SNO
A smarter tomorrow.

MANAGED SECURITY OPERATIONS SERVICE FOR ENTERPRISE AND PUBLIC SECTOR CUSTOMERS

ALWAYS-ON SECURITY MONITORING AND INCIDENT RESPONSE FOR MISSION-CRITICAL ENVIRONMENTS

Specialist Network Operations

Service Overview

SNO's Managed Security Operations (SecOps) service provides enterprise and public sector customers with continuous security monitoring, threat detection, investigation and response across their digital environment. The service combines advanced security analytics, integrated threat intelligence, automation and analyst-led operations to improve visibility, reduce risk and strengthen operational resilience.

Designed for organisations that require 24x7 security operations without the cost and complexity of running an in-house Security Operations Centre (SOC), SNO's Managed SecOps service enables customers to maintain control of their security posture while SNO delivers continuous monitoring, incident management and response services aligned with agreed service levels.

The service supports complex, distributed environments spanning network, endpoint, identity, cloud and application layers, providing a centralized operational view of security risk and active threats.

What You Get

Unified Security Monitoring Across the Environment

SNO's Managed SecOps service delivers centralized visibility across multiple security domains, enabling faster detection and more effective response.

- Continuous monitoring of security telemetry from network, endpoint, identity, cloud and security control platforms.
- Correlation of events across domains to identify attack paths and coordinated threats.
- Reduction of alert noise through contextual analysis and analyst validation.
- Centralized security analytics providing a single operational view of threats and incidents.

24/7 Monitoring with Integrated Threat Intelligence

Your environment is continuously monitored using real-time analytics enriched with up-to-date global threat intelligence.

- Real-time detection of known and emerging attack techniques.
- Continuous updates to detection logic without operational disruption.
- Intelligence-driven prioritization of threats based on risk and impact.
- Protection aligned to active threat campaigns targeting enterprise and public sector organisations

Security Incident Management & Customer Communications

SNO provides end-to-end ownership of security incidents through a structured Incident Management process designed to minimize business disruption and ensure rapid, controlled recovery.

Each incident is owned by a dedicated Service Delivery Manager (SDM) or NOC Team Lead, who acts as the single point of accountability throughout the incident lifecycle. All incidents are managed through SNO's Service Desk, ensuring clear governance, traceability and consistent communication.

Situation updates are provided at intervals aligned with incident severity and customer impact. All investigation, containment and remediation actions are logged within SNO's Service Management platform, ensuring full transparency, progress tracking and audit readiness.

SNO's primary objective is to restore secure operations as quickly as possible, prioritizing containment and service stability while preserving forensic integrity and evidence.

Post-incident reviews are conducted for significant events, with lessons learned used to improve detection logic, security controls and operational procedures through formal Change Management.

Automated Response with Expert Oversight

The Managed SecOps service combines automation with experienced security analysts to deliver fast, controlled response actions.

- Analyst-validated alerts to eliminate false positives and prioritize real threats.
- Automated containment actions aligned with predefined response playbooks.
- Coordinated response across security controls to limit threat spread.
- Guided remediation workflows to restore affected services to a known good state.
- Formal Root Cause Analysis (RCA) for high-impact incidents, including attack vectors, affected assets and risk reduction recommendations.

Security Use Case & Playbook Management

Security detection and response are driven by structured use cases and operational playbooks.

- Predefined and custom security use cases aligned to customer risk profiles.
- Continuous tuning of detection logic based on threat trends and operational feedback.
- Documented response playbooks to ensure consistent, repeatable incident handling.

- Alignment with recognised security frameworks such as NIST and MITRE ATT&CK.

Policy-Driven Control & Governance

Security operations are delivered within a governed, auditable framework aligned to customer policies and compliance requirements.

- Role-based access control (RBAC) aligned with least-privilege principles.
- Segregation of duties across operational and administrative roles.
- Formal configuration, change and incident governance.
- Full audit trail of security events, actions and changes.

Configuration & Change Management

SNO operates the Managed SecOps service under a formal Configuration and Change Management framework to ensure security controls remain consistent, controlled and auditable throughout the service lifecycle.

Configuration Management includes:

- Establishment of secure baseline configurations for monitored security controls.
- Centralized management of detection rules, correlation logic and response action.
- Continuous validation to detect configuration drift or unauthorized changes.
- Secure documentation and versioning of all configurations.

Change Management ensures:

- Risk and impact assessment prior to implementing changes.
- Expedited handling of emergency changes related to active incidents.
- Full change logging, validation and post-implementation review.

Reduced Risk & Improved Security Posture

The Managed SecOps service actively reduces security risk by:

- Detecting threats earlier through cross-domain correlation.
- Limiting attacker dwell time through rapid containment.
- Improving consistency and quality of incident response.
- Providing expert guidance to strengthen security posture over time.

Built for Resilience and Continuity

SNO's Managed SecOps service is designed to support always-on operations.

- Resilient analytics and monitoring components.
- Secure storage of security telemetry, alerts and forensic data.
- Business Continuity and Disaster Recovery (BCDR) planning and testing.
- Operational processes designed to support mission-critical environments.

Seamless Integration with Your Security Ecosystem

Where required, the service can integrate with your existing tools and platforms, including:

- Network and endpoint security controls.
- Identity and access management systems.
- Cloud and infrastructure platforms.
- Logging, analytics and ticketing systems.

*** Integration scope subject to separate scoping and agreement.*

Clear Reporting & Audit Readiness

Service Performance & Operational Metrics

- Monitoring of key service performance indicators including detection time, analyst response time, containment execution and incident resolution timelines
- Visibility into security coverage and monitoring effectiveness.
- Trend analysis to identify recurring performance bottlenecks or operational risks.
- Review of SLA adherence and service outcomes as part of regular service reporting.

Reporting cadence

- Monthly incident reporting
- Quarterly executive reporting
- Annual or on-demand compliance and audit reporting

Service Levels (At a Glance)

SLA Metric	Target
Threat Detection	< 5 minutes
Analyst Response	< 30 minutes
Containment Action	As defined per Playbook
Root Cause Analysis	< 7 days (High / Critical Incidents)
Reporting Delivery	As agreed

Operational Service Elements (At a Glance)

Service Element	Availability	Description
Service Desk Management	24x7x365	Acts as the single point of contact for all security incidents, service requests, and operational queries related to the Managed SecOps service. Ensures consistent intake, tracking, and governance of all customer interactions.
Security Incident Management	24x7x365	Manages security incidents to minimize business impact by restoring secure operations as quickly as possible using a structured, repeatable incident lifecycle aligned with agreed service levels.

Escalation Management	24x7x365	Ensures functional and hierarchical escalations are executed within defined KPIs to maintain response momentum and service assurance.
Security Event Monitoring & Analysis	24x7x365	Continuous monitoring, correlation and analysis of security events and alerts generated across network, endpoint, identity, cloud and security control platforms.
Threat Detection & Use Case Management	Included	Development, tuning and ongoing management of security detection use cases and response playbooks aligned to evolving threats and customer risk profiles.
Automated Response & Orchestration	Included	Execution of automated and semi-automated response actions based on defined playbooks to contain threats and reduce attacker dwell time.
Account Manager	Mon-Fri 08:45-17:30	A named Account Manager provides commercial oversight and acts as an escalation point during core business hours.
Service Delivery Manager	Mon-Fri 08:45-17:30	A named Service Delivery Manager (SDM) is responsible for operational governance, SLA oversight, incident accountability, and service performance reporting and acts as an escalation point during core working hours.
Technical Account Manager	Mon-Fri 08:45-17:30	A named Technical Account Manager provides technical oversight, supports service optimization and acts as an escalation point for complex technical matters and acts as an escalation point during core working hours.
SLA Management	Included	Definition, monitoring and reporting of detection, response, and resolution targets aligned with Managed SecOps service levels.
Customer Portal Access	Included	Secure access to SNO's service portal for incident logging, service requests, status visibility and reporting access.
Performance Management	Included	Continuous monitoring of service performance to ensure detection, response and containment objectives are met and to support future capacity and demand planning.
Availability Management	Included	Ensures the Managed SecOps service delivers agreed levels of availability and resilience to support business-critical operations.
Change Enablement / Release Management	Included	Controls changes to detection logic, response playbooks, configurations and platform updates to minimize risk while maintaining operational stability.
Service Request Management	Included	Handles standard security and operational service requests through defined workflows as part of business-as-usual service delivery.
Problem Management	Included	Identifies root causes of recurring security incidents and implements corrective actions to reduce future risk and operational impact.
Security Governance & Risk Management	Included	Oversees risks related to confidentiality, integrity, and availability of security data, controls, and operational processes within the Managed SecOps service.
Asset & Data Source Management	Included	Maintains visibility and lifecycle control of monitored assets, data sources and integrations to ensure consistent coverage and data quality.
Configuration Management	Included	Maintains controlled, auditable security configurations including baselines, change tracking and configuration integrity monitoring.

Service Reporting	Included	Comprehensive monthly reporting covering incidents, performance metrics, SLA adherence and service trends across all service elements.

Why Choose SNO's Managed SecOps Service for Enterprise and Public Sector?

SNO's Managed SecOps service delivers enterprise-grade security operations without the burden of running your own SOC. By combining continuous monitoring, intelligence-driven detection, automation and expert operational oversight, we help enterprise and public sector organisations stay resilient, compliant and secure. Allowing teams to focus on their core mission with confidence.