SOC AS A SERVICE · OPEN XDR AI-NATIVE

Un SOC che pensa, correla e agisce in tempo reale, 24 ore su 24

Rilevamento, indagine e risposta unificati su un'unica piattaforma nativa dell'Intelligenza Artificiale. Cyber security aziendale snella, intuitiva e continua, gestita dai nostri analisti certificati.

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

Una piattaforma Open XDR unificata

DETECTION · INVESTIGATION · RESPONSE

NSI Advisor eroga servizi di **Security Operations Center** basati su una piattaforma **Open XDR** tra le più avanzate del mercato, **nativa dell'IA** e progettata per una cyber security aziendale snella ed intuitiva. La piattaforma unifica le operazioni di sicurezza in ambienti ibridi complessi, riunendo in un unico ecosistema rilevamento, indagine, triage e risposta con la **Multi-Layer AI™**, per una protezione proattiva e continua delle infrastrutture dei clienti.

SIEM
Correlazione e analisi centralizzata dei log e degli eventi

NDR / OT
Visibilità su traffico di rete e ambienti industriali

ITDR / UEBA
Rilevamento minacce su identità e comportamenti anomali

Response
Triage, indagine e risposta orchestrata agli incidenti

AI TRIAGE

Triage potenziato dall'AI

Nei profili **Standard** e **Avanzato**, la Multi-Layer AI™ classifica, arricchisce e prioritizza automaticamente ogni evento, riducendo i falsi positivi. La validazione finale resta sempre all'analista umano: **AI + Human** su tutti gli eventi e i casi.

AI OPERATIONS

Operazioni quotidiane assistite dall'AI

L'Intelligenza Artificiale supporta gli analisti nella gestione operativa di ogni giorno: correlazione continua, threat hunting guidato e automazioni che accelerano indagine e risposta, mantenendo il servizio snello ed efficiente.

ISO/IEC 27001:2022
Certificazione BSI Group

Analisti certificati
Processi strutturati e documentati

Tracciabilità & conformità
Massimi livelli di sicurezza e audit trail

Tre livelli di SOC, un unico standard di qualità

SCEGLI LA COPERTURA ADATTA A TE

Il servizio è modulare e cresce con la tua organizzazione: dal monitoraggio essenziale dei sensori fino alla copertura **H24 in reperibilità** con SLA garantiti. Ogni livello include la piattaforma Open XDR AI-native; l'apporto di **AI e analisti** aumenta con il profilo scelto.

LIVELLO 1

Base

Lun–Ven · 9:00–19:00

- **Verifica del funzionamento** continuativa dei sensori e della piattaforma
- Monitoraggio della salute e della copertura dell'infrastruttura
- **Avviso al cliente** in caso di evento critico con score **superiore a 95**
- Operazioni quotidiane assistite dall'AI nativa della piattaforma

Presidio essenziale, sempre attivo sul funzionamento

LIVELLO 2 — PIÙ SCELTO

Standard

Lun–Ven · 9:00–19:00

- Tutto ciò che è incluso nel livello **Base**
- **Controllo AI-based + Umano** su **tutti** gli eventi e i casi
- Triage potenziato dalla **Multi-Layer AI™** con validazione dell'analista
- Riduzione dei falsi positivi e prioritizzazione intelligente
- Indagine e raccomandazioni di risposta sugli incidenti rilevati

AI + Human su ogni evento e caso

LIVELLO 3

Avanzato

Presenza 9–19 · Reperibilità H24

- Tutto ciò che è incluso nel livello **Standard**
- **Presidio in presenza** Lun–Ven, 9:00–19:00
- **Reperibilità H24** per qualsiasi urgenza o evento generato
- **SLA di intervento entro 2 ore** sugli eventi critici
- Gestione prioritaria di incident e coordinamento della risposta

Copertura H24 con SLA garantito ≤ 2 ore

Confronto rapido dei livelli

Caratteristica	Base	Standard	Avanzato
Copertura in presenza	Lun–Ven 9–19	Lun–Ven 9–19	Lun–Ven 9–19
Reperibilità H24 su urgenze/eventi	—	—	✓
Verifica funzionamento sensori	✓	✓	✓
Avviso su evento critico (score > 95)	✓	✓	✓
Triage AI-based su tutti gli eventi	—	✓	✓
Analisi & validazione umana su ogni caso	—	✓	✓
Gestione operativa assistita dall'AI	✓	✓	✓
SLA di intervento entro 2 ore	—	—	✓

OLTRE IL SOC

Costruisci la tua postura di sicurezza, un modulo alla volta

Il SOC è il cuore operativo. Attorno ad esso puoi attivare servizi opzionali che aggiungono intelligence, prevenzione e governance — attivabili singolarmente o in combinazione, in base alle tue esigenze.

1 CTI — Cyber Threat Intelligence

DARK/DEEP WEB · TELEGRAM · X · OSINT

Monitoraggio proattivo di Dark/Deep Web, canali Telegram, X e forum underground per identificare in anticipo minacce mirate, credenziali compromesse e dati esfiltrati relativi alla tua organizzazione.

2 Early Warning Vulnerabilità

CVE MONITORING · EPSS · CISA KEV

Alert proattivo sulle vulnerabilità che riguardano le tue tecnologie, con valutazione della criticità (EPSS + CISA KEV) e raccomandazioni di remediation **prima dello sfruttamento attivo.**

3 vCISO — Virtual CISO

GOVERNANCE · CON PANORAYS TPCRM OPZIONALE

Supporto strategico alla governance cyber: scelte tecnologiche, hardening, assessment e conformità (ISMS, DORA, NIS2). Estendibile alla gestione del rischio della supply chain con la tecnologia **Panorays TPCRM.**

4 Vulnerability Assessment Periodico

POWERED BY QUALYS

Scansioni periodiche e strutturate delle vulnerabilità sull'infrastruttura, con reportistica chiara e prioritizzazione del rischio per un ciclo di remediation continuo e misurabile.

5 Red Teaming — Penetration Testing

INFRASTRUTTURALE E/O APPLICATIVO · SU PROGETTO

Attività offensive su progetto specifico per mettere alla prova le difese: Penetration Test infrastrutturale e/o applicativo, per validare sul campo l'efficacia della tua sicurezza e individuare i punti di esposizione reali.

Vuoi approfondire uno di questi servizi?

Il nostro team costruisce con te il perimetro di protezione più adatto alla tua realtà. Parliamone.

Richiedi un approfondimento →