An Indra company

SIA SMART CYBERSECURITY CENTERS

“The SOCless approach”

La nuova generazione dei centri di Cybersecurity.
Oltre il SOC.

Il SOC è morto. Il futuro è un approccio SOCless:

L'aumento e la complessità delle minacce informatiche e degli attacchi generano una **ingente quantità di informazioni**, questo può rendere un **SOC tradizionale non in grado** di affrontare e gestire adeguatamente uno scenario in costante evoluzione e sempre più sfidante. Per questo noi di SIA sappiamo che una **strategia di cybersecurity vincente** richiede un **nuovo modello** che definiamo **SOCless**. Per massimizzare il ritorno sugli investimenti in cybersecurity e gestirli in modo efficace ed efficiente.

SOC Tradizionale	Smart SOCless Center
Numerosi avvisi, molti dei quali **superflui**.	**L'automazione riduce il rumore** di allarme non necessari.
Avvisi generici: non c'è specializzazione perché la maggior parte del tempo è impiegata **senza alcun valore tecnico aggiunto.**	**Gli avvisi di alto valore, arricchiti automaticamente** con dati di contesto e storici, rendono gli analisti molto efficienti.
Troppe persone coinvolte nella gestione, con grandi **inefficienze**.	La **specializzazione degli analisti** crea nuove capacità e migliora continuamente la risposta.

Tutti i nostri servizi di rilevamento e risposta agli incidenti si basano sul modello **SOCless**. Il nostro **team di esperti altamente specializzati** e il nostro **stack tecnologico all'avanguardia** formano una eccellente combinazione in grado di prevenire gli incidenti di cybersecurity.

I nostri gruppi di **analisti, hunters e di intelligence** utilizzano la medesima piattaforma tecnologica per eseguire tutte le operazioni. Questo genera **preziose sinergie** e garantisce un **processo di miglioramento continuo** da parte di tutto il team.

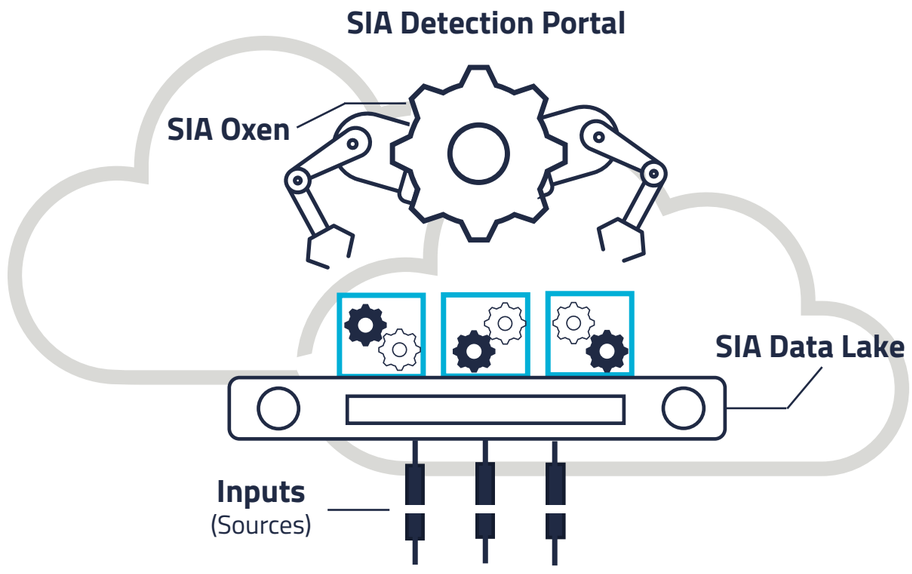
Questo ci permette di ottenere la **massima efficienza** prevenendo gli incidenti di sicurezza e fornendo risposte efficaci.

$$(A^2 + E^2)$$

Autonomous Automation — Effective Efficient

Formula SOCless

I nostri servizi sono forniti **secondo il modello SOCless e sono 100% cloud (PaaS e SaaS): MDR** e **Endpoint MDR**



Stack tecnologico proprietario per i servizi MDR e EndPoint MDR

Efficienza ed efficacia SOCless

Ambito di lavoro degli specialisti di sicurezza SIA in relazione all'ambiente del Cliente

Threat Intelligence	Esterno	Esterno	Esterno	Esterno
Threat Hunting		Interno	Interno	Interno
Threat Analysis			Interno	

Prima dell'inizio del servizio — **Tra l'inizio del servizio e il presente** — **Nel presente** — **Verso il futuro**

I servizi di **Managed Detection and Response (MDR) e Endpoint Managed Detection and Response (EndPoint MDR)** presentano entrambi queste caratteristiche:

EndToEnd

Rilevamento dalla sorgente all'endpoint

Orchestrato

Applicazione di workflows per accelerare le operazioni di identificazione di tattiche, tecniche e procedure.

Automatizzato

Gestione di migliaia di operazioni garantendo la massima efficienza.

Risposta immediata

Attuazione di una risposta immediata sull'asset e riduzione al minimo dei rischi.

Autonomo

Focus sull'automazione: agilità, adattabilità ad ambienti in rapida evoluzione e utilizzo di personale tecnico con totale efficacia. Generazione di informazioni utili per arricchire gli avvisi di sicurezza.

Delocalizzato

Erogazione del servizio da qualsiasi parte del mondo.

Alto rendimento

Massime prestazioni nella gestione dei logs e dei risultati delle query.

Flessibile e agile

Facile e personalizzabile per il cliente, veloce implementazione e rapida messa in esercizio.

Hub di allerta avanzato

È il centro di eccellenza **in prima linea nella gestione dei servizi di rilevazione**. Tutte le operazioni sono gestite dall'hub avanzato. Opera con **analisti e non con operatori**.

Hub di specializzazione

Si tratta di **centri con una specializzazione specifica**. Lavorano nella loro area specifica generando **informazioni utili per tutti i clienti SIA** e per l'evoluzione dei servizi.

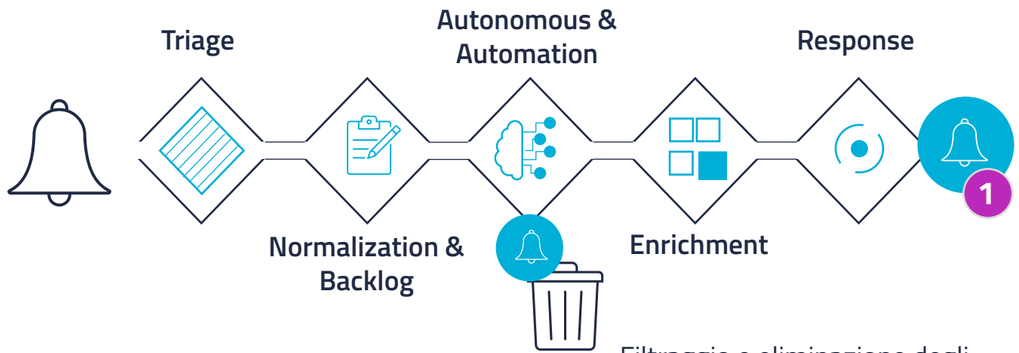
Hub di risposta

I **contatti con i clienti locali** vengono gestiti dai centri di risposta.

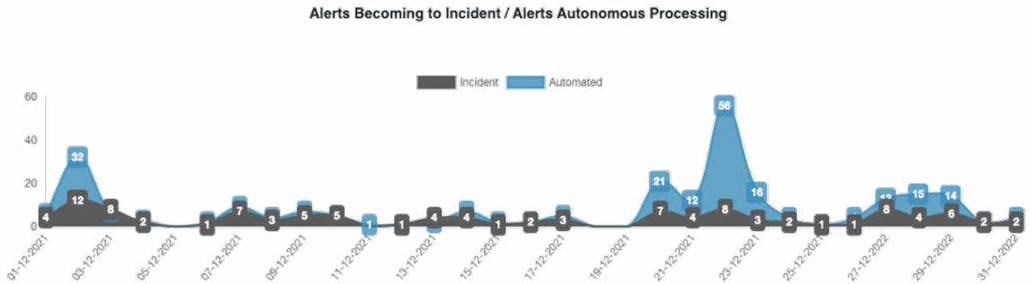
Abbiamo anche **centri di eccellenza** che fanno parte dell'ecosistema di fornitura di servizi globali con una risposta locale. Tutti i nostri servizi sono forniti su base 24x7x365. (Approccio Glocal).

SIA Detect One è il portale di gestione dei servizi SOCless. Presenta al cliente **la modalità e l'ambito dei servizi in modo rapido e sicuro**, fornendo una panoramica completa e accurata.

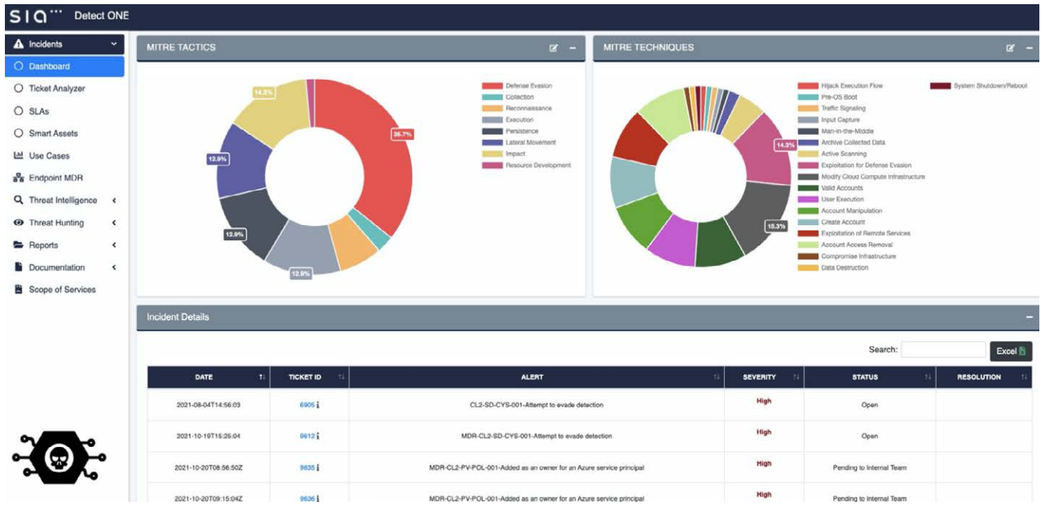
Le caratteristiche principali del modello SOCless sono una **riduzione degli sforzi** dovuti all'eccessivo numero di allarmi e un maggior controllo della loro evoluzione, grazie **all'automazione** e alla **visualizzazione** da parte del cliente direttamente nel portale SIA Detect One.



Filtraggio e eliminazione degli avvisi dovuti a operazioni automatiche



Rappresentazione reale degli avvisi gestiti in automatico e gli avvisi considerati incidenti



SIA Customer portal: Panel de control MITRE ATT&CK

100%

Allarmi arricchiti

98%

Livello di servizio

68%

Riduzione degli sforzi

2%

Falsi positivi

In breve, la nuova generazione dei centri di cybersecurity di SIA secondo il modello **SOCless** rappresenta un **abbandono** dello status quo rappresentato dalle **tradizionali modalità operative** attuate in ambito cybersecurity e un **impegno rigoroso** nei confronti dei principi delle **best practice di sicurezza, dell'automazione e di una logica di rilevamento e risposta agli incidenti di sicurezza fortemente proattiva.**

In questo modo, siamo in grado di proteggere i nostri clienti e di fidelizzarli.

NET STUDIO

Your data, your way

Net Studio è l'azienda italiana leader nelle soluzioni di Digital Identity e Access Management.

Nel 2021, Net Studio è stata acquisita da SIA - società del Gruppo Indra, presente in Italia con il marchio Minsait - con l'obiettivo di integrare il suo catalogo di soluzioni e servizi con l'offerta di Cybersecurity di Minsait.

NET STUDIO
an Indra Company
Corporate Headquarters
Viale Montegrappa 278/E
59100 Prato (Italy)

www.netstudio.it
info@netstudio.it

INDRA IN ITALIA
Sede Legale
Via del Serafico 200
00142 Roma (Italy)

www.minsait.com