spread, known malware confirmed.	Acknowledge ≤ 5 min; escalate immediately	SOC Lead + IR team
P2 — High	Strong indicator: threat intel match, unusual privilege activity, lateral movement pattern, high-confidence anomaly.	Acknowledge ≤ 15 min; resolve or escalate within shift	SOC Lead
P3 — Medium	Moderate indicator: behavioral anomaly, single-host concern, policy violation, no confirmed impact.	Acknowledge ≤ 1 hour; document within shift	Monitor; escalate if pattern develops
P4 — Low	Informational: minor baseline deviation, known noisy rule, first-occurrence event, no business impact.	Acknowledge ≤ 4 hours; batch review acceptable	No escalation unless pattern changes

5.3 Alert Tuning and False Positive Management

Untuned alert rules generate excessive false positives that degrade analyst attention and increase mean time to detect genuine threats. Every false positive represents both wasted analyst time and a potential detection gap.

- Every false positive closure must include a tuning recommendation in the case notes.
- Tuning recommendations are reviewed weekly by the NSM lead and prioritized by alert volume impact.
- No tuning change that suppresses a MITRE ATT&CK; technique may be made without CISO review.
- Tuning changes are tracked in the SIEM Change Log (VTG-SIEM-CHG) with before/after expected alert volume.
- Suppressed rules must be reviewed quarterly to confirm the suppression condition is still valid.

6. Threat Intelligence Integration

6.1 TI Feed Sources and Confidence Tiers

The NSM platform ingests threat intelligence from multiple sources with different confidence levels and update frequencies. Analysts must understand the confidence tier of each feed before acting on a match — not all TI matches require the same response.

Tier	Source Type	Confidence	Action on Match	Expiry
Tier 1	Government / CISA, FBI, sector ISAC (FS-ISAC)	High	Immediate alert; P1/P2 escalation	90 days or until revoked
Tier 2	Commercial TI subscription (premium feeds)	High–Medium	P2 alert; analyst review required	60 days
Tier 3	Open source (OSINT) and community feeds	Medium	P3 alert; verify before acting	30 days
Tier 4	Internal — indicators from past incidents	Variable	Enhanced monitoring; context-dependent action	Reviewed per incident PIR
Tier 5	Analyst-submitted suspect indicators (unverified)	Low	Watch-only; do not escalate on single match	7 days; confirm or discard

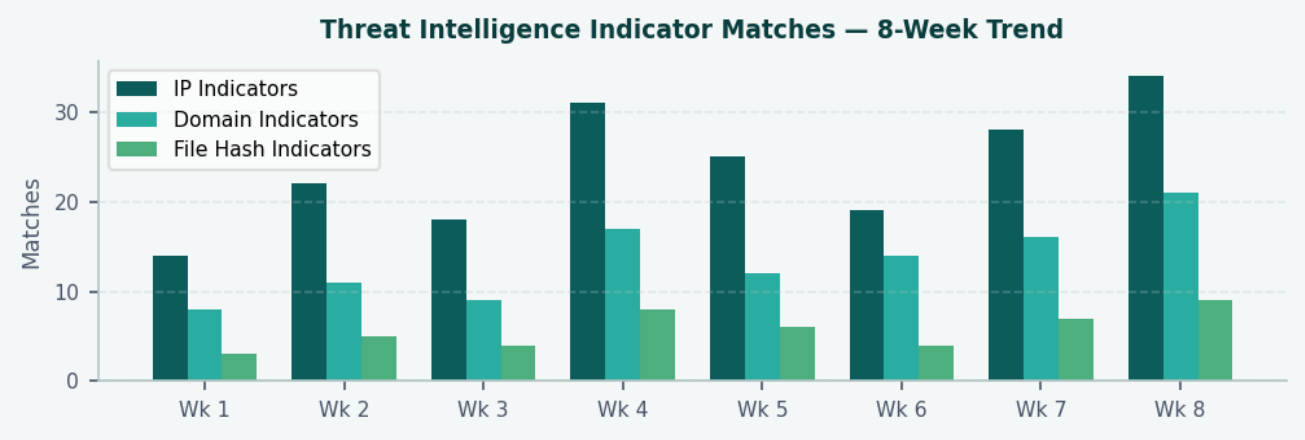


Figure 4 — Threat intelligence indicator matches by type over 8-week trend period. Rising match counts may indicate active campaign activity.

6.2 TI Indicator Handling Procedures

◆ **New Tier 1 indicator received:** Block at perimeter immediately. Search SIEM for prior 30-day history against all assets. Open monitoring case. Notify SOC Lead.

◆ **Tier 2/3 indicator match on internal host:** Open P2 or P3 case. Confirm asset, gather context, verify no false positive before escalating.

◆ **Expired indicator:** Remove from active blocking after review. Retain in historical search scope. Document removal decision.

◆ **Analyst-submitted indicator (Tier 5):** Log in TI platform. Watch-only status. Requires Tier 2 corroboration before upgrade.

NOTE	Threat intelligence sharing with external parties (ISAC, law enforcement) requires Legal and CISO approval. Do not share internal TI indicators externally without authorization.

7. Network Segmentation and Monitoring Zones

7.1 Segmentation Monitoring Principles

Network segmentation is only effective when crossing of segment boundaries is monitored and controlled. The NSM program treats every segment boundary as a detection opportunity. Unmonitored traffic crossing a segment boundary represents a coverage gap regardless of whether a firewall rule exists at that boundary.

◆ Every east-west traffic path between classified network zones must pass through at least one monitored inspection point.

◆ Firewall log completeness for all inter-segment rules must be confirmed weekly by the NSM team.

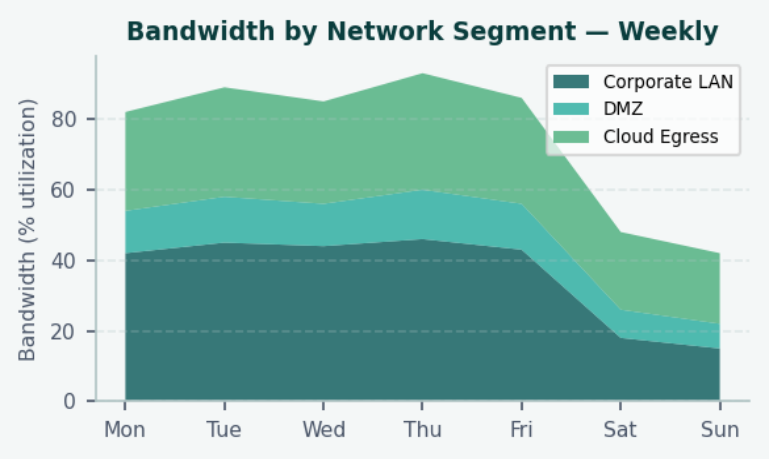
◆ New network segments introduced through infrastructure changes require NSM coverage design before production deployment.

◆ VLAN hopping and 802.1Q double-tagging should be tested for in the quarterly network segmentation validation exercise.

◆ Microsegmentation (where deployed) should have monitoring hooks feeding the central NSM platform.

7.2 Traffic Monitoring by Zone Classification

Zone	Expected Traffic Patterns	Key Anomalies to Detect
Internet Perimeter	Outbound: HTTPS, DNS, SMTP. Inbound: responses to initiated sessions only for general users.	Unexpected inbound connection initiation; raw socket connections; non-standard ports.
DMZ	Well-defined service ports only. Limited internal origination.	Internal host initiating connections to DMZ; DMZ host communicating to internal non-approved subnet.
Corporate LAN	Standard business protocols. Authentication traffic. File share access during business hours.	After-hours bulk file access; admin share access from workstations; Pass-the-Hash or Pass-the-Ticket patterns.
VPN / Remote Access	Authenticated user sessions. Standard application traffic per user role.	Session from unexpected geography; split-tunnel abuse; concurrent sessions from different source IPs.
Critical Asset Subnet	Tightly controlled — only expected management and application protocols.	Any unexpected connection; protocol outside approved baseline; connection from non-approved source.
Cloud Egress	OAuth, HTTPS to known SaaS/IaaS endpoints. Expected backup and sync traffic.	Unexpected upload volume; connection to unsanctioned cloud storage; new OAuth application authorization.



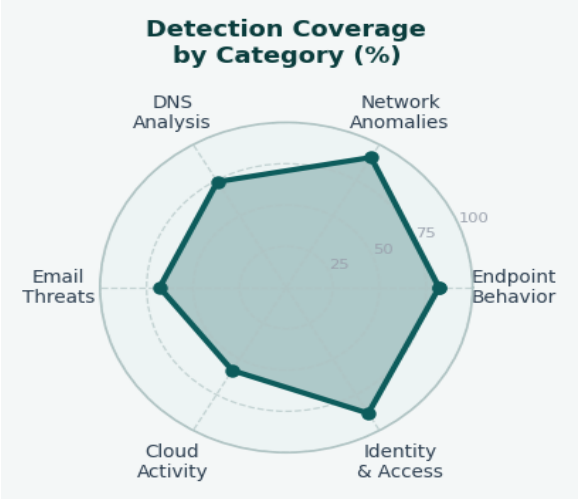


Figure 5 (left) — Bandwidth utilization by network segment across a representative week. Figure 6 (right) — Detection coverage percentage by monitoring category (radar chart).

8. Sensor Health and Coverage Management

8.1 Sensor Health Monitoring Requirements

A security monitoring program is only as strong as its sensor infrastructure. Sensor failures, interface flapping, storage overflow, and misconfiguration can create silent detection gaps that are invisible to analysts reviewing alert queues. Sensor health must be monitored continuously and treated with the same urgency as security alerts.

Health Metric	Normal Range	Warning Threshold	Critical Threshold	Action
Packet Loss Rate	0–0.5%	>1%	>3%	Notify NSM lead; check TAP/SPAN config
CPU Utilization	< 70%	70–85%	> 85%	Evaluate rule optimization; add capacity
Disk / Storage Utilization	< 75%	75–88%	> 88%	Rotate logs; expand storage; alert NSM lead
Alert Queue Depth	Normal processing backlog	> 500 unacknowledged	> 1000 unacknowledged	Add analyst resources; notify SOC Lead
Sensor Last-Seen (heartbeat)	< 5 min ago	5–15 min	> 15 min / offline	Confirm status; open coverage gap ticket
Log Source Last Event	< 10 min ago	10–30 min	> 30 min / no data	Verify log source; confirm network path
False Positive Rate	< 15%	15–25%	> 25%	Immediate tuning review with NSM lead

8.2 Coverage Gap Response Procedure

A coverage gap occurs any time a monitored network segment loses visibility due to sensor failure, configuration error, or network change. Coverage gaps in critical or high-priority zones must be treated as high-priority operational events.

◆ **Step 1 — Identify:** Sensor health alert generated or analyst notices missing log source. Open coverage gap ticket immediately.

◆ **Step 2 — Classify:** Determine affected zone (Critical / High / Standard). Critical zone gaps escalate to NSM Lead within 15 minutes.

◆ **Step 3 — Compensating Control:** Identify alternative visibility source (perimeter logs, endpoint telemetry, cloud logs) to maintain partial coverage during outage.

◆ **Step 4 — Notify:** Notify SOC Lead of monitoring gap and compensating controls in place. Update shift handoff notes.

◆ **Step 5 — Remediate:** Engage network or systems team for sensor restoration. Track in Change Management.

◆ **Step 6 — Validate:** Confirm full sensor recovery and validate data flow with test traffic or log source review. Close gap ticket with restoration confirmation.

9. Log Collection, Retention, and Correlation

9.1 Required Log Sources

Complete NSM coverage requires correlated analysis across multiple log source categories. Network flow data alone is insufficient — correlation with endpoint, identity, and application logs is essential for high-confidence detection and investigation support.

Log Source Category	Required Sources	Retention Minimum	Collection Priority
Network Flow (NetFlow/IPFIX)	All routers and switches at segment boundaries; cloud VPC flow logs	1 year	Critical
Firewall Logs	All perimeter and internal NGFW; allow and deny events; rule change events	1 year	Critical
IDS/IPS Alerts	All sensor alert events; signature updates; tuning changes	1 year	Critical
DNS Logs	All internal resolver queries; responses; NXDOMAIN counts	1 year	Critical
Proxy / Web Gateway	HTTP/HTTPS request logs; category/reputation decisions; blocked requests	90 days	High
Authentication Events	Active Directory; VPN; cloud SSO; MFA events; failed login attempts	1 year	Critical
Endpoint Telemetry (EDR)	Process execution; network connections; file events; registry changes	90 days	High
Email Gateway	Inbound/outbound message headers; attachment scan results; phish/spam dispositions	1 year	High
Cloud Platform Logs	AWS CloudTrail / Azure Activity Log / GCP Audit Log; API calls; config changes	1 year	High
DHCP / IPAM	IP address assignment history; hostname resolution; lease events	180 days	Standard

9.2 SIEM Correlation and Use Case Management

Log collection without structured correlation produces data, not intelligence. The SIEM platform implements use-case-driven correlation rules mapped to MITRE ATT&CK; techniques. Use cases must be reviewed, tuned, and validated on a defined cycle.

- ◆ Each SIEM use case must document: detection objective, ATT&CK; technique mapping, required log sources, false positive rate, and last tuning date.
- ◆ New use cases must be tested in a dev/staging SIEM environment before production deployment.
- ◆ Use cases with false positive rates exceeding 25% must be suspended and re-engineered before reactivation.
- ◆ The SIEM use case library is reviewed semi-annually against the current threat landscape and ATT&CK; updates.

IMPORTANT

Log retention requirements may be subject to legal hold orders or regulatory mandates that exceed the minimums defined in this guide. Always confirm retention obligations with Legal and Compliance before modifying log storage configurations.

10. Incident Detection Escalation and Handoff

10.1 Escalation Criteria from NSM

NSM-detected events escalate to the Incident Response program when they meet one or more of the following criteria. Analysts should reference the Incident Response Playbook (VTG-IR-PLY-2026) for full escalation procedures after initiating the handoff.

- Active confirmed C2 communication from an internal host to a known malicious infrastructure.
- Data exfiltration pattern confirmed: large outbound transfer to unexpected external destination.
- Lateral movement confirmed: credential-based access to multiple hosts in rapid sequence.
- Ransomware indicators: rapid file rename activity, SMB encryption behavior, or known ransomware hash match.
- Threat intelligence Tier 1 or Tier 2 indicator match on internal production host.
- Coverage gap in a Critical monitoring zone exceeding 30 minutes without compensating control.
- Confirmed exploitation of a known vulnerability on an internet-facing system.

10.2 NSM Escalation Notice Template

NSM DETECTION ESCALATION — VERTEX TECHNOLOGIES GROUP
Case ID: [NSM-YYYY-NNNN] **Priority:** [P1 / P2] **Detected By:** [Sensor / Rule Name] **Detection Time:** [Timestamp — exact] **Analyst:** [Name / ID]
Detection Summary: [What was detected, by which sensor, on which asset or segment, and why it meets escalation criteria. Be specific — include protocol, direction, volume, and any matching threat intelligence indicator or rule.]
Evidence Collected: [Flow records, PCAP reference, SIEM alert IDs, TI indicator ID, asset identity confirmation method]
Current Status: [Monitoring continues / Blocking rule applied / Asset isolated / Awaiting IR team direction]
Action Requested: [IR team engagement / Confirm escalation priority / Coordinate containment / Other]

NOTE	NSM analysts are responsible for detection and initial notification. Incident response ownership transfers to the IR team upon escalation acceptance. NSM analysts maintain monitoring posture and support the IR team with additional network evidence as requested.

11. Reporting, Metrics, and Continuous Improvement

11.1 NSM Performance Metrics

Metric	Definition	Target	Frequency
Sensor Uptime	Percentage of time each monitored zone has active sensor coverage.	≥ 99.5% for Critical zones	Weekly
Mean Time to Acknowledge (MTTA)	Average time from alert generation to analyst acknowledgment.	P1 ≤ 5 min; P2 ≤ 15 min	Weekly
Alert-to-Escalation Rate	Percentage of alerts that meet escalation criteria and are escalated.	Tracked; benchmark within 90 days	Monthly
False Positive Rate	Percentage of closed alerts classified as false positive.	< 15% per rule category	Weekly
TI Match Response Time	Time from TI indicator match alert to analyst action.	P1 match ≤ 15 min	Monthly
Coverage Gap Duration	Total minutes per month that Critical zones lacked sensor visibility.	< 30 min/month per zone	Monthly
Use Case Coverage vs ATT&CK;	Percentage of prioritized ATT&CK; techniques covered by at least one active detection rule.	≥ 80% of prioritized techniques	Quarterly
SIEM Log Source Completeness	Percentage of required log sources actively feeding the SIEM.	≥ 98%	Weekly

11.2 Required Reports and Reporting Cycle

Report	Contents	Audience	Cycle
Weekly NSM Operations Report	Alert volume, top rules fired, sensor health summary, false positive rate, open P1/P2 cases.	SOC Lead, NSM Manager	Weekly — Monday
Monthly Threat Landscape Summary	TI match trends, new attack technique detections, ATT&CK; coverage gaps, tuning actions taken.	CISO, Security Leadership	Monthly
Quarterly NSM Effectiveness Review	Full KPI review, coverage gap analysis, use case performance, sensor investment recommendations.	CISO, Security Governance Committee	Quarterly
Coverage Gap Incident Report	Triggered by any Critical zone gap > 30 min. Root cause, duration, compensating controls, corrective action.	NSM Manager, CISO	As needed

11.3 Continuous Improvement Program

◆ **Red Team / Purple Team exercise findings** are reviewed within 5 business days. Any detection gap confirmed by an exercise generates a required use case or tuning action within 30 days.

◆ **Threat intelligence updates** (new campaigns, emerging TTPs) trigger a review of existing detection rules for coverage within 14 days of ISAC/CISA advisory.

◆ **Post-incident NSM review:** After every P1/P2 incident, NSM team reviews whether the detection occurred at the earliest possible point and documents any earlier detection opportunity.

◆ **Technology refresh:** NSM toolset is reviewed annually against vendor roadmap and emerging detection technology. Recommendations presented to CISO with cost-benefit analysis.

Portfolio Demonstration Note

This document is a non-proprietary technical writing sample prepared by Bradley Documentation & Learning. It demonstrates the ability to produce structured, operational network security monitoring documentation suitable for real enterprise security teams. All company names, personnel, configurations, and metrics are fictional. No live network data, client systems, or restricted configurations are included.

Prepared by: Mark R. Bradley | Bradley Documentation & Learning | bradleyconsultingoh.io