SOC AS A SERVICE · OPEN XDR AI-NATIVE

A SOC that thinks, correlates and acts in real time, 24/7

Unified detection, investigation and response on a single AI-native platform. Lean, intuitive and continuous enterprise cyber security, managed by our certified analysts.

Multi-Layer AI™ | SIEM · NDR/OT · ITDR/UEBA | ISO/IEC 27001:2022

A unified Open XDR platform

DETECTION · INVESTIGATION · RESPONSE

NSI Advisor delivers **Security Operations Center** services built on one of the market's most advanced **Open XDR** platforms — **AI-native** and designed for lean, intuitive enterprise cyber security. The platform unifies security operations across complex hybrid environments, bringing detection, investigation, triage and response together in a single ecosystem with **Multi-Layer AI™**, for proactive and continuous protection of client infrastructures.

SIEM
Centralized correlation and analysis of logs and events

NDR / OT
Visibility over network traffic and industrial environments

ITDR / UEBA
Threat detection across identities and anomalous behavior

Response
Triage, investigation and orchestrated incident response

AI TRIAGE

AI-powered triage

In the **Standard** and **Advanced** tiers, Multi-Layer AI™ automatically classifies, enriches and prioritizes every event, reducing false positives. Final validation always rests with the human analyst: **AI + Human** on all events and cases.

AI OPERATIONS

AI-assisted daily operations

Artificial Intelligence supports analysts in day-to-day operations: continuous correlation, guided threat hunting and automations that accelerate investigation and response, keeping the service lean and efficient.

ISO/IEC 27001:2022
BSI Group certified

Certified analysts
Structured, documented processes

Traceability & compliance
Top security levels and audit trail

Three SOC tiers, one quality standard

CHOOSE THE COVERAGE THAT FITS YOU

The service is modular and grows with your organization: from essential sensor monitoring to **24/7 on-call** coverage with guaranteed SLAs. Every tier includes the AI-native Open XDR platform; the contribution of **AI and analysts** increases with the tier you choose.

TIER 1 — Base

Mon–Fri · 9:00–19:00

- **Continuous health checks** of sensors and the platform
- Monitoring of infrastructure health and coverage
- **Client alert** for any critical event with a score **above 95**
- Daily operations assisted by the platform's native AI

Essential oversight, always on for operational health

TIER 2 — Standard (MOST CHOSEN)

Mon–Fri · 9:00–19:00

- Everything included in the **Base** tier
- **AI-based + Human review** on **all** events and cases
- Triage powered by **Multi-Layer AI™** with analyst validation
- False-positive reduction and intelligent prioritization
- Investigation and response recommendations on detected incidents

AI + Human on every event and case

TIER 3 — Advanced

On-site 9–19 · On-call 24/7

- Everything included in the **Standard** tier
- **On-site coverage** Mon–Fri, 9:00–19:00
- **24/7 on-call** for any urgency or generated event
- **Response SLA within 2 hours** on critical events
- Priority incident handling and response coordination

24/7 coverage with a guaranteed SLA ≤ 2 hours

Quick tier comparison

Feature	Base	Standard	Advanced
On-site coverage	Mon–Fri 9–19	Mon–Fri 9–19	Mon–Fri 9–19
24/7 on-call for urgencies/events	—	—	✓
Sensor health checks	✓	✓	✓
Critical-event alert (score > 95)	✓	✓	✓
AI-based triage on all events	—	✓	✓
Human analysis & validation on every case	—	✓	✓
AI-assisted operations	✓	✓	✓
Response SLA within 2 hours	—	—	✓

BEYOND THE SOC

Build your security posture, one module at a time

The SOC is the operational core. Around it you can activate optional services that add intelligence, prevention and governance — available individually or combined, based on your needs.

1 CTI — Cyber Threat Intelligence

DARK/DEEP WEB · TELEGRAM · X · OSINT

Proactive monitoring of the Dark/Deep Web, Telegram channels, X and underground forums to identify targeted threats, compromised credentials and exfiltrated data related to your organization early.

2 Vulnerability Early Warning

CVE MONITORING · EPSS · CISA KEV

Proactive alerts on vulnerabilities affecting your technologies, with severity scoring (EPSS + CISA KEV) and remediation guidance **before active exploitation.**

3 vCISO — Virtual CISO

GOVERNANCE · WITH OPTIONAL PANORAYS TPCRM

Strategic support for cyber governance: technology choices, hardening, assessments and compliance (ISMS, DORA, NIS2). Extendable to supply-chain risk management with **Panorays TPCRM.**

4 Periodic Vulnerability Assessment

POWERED BY QUALYS

Periodic, structured vulnerability scans across the infrastructure, with clear reporting and risk prioritization for a continuous, measurable remediation cycle.

5 Red Teaming — Penetration Testing

INFRASTRUCTURE AND/OR APPLICATION · PROJECT-BASED

Project-based offensive activities to test your defenses: infrastructure and/or application Penetration Testing, to validate the effectiveness of your security in the field and identify real exposure points.

Want to explore one of these services?

Our team builds the protection perimeter best suited to your organization, together with you. Let's talk.

Request more information →