HWG Sababa

HWG Sababa HyperSOC™

Trasformare la cybersecurity: dalla reazione alla resilienza

SOC sotto pressione

Oggi i Security Operations Center (SOC) devono garantire la protezione di ecosistemi digitali sempre più complessi, affrontando allo stesso tempo tagli di budget, carenza di personale, regolamentazioni più stringenti e minacce sempre più sofisticate.

Nonostante le crescenti aspettative, molte aziende continuano ad operare in ambienti di sicurezza frammentati: strumenti che non dialogano tra loro, un eccesso di falsi positivi e tempi di risposta troppo lunghi. I team sono sovraccaricati dagli alert. Gli audit di conformità diventano colli di bottiglia. E quando si verificano incidenti, la mancanza di visibilità contestuale in ambienti IT, OT, IoT e cloud rende l'analisi delle cause e il contenimento del rischio estremamente lenti.

Ai responsabili della sicurezza non basta più individuare le minacce: oggi devono dimostrare concretamente la riduzione del rischio, garantire risultati tangibili e allineare gli investimenti agli obiettivi strategici dell'organizzazione.

Perché il SOC tradizionale non è più adeguato

- **Crescente complessità.**
  Le organizzazioni si trovano sempre più spesso ad affrontare attacchi su più fronti – OT, cloud e ambienti ibridi. Con volumi di dati in aumento del 30% anno su anno[1] e una media di oltre 45 strumenti di sicurezza per azienda[2], questi ecosistemi diventano sempre più difficili da proteggere.

- **Carenza di competenze.**
  A livello globale il divario di professionisti della cybersecurity ha raggiunto i 4 milioni[3] e la situazione è destinata a peggiorare entro il 2028. Il gap di competenze continuerà ad ampliarsi, con circa un terzo dei ruoli senior che resteranno scoperti per oltre un anno[4].

- **Normative più stringenti.**
  Regolamenti UE come NIS2, DORA e CRA, insieme a framework settoriali (per esempio, l'IEC 62443), impongono reporting veloce, visibilità lungo l'intero ciclo di vita e controlli di sicurezza integrati nei processi.

- **Il top management chiede prove.**
  I CISO devono oggi dimostrare come la sicurezza incida direttamente su KPI di business quali uptime operativo, aderenza normativa ed esposizione finanziaria.

In questo contesto, i tradizionali MSSP mostrano i loro limiti: servizi di detection troppo limitati, piattaforme rigide e poca capacità di adattarsi ai diversi settori o modelli di rischio.

[1]How Hyperautomation Is Used to Reduce Gaps and Inefficiencies in Network Cybersecurity, IDC, September 2023
[2]The more cybersecurity tools an enterprise deploys, the less effective their defense is, ZDNET
[3]ISC² 2024 Cybersecurity Workforce Study
[4]Predict 2025: There Will Never Be an Autonomous SOC, Gartner, December 2024
(https://www.gartner.com/doc/reprints?id=1-2KBPAKPG&ct=250220&st=sb)

Perché HyperSOC™

Monitoraggio 24/7/365
Sempre attivi, sempre pronti: rilevamento e risposta alle minacce in tempo reale.

Operazioni potenziate da IA e automazione
Intelligenza artificiale e automazione per ridurre il rumore, accelerare le azioni e fornire risposte contestualizzate e rapide.

Visibilità completa IT + OT
Monitoraggio end-to-end su ecosistemi IT, OT, IoT, cloud e ambienti ibridi.

Integrazione vendor-agnostic
Integrazione flessibile e vendor-agnostic, che preserva le soluzioni già in uso senza costi aggiuntivi di sostituzione.

Playbook e metodologie su misura
Framework di risposta comprovati e SLA adattabili al tuo ambiente.

Competenze certificate
300+ certificazioni multi-disciplinari assicurano eccellenza e qualità operativa.

CARES
Piena visibilità su postura di sicurezza, KPI, ticket e documentazione tramite CARES – il portale clienti dedicato.

Design modulare e scalabile
Servizio modulare e progressivo, pensato per accompagnare la tua crescita.

HyperSOC™: la nuova generazione di SOC-as-a-Service

Con HyperSOC™, HWG Sababa supera i limiti dei modelli SOC tradizionali, offrendo visibilità completa, orchestrazione intelligente e supervisione continua su ambienti IT, OT, IoT, cloud e ibridi. Non si limita a rilevare le minacce: le anticipa.

Attraverso la piattaforma proprietaria PULSE™, che integra monitoraggio in tempo reale, threat intelligence e hyperautomation, HyperSOC aiuta le organizzazioni a ridurre la complessità, velocizzare le risposte e acquisire fiducia operativa, restando sempre pronte agli audit. La sua struttura modulare si adatta ai rischi specifici di settore e alle esigenze normative, risultando ideale sia per gli operatori di infrastrutture critiche sia per le aziende in crescita.

Vendor-agnostic, facile da integrare e supportato da consulenza strategica, HyperSOC trasforma il monitoraggio della sicurezza in una leva di business: resiliente, scalabile e pronto ad affrontare le sfide future.

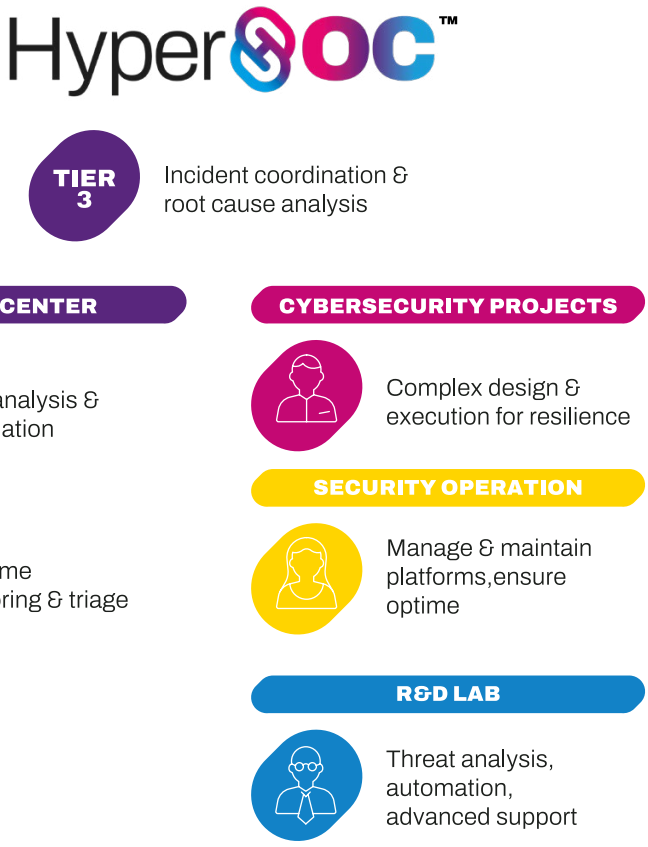

Figura 1 *- HyperSOC: livelli e ruoli*

HWG Sababa

PULSE: il motore operativo di HyperSOC™

PULSE™ è la piattaforma proprietaria di HWG Sababa – la spina dorsale di HyperSOC™. Perfettamente integrata con strumenti esterni e allineata a framework come NIST e MITRE ATT&CK, semplifica e standardizza le operazioni SOC, rendendole più efficienti.

Con **PULSE** le organizzazioni ottengono:

- Visibilità e orchestrazione in tempo reale su tutti gli ambienti
- Integrazione nativa con gli ecosistemi già presenti, senza necessità di sostituzioni
- Automazione dei processi di detection, triage e containment
- Conformità normativa incorporata e miglioramento continuo

PULSE rende il SOC un motore di sicurezza proattivo, intelligente e scalabile, capace di affrontare la complessità di oggi e le sfide di domani.

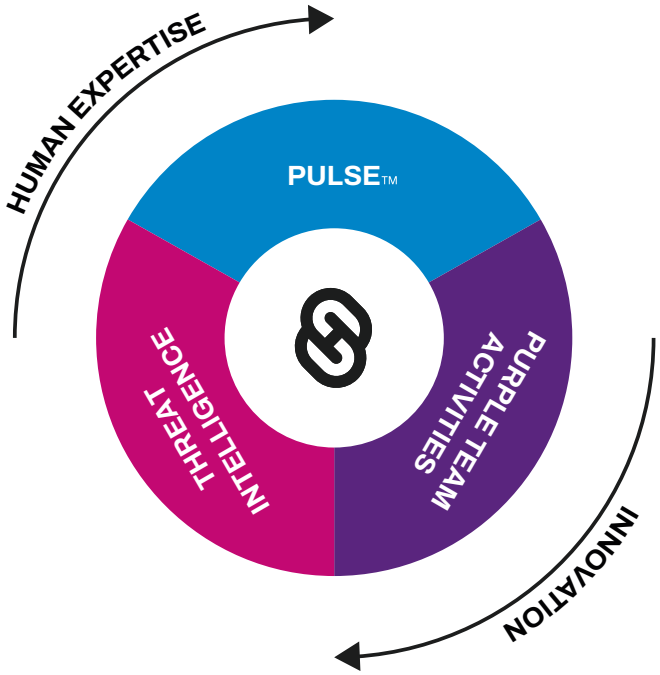

Figura 2 *- Il motore operativo di HyperSOC*

La **Threat Intelligence**, integrata in ogni livello di HyperSOC, trasforma dati frammentati in insight azionabili. Grazie alla combinazione di feed proprietari, telemetria dei vendor e intelligence di terze parti, il SOC ottiene una visione unificata e in tempo reale del panorama delle minacce. Questa intelligence supporta le attività di rilevamento e triage con elevata precisione operativa: dal profiling degli avversari al monitoraggio del dark web, fino alla produzione di bollettini settimanali di sicurezza e del Threat Landscape Report annuale. Il risultato è una chiarezza contestuale che consente di stabilire le priorità di rischio e accelerare la risposta.

Oltre il semplice rilevamento, HyperSOC garantisce una **validazione continua delle minacce**. I nostri analisti conducono attività mirate di threat hunting e indagini approfondite basate su reali indicatori di compromissione. A queste si affiancano simulazioni Purple Team integrate che mettono alla prova le difese contro le stesse tattiche utilizzate dagli attaccanti nel mondo reale. Insieme, queste pratiche assicurano non solo una gestione più accurata degli alert, ma anche miglioramenti tangibili in termini di visibilità sulle minacce, prontezza operativa e resilienza complessiva.

Funzioni Core: Always On

Il cuore di HyperSOC è costituito da funzionalità essenziali progettate per garantire monitoraggio continuo e risposta proattiva, 24 ore su 24, 7 giorni su 7. Queste capacità si basano su una logica di rilevamento avanzata, sull'automazione guidata dall'IA e sul portale clienti CARES, che offre trasparenza totale e collaborazione proficua.

Rilevamento guidato dai casi d'uso, monitoraggio costante della piattaforma e meccanismi di hardening contro le minacce costituiscono il nucleo della protezione quotidiana – favorendo un contenimento rapido degli attacchi e un miglioramento continuo.

Queste funzioni "always on" non sono componenti opzionali: costituiscono il DNA di HyperSOC. Potenti di default, sono progettate per scalare ed evolvere insieme alla maturità di sicurezza dell'organizzazione.

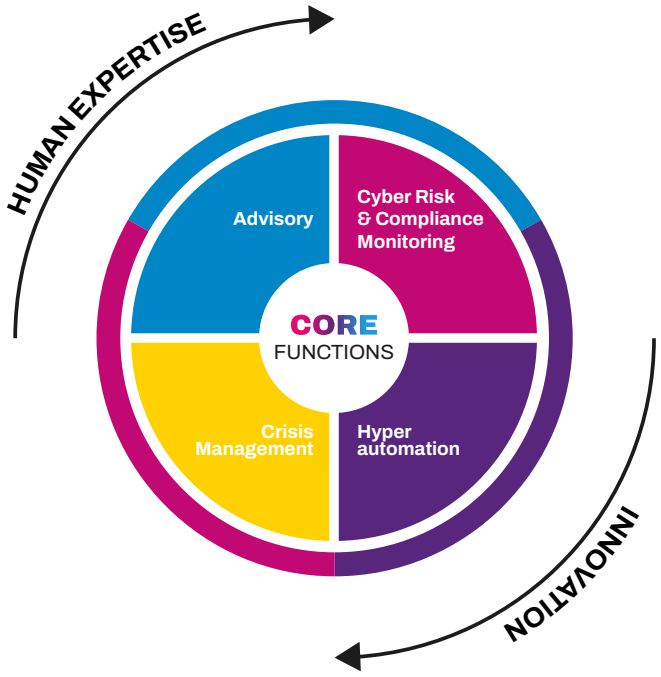

Figura 3 *- Le funzioni CORE di HyperSOC*

Di fronte a scenari di rischio sempre più complessi, HyperSOC integra nativamente nelle sue fondamenta servizi avanzati come **Hyperautomation, Advisory, Cyber Risk & Compliance Monitoring** e **Crisis Management.** Queste funzionalità evolvono insieme alla maturità del cliente, ampliandosi in modo progressivo per sostenere obiettivi mirati di governance, conformità e resilienza.

Da *Core* a *Complete*

Se le funzionalità *core* di HyperSOC garantiscono una solida base, le organizzazioni più mature richiedono spesso maggiore visibilità, tempi di risposta più rapidi e un allineamento strategico più profondo. È qui che HyperSOC si espande, con moduli avanzati e flessibili che trasformano il SOC da semplice centro reattivo a vero e proprio asset strategico, parte integrante della resilienza aziendale. Questi componenti possono essere attivati in base alle esigenze dell'organizzazione, offrendo intelligence potenziata, consulenza specializzata e capacità di risposta dinamica.

Hyperautomation

Ciò che rende unico HyperSOC è l'integrazione fluida di tecnologie avanzate di intelligenza artificiale, machine learning e workflow orchestrati, in grado di eliminare il rumore, ridurre lo stress degli analisti e velocizzare la risposta fin dal primo segnale. Attraverso correlazioni intelligenti, arricchimento contestuale e prioritizzazione dinamica, HyperSOC riduce in modo significativo MTTD e MTTR, liberando le risorse interne per concentrarsi su attività strategiche e basate sul rischio. Allo stesso tempo, estende la visibilità del SOC anche ai domini operativi più critici, storicamente riservati alla gestione amministrativa interna dell'organizzazione. Grazie a un closed-loop containment sotto governance diretta del cliente, garantisce azioni rapide e coordinate contro le minacce emergenti, senza creare colli di bottiglia operativi e portando la sicurezza verso una vera hyperautomation (Figura 5).

55%
degli alert SOC completamente automatizzati*
dall'ingestione alla risposta, senza intervento umano

95%
di riduzione dei tempi di rilevamento e risposta
per incidenti a media e bassa priorità, con un abbattimento significativo di tempi e carichi di lavoro

85%
di riduzione nei tempi di risposta alle minacce ad alta priorità, grazie a triage basato su IA e azioni mirate

Figura 4 *- Ottimizzazione delle performance con HyperSOC***

**Questa percentuale si riferisce alle operazioni interne del nostro SOC*
***HWG Sababa Hyperautomates Their Managed SOC to Fuel Customer ROI – Torq*

Cyber Risk & Compliance Monitoring

HyperSOC garantisce una visibilità continua e in tempo reale sul livello complessivo di rischio di un'organizzazione – non solo in termini di esposizione cyber, ma anche dal punto di vista del risk management e della conformità normativa. Aggregando dati provenienti da IT, OT, IoT, cloud ed ecosistemi di terze parti, offriamo insight azionabili su vulnerabilità, percorsi di attacco, comportamenti anomali e gap di governance. Questa funzionalità consente alle organizzazioni di passare da un approccio reattivo ad uno di miglioramento continuo, in cui i rischi cyber e di compliance vengono monitorati in modo dinamico e affrontati proattivamente, prima che si trasformino in interruzioni operative o violazioni normative.

Advisory

La funzione advisory di HyperSOC offre ai clienti una guida esperta e continuativa per allineare le strategie di cybersecurity alle minacce emergenti, ai requisiti normativi e agli obiettivi di business. I nostri advisor operano come un'estensione del team del cliente, offrendo competenze su progettazione delle architetture, mappatura della compliance (NIS2, DORA, CRA), threat modelling e preparazione alla gestione degli incidenti. In questo modo, la cybersecurity non resta un'attività isolata, ma diventa una leva strategica basata su intelligence di rischio e orientata alla resilienza nel lungo periodo.

Crisis Management

HyperSOC non si limita a gestire gli incidenti: prepara le organizzazioni ad affrontare le crisi con sicurezza e controllo. Definiamo procedure critiche, formiamo gli stakeholder e testiamo la prontezza operativa attraverso cyber drill ed esercitazioni tabletop. In caso di crisi, mettiamo in campo il giusto mix di esperti verticali e analisti SOC per contenere le minacce, coordinare la fase di recovery e gestire la comunicazione, riducendo l'impatto operativo, accelerando la ripartenza e rafforzando la fiducia.

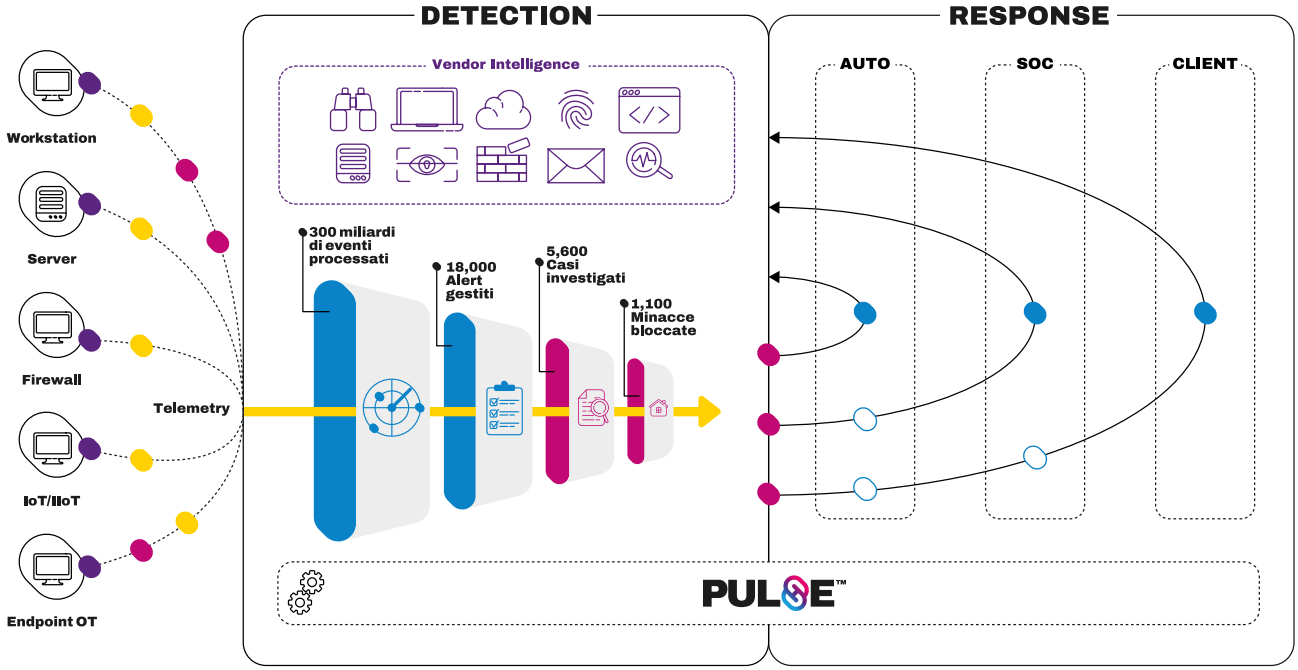

Figura 5 *- Dalla telemetria alla risposta: il percorso completo. I segnali vengono acquisiti, analizzati e subito trasformati in risposta concreta. Grazie all'hyperautomation integrata, non c'è attesa di contesto aggiuntivo né bisogno di azioni manuali.*

Valore per tutto il business

- Visibilità 24/7 sul panorama delle minacce, con tempi di risposta ridotti e una piattaforma unificata e allineata a framework di settore e metriche di performance
- Integrazione fluida tra ambienti IT, OT e cloud, senza impattare sui sistemi esistenti.
- Compliance semplificata grazie a dashboard in tempo reale, documentazione strutturata degli incidenti e report sempre audit-ready.
- Modelli di servizio flessibili e architettura vendor-neutral, adattabili a diverse esigenze di procurement e operation.
- ROI misurabile attraverso il consolidamento degli strumenti di sicurezza, la riduzione dei rischi e l'ottimizzazione dei costi operativi.
- Resilienza organizzativa rafforzata da metriche chiar e che proteggono la reputazione, garantiscono la continuità dei servizi e consolidano la fiducia degli stakeholder.

Scopri come HyperSOC™ può supportare i tuoi obiettivi di sicurezza e di business: scarica ora il report Spotlight IDC.

HWG Sababa

Follow us on:

www.hwgsababa.com