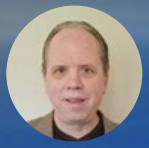
IDC Spotlight, sponsorizzato da HWG Sababa
Agosto 2025

SOC a prova di futuro: cinque elementi fondamentali per i dirigenti della sicurezza informatica



Craig Robinson
Research VP, IDC

SOC a prova di futuro: cinque elementi fondamentali per i dirigenti della sicurezza informatica

Agosto 2025

Autore: Craig Robinson, VP

I. Introduzione

Le tensioni geopolitiche non sono certo una novità. Dall'Europa, culla dei due conflitti mondiali, al Medio Oriente, in cui le fragili tregue possono cadere da un momento all'altro, la pace resta un concetto difficile da consolidare. Per un CISO, un CIO o qualsiasi dirigente della sicurezza, oltre alle notizie di guerra che fanno scattare campanelli d'allarme si aggiunge un'ulteriore sfida: far fronte a minacce informatiche sempre più sofisticate e in rapida espansione che prendono di mira le infrastrutture delle aziende.

IN SINTESI

Le organizzazioni che intendono ottenere una resilienza informatica a lungo termine devono scegliere MSSP competenti su cinque aree cruciali: **conformità** alle normative in evoluzione, strategie di gestione dei **dati** in grado di garantire analisi scalabili e standardizzate, gestione continua delle **piattaforme** con integrazione e risposta h24, **threat intelligence** capace di contestualizzare i rischi e automazione basata sull'**AI** per ottenere velocità e precisione. L'insieme di questi elementi permette agli MSSP di offrire operazioni di sicurezza proattive, pronte al futuro, capaci di allinearsi agli obiettivi di business e adattarsi a uno scenario caratterizzato da minacce in costante trasformazione.

Gli incrementi a doppia cifra dei budget per la sicurezza informatica, tipici dei primi anni del 2020, sono diventati sempre più rari. Per ottenere l'approvazione dei CEO e dei COO , figure a cui i CISO rispondono sempre più spesso, i dirigenti della sicurezza devono superare il linguaggio tecnico e adottare quello del business e della finanza. Questo linguaggio non appartiene ai Security Operations Center (centro delle operazioni di sicurezza, SOC), ma ruota attorno a concetti come riduzione del rischio, sovranità dei dati, ROI, compliance e resilienza informatica e operativa. La sfida è duplice: aumentare rapidamente il livello di maturità informatico per restare al passo con un panorama di minacce in continua evoluzione senza perdere di vista le priorità del top management. Per questo motivo, molti dirigenti della sicurezza scelgono di affidarsi ai fornitori di servizi gestiti per rispondere alle esigenze diversificate e accedere a competenze e capacità che, se sviluppate internamente, richiederebbero tempi e costi elevati. Affidarsi ai Managed Security Service Provider (fornitore di servizi gestiti di sicurezza, MSSP) rende più realistici obiettivi come la riduzione del rischio, il miglioramento del ROI e altri risultati strategici.

I CISO dell'area Europa, Medio Oriente e Africa (EMEA) devono verificare che l'MSSP scelto possa offrire soluzioni adeguate a tutelare le necessità presenti e **future**. IDC pone l'accento su questo aspetto, poiché l'evoluzione della tecnologia e delle minacce informatiche procede a ritmi sempre più elevati. Non a caso, molti CISO considerano l'MSSP

un'estensione naturale del proprio team. Come per ogni squadra, è possibile ottenere performance di qualità riducendo il turnover al minimo, aspetto che richiede una scelta ottimale sin dall'inizio.

La figura 1 illustra i cinque elementi che IDC considera essenziali per un MSSP a prova di futuro: i fattori chiave di successo per le aziende che acquistano servizi di sicurezza.

FIGURA 1
Cinque elementi per un MSSP a prova di futuro

Fonte: IDC, 2025

Conformità

I clienti degli MSSP dell'area EMEA devono scegliere un partner conforme ai principali regolamenti e framework di sicurezza informatica. La conformità offre protezione dei dati, continuità operativa e allineamento normativo. Seguono alcuni motivi alla base dell'importanza dell'aderenza di un MSSP ai quadri normativi e agli standard più diffusi.

- **ISO 27001**. Dimostra il rispetto, da parte dell'MSSP, di uno standard internazionale riconosciuto per la gestione della sicurezza delle informazioni. Ciò garantisce una protezione efficace dei dati sensibili, riduce il rischio di violazioni e assicura la conformità ai requisiti contrattuali, rafforzando la fiducia e l'affidabilità nei mercati EMEA. Non sorprende che l'adesione a questo framework venga spesso prevista come clausola contrattuale obbligatoria.
- **Network and Information Security Directive 2 (NIS 2)**. Per i clienti che operano in settori critici, la conformità di un MSSP alla NIS 2 assicura l'aderenza alle rigorose regole UE in materia di sicurezza informatica, come ad esempio la notifica tempestiva degli incidenti (24-72 ore) e la protezione della filiera. Ciò riduce i rischi di interruzioni e garantisce il pieno rispetto degli obblighi normativi, salvaguardando le operazioni dei clienti.
- **Cyber Resilience Act (CRA)**. La conformità di un MSSP al CRA fa in modo che i servizi offerti siano sicuri in ogni fase del proprio ciclo di vita, dallo sviluppo alla manutenzione. Per i clienti, ciò si traduce in una riduzione delle vulnerabilità delle soluzioni fornite e una maggiore fiducia nella sicurezza della propria infrastruttura digitale.
- **Digital Operational Resilience Act (DORA)**. Per i clienti dell'UE attivi nel settore finanziario, la conformità di un MSSP al DORA è un elemento fondamentale, poiché impone una gestione rigorosa dei rischi ICT, la segnalazione rapida degli incidenti (entro 4-24 ore) e test periodici di resilienza. Ciò garantisce la sicurezza dei dati finanziari e la continuità operativa, proteggendo i clienti da sanzioni normative e interruzioni.
- **National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)**. Pur non essendo obbligatoria, l'adozione del NIST CSF da parte di un MSSP dimostra un approccio alla sicurezza informatica proattivo e basato sul rischio. Per i clienti, ciò significa allineamento alle best practice, maggiore resilienza e supporto alla conformità con altre normative come la NIS 2, rafforzando la fiducia nelle capacità dell'MSSP.

I dati sono il cuore del SOC

Per i clienti degli MSSP, i dati sono un asset da proteggere e il fondamento delle analisi che alimentano il rilevamento e la risposta alle minacce. La strategia relativa ai dati di un MSSP deve gestire in modo efficace la crescita continua del volume, della varietà e velocità dei dati di sicurezza, garantendo protezione, conformità normativa e continuità operativa in un contesto che presenta rischi in costante cambiamento.

Formati dati standard per un'integrazione efficace

L'adozione di formati di dati standard, come ad esempio *Common Event Format* (formato comune degli eventi, CEF) o *Structured Threat Information Expression* (espressione delle informazioni delle minacce strutturate, STIX), consente agli MSSP di integrare e analizzare le informazioni in maniera più rapida ed efficace. Per i clienti, ciò significa contare su un MSSP in grado di correlare in modo efficiente gli eventi provenienti da sistemi diversi, accelerando l'identificazione delle minacce. L'uso dei formati standardizzati facilita l'automazione, riduce la complessità delle analisi e favorisce l'onboarding rapido di nuove fonti di dati, in modo che le informazioni di sicurezza vengano gestite in maniera coerente ed efficace.

Protocolli uniformi di raccolta dei dati per ottenere l'affidabilità

L'adozione dei protocolli standardizzati consente agli MSSP di fornire ai clienti dati completi, precisi e coerenti. Questi protocolli definiscono la frequenza della raccolta, i dati specifici da acquisire (es. eventi legati alla creazione di processi o alle connessioni di rete) e le procedure di gestione degli errori. Per i clienti, questo approccio riduce al minimo le lacune e incoerenze che potrebbero causare il mancato rilevamento delle minacce o i falsi positivi, assicurando una raccolta affidabile delle informazioni critiche di sicurezza su tutte le piattaforme, indipendentemente dalle differenze.

Strategia basata su data lake flessibile per il futuro

Una strategia ben strutturata e basata sui data lake consente agli MSSP di preparare la propria architettura dati alle sfide future, integrando nuove fonti senza influenzare i servizi forniti ai clienti. Quale repository centralizzato, il data lake raccoglie dati raw, log strutturati, informazioni non strutturate e dati cloud semi-strutturati, consentendo di eseguire analisi cronologiche approfondite e favorendo l'individuazione degli schemi. Questa flessibilità permette agli MSSP di adattarsi a nuovi tipi di dati e rispettare la conformità a regolamenti come NIS 2 e DORA, garantendo sicurezza e scalabilità nel lungo periodo.

Le piattaforme e gli strumenti di sicurezza richiedono una gestione 24/7

La complessità di tecnologie come *Endpoint Detection and Response* (risposta e rilevamento degli endpoint, EDR), *Extended Detection and Response* (risposta e rilevamento estese, XDR), *Security Information and Event Management* (gestione eventi e informazioni di sicurezza, SIEM) e dei firewall spinge numerose organizzazioni ad affidare la gestione di tali elementi a un MSSP dotato delle competenze e dell'esperienza necessarie per garantirne un utilizzo efficace e sicuro. Un MSSP può semplificare l'integrazione, l'operatività e l'ottimizzazione di questi strumenti, affrontando minacce informatiche sempre più sofisticate e assicurando la conformità normativa e l'efficienza operativa.

La supervisione di questi strumenti richiede competenze avanzate nell'integrazione e nell'analisi dei dati, che gli MSSP possono offrire grazie a team di analisti qualificati e a una gestione centralizzata. Questo approccio offre prestazioni coerenti, rilevamento rapido delle minacce e risposte efficaci, elementi fondamentali per contrastare attacchi come il

ransomware. Inoltre, gli MSSP aiutano i clienti nella scelta di strumenti e piattaforme a prova di futuro, suggerendo soluzioni scalabili come ad esempio gli XDR con architetture modulari, in grado di adattarsi a nuove minacce, origini dei dati ed evoluzioni tecnologiche senza interventi complessi.

Sempre più organizzazioni si affidano ai propri MSSP non solo per la gestione e l'integrazione dei sistemi di sicurezza, ma anche per servizi di *Managed Detection and Response* (risposta e rilevamento gestiti, MDR) attivi 24/7/365. Le aziende dotate di risorse limitate delegano spesso all'MSSP l'intero ciclo di rilevamento e risposta, intervenendo direttamente solo nelle attività investigative. Le realtà più grandi, dotate di team di sicurezza più strutturati, scelgono un modello di gestione congiunta che consente di ottenere risorse aggiuntive mantenendo il controllo decisionale interno.

Threat Intelligence: qualità e quantità

Come spesso sostengono gli analisti del settore, le aziende costruiscono un muro a protezione dei propri asset più preziosi. La threat intelligence determina l'altezza di quel muro.

Si tratta di un elemento fondamentale che offre a un SOC moderno informazioni contestuali e utilizzabili sulle minacce potenziali o in atto. Esso non si limita a fornire dati raw, ma li arricchisce con analisi che indicano tattiche, tecniche e procedure dei criminali. All'interno di un SOC, i feed di threat intelligence costituiscono la base per le regole di rilevamento, la definizione delle strategie di risposta e il potenziamento delle operazioni di individuazione delle minacce. Grazie alla threat intelligence, il SOC è in grado di anticipare le minacce emergenti, comprendere le motivazioni degli attacchi e definire in modo efficace le priorità difensive. Allo stesso tempo, esso supporta la valutazione dei rischi e le decisioni strategiche, consentendo alle organizzazioni di assegnare al meglio le risorse e adattare la propria postura di sicurezza alle minacce più rilevanti.

La threat intelligence è destinata a giocare un ruolo sempre più strategico nella gestione aziendale della sicurezza informatica. In poche parole, se gli strumenti di sicurezza tradizionali consentono di gestire i dati, preservare le configurazioni e rilevare le anomalie entro i confini aziendali, la threat intelligence consente di andare oltre tale perimetro, tracciando i movimenti della proprietà intellettuale fuori dall'organizzazione.

L'MSSP deve contestualizzare la threat intelligence non solo all'interno del proprio ambiente ma anche integrando feed esterni eterogenei: un requisito che dovrebbe essere presente in ogni offerta di servizi di sicurezza gestita.

AI

La sicurezza informatica, così come l'IT, il suo "gemello digitale", ha sempre richiesto velocità. Un tempo il problema era legato all'*automazione:* gran parte di ciò che oggi viene definito "*intelligenza artificiale*" è un'automazione portata a un livello superiore.

L'automazione riduce il carico delle attività ripetitive e basate su regole, permettendo agli analisti di concentrarsi su compiti più complessi. In un SOC, essa trova applicazione soprattutto nel triage degli avvisi, nella creazione dei ticket e nella raccolta routinaria dei dati. Inoltre, essa consente di filtrare i falsi positivi in base a regole predefinite, dimensionare automaticamente gli avvisi critici o avviare procedure standard di risposta agli incidenti.

Nel campo della sicurezza, l'automazione offre tre vantaggi principali. Il primo è la riduzione degli errori umani. Ad esempio, nel triage degli avvisi, un analista del SOC deve collegare le informazioni di threat intelligence a una minaccia specifica e definire un'azione di mitigazione, come ad esempio isolare un endpoint o applicare il playbook corretto, in

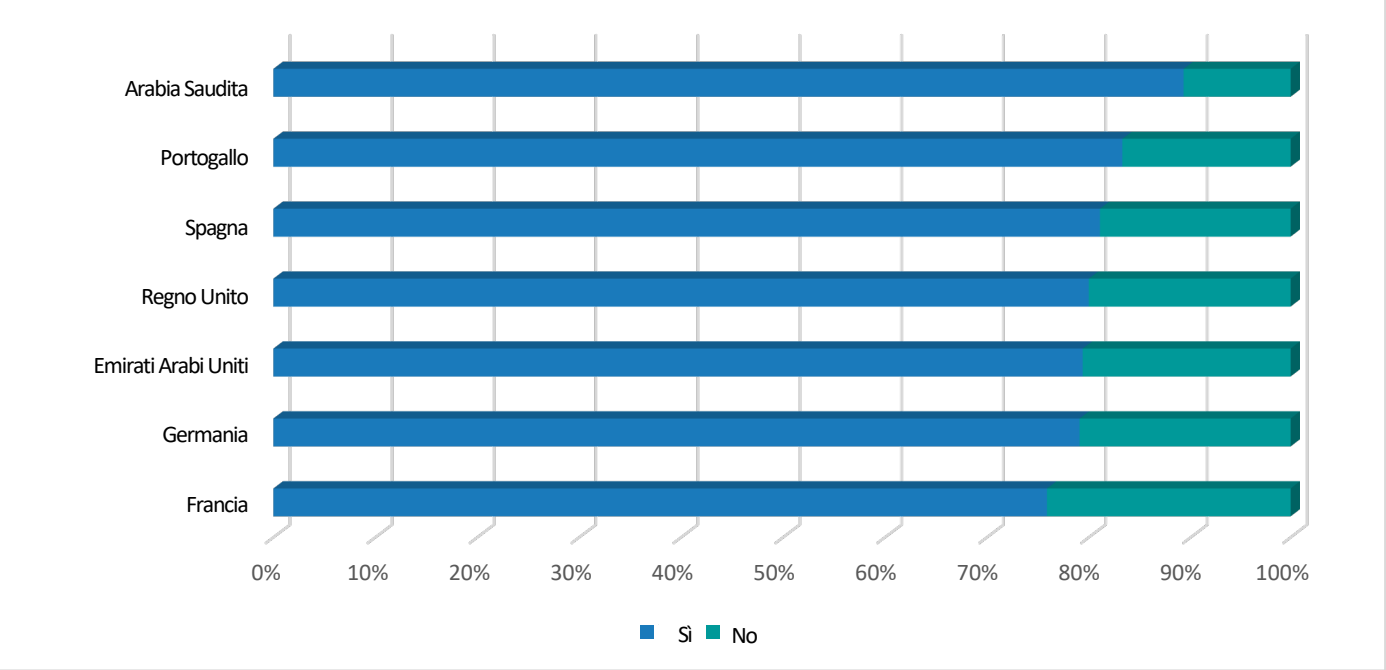
modo da garantire la conformità. È possibile svolgere tutto questo manualmente, ma una soluzione automatizzata consente di applicare sempre la procedura corretta. Il secondo beneficio è la capacità di agire da ponte tra funzioni IT differenti. Un esempio comune: supponiamo che il team di sicurezza debba aggiornare una regola del firewall o procedere con l'installazione di una patch. Normalmente, occorrerebbe coordinarsi con il team delle operazioni per pianificare la finestra di intervento. Usando i permessi predefiniti e l'automazione, è possibile gestire l'intero processo in modo semplice ed efficiente. Il terzo vantaggio risiede nel risparmio di tempo. Attività come il triage degli avvisi e la raccolta dei dati, se svolte manualmente, sono lente e laboriose. L'automazione trasforma radicalmente queste procedure, quasi come il passaggio dallo spostamento a piedi all'utilizzo delle vetture in autostrada.

Negli ultimi anni, la GenAI ha aggiunto intelligenza a un processo legato alla sola velocità di automazione. Sempre più spesso l'AI viene considerata il componente chiave per rendere il SOC a prova di futuro: in prospettiva essa potrebbe assorbire molte funzioni legate alla classificazione e gestione dei dati. Già oggi, l'AI è un elemento cruciale sia come collante logico che come fattore di estendibilità delle piattaforme. La threat intelligence guidata dall'AI permetterà di personalizzare l'enorme flusso informativo della rete, generando feed utili e mirati per ciascuna azienda. Allo stesso tempo, l'automazione basata sull'AI sta iniziando a esprimere il proprio potenziale, affermandosi come connettore tra utenti, applicazioni e dati, generando risultati concreti in termini di sicurezza.

È possibile riprodurre il valore della GenAI all'interno di un SOC, ma si tratta di un processo che richiede investimenti significativi in termini di competenze ingegneristiche, infrastrutture e temporali. Gli MSSP che hanno già intrapreso questa evoluzione possono valorizzare la propria esperienza presentando applicazioni in grado di offrire risultati più rapidi, efficaci e convenienti rispetto a quanto è possibile ottenere con le sole risorse interne.

FIGURA 2

Organizzazioni della regione EMEA che utilizzano la GenAI per rilevare o rispondere a potenziali attacchi informatici, suddivise per Paese



Fonte: IDC, 2025

Alcuni importanti casi d'uso della GenAI in un SOC.

- **Sintesi degli incidenti.** La GenAI è in grado di elaborare e riassumere rapidamente gli incidenti quasi in tempo reale, favorendo un'escalation tempestiva e una risposta immediata.
- **Creazione di regole di rilevamento**. Le regole di rilevamento consentono di individuare i comportamenti anomali rispetto alla base o le violazioni legate agli accessi e all'utilizzo delle applicazioni. In pratica, si tratta di filtri che permettono di isolare le attività sospette.
- **Indagini guidate.** Si tratta di una delle prime applicazioni della GenAI nel campo della sicurezza informatica, che svolge due funzioni principali, vale a dire raccolta automatica di artefatti e metadati per la documentazione e l'analisi dei casi e utilizzo dell'elaborazione del linguaggio naturale (NLP) per aiutare gli analisti lungo l'intero processo investigativo.
- **Esecuzione e implementazione dei playbook. I**l passo che segue le indagini guidate. Il playbook è specifico per ciascuna applicazione e viene sviluppato in base alla tipologia di attacco (ad esempio, ransomware o SQL injection). È possibile usare la GenAI per il rilevamento e la risposta alle minacce, aiutando gli analisti a sviluppare playbook più efficaci grazie a modelli di apprendimento basati sui dati.

HWG Sababa HyperSOC

Operazioni di sicurezza informatica smart e scalabili per una nuova era digitale

Nel mondo iperconnesso di oggi, le organizzazioni devono gestire una superficie d'attacco sempre più estesa. Non è più sufficiente reagire rapidamente: occorrono operazioni di sicurezza proattive, basate sul rischio, in grado di anticipare le minacce, adattarsi all'evoluzione e crescere con il business. HWG Sababa HyperSOC ridefinisce il ruolo di un moderno Security Operations Center, rendendolo intelligente, modulare e in grado di anticipare minacce e requisiti normativi.

HyperSOC è molto più di una soluzione tradizionale di Managed Detection and Response (risposta e rilevamento gestiti, MDR). Si tratta di una piattaforma SOC-as-a-Service (SOCaaS) di nuova generazione che colloca la prevenzione, la visibilità continua del rischio e la difesa adattiva al centro dell'azione. Grazie al monitoraggio 24/7, all'automazione avanzata e alla protezione integrata negli ambienti IT, OT e IoT, HyperSOC consente alle organizzazioni di gestire il rischio informatico a tutto tondo e non solo gli incidenti.

Il cuore di HyperSOC è Pulse, la piattaforma proprietaria di HWG Sababa, che offre un'orchestrazione intelligente dei processi di rilevamento, triage, mitigazione e risoluzione, decisioni rapide, riduzione del rumore e una postura di sicurezza resiliente e reattiva per design.

Su misura per le esigenze del settore

HyperSOC nasce con una missione chiara: permettere alle organizzazioni che operano in settori complessi, regolamentati e caratterizzati da un forte utilizzo dell'OT , come ad esempio servizi pubblici, trasporti, manifattura e settore farmaceutico, di raggiungere una reale resilienza informatica senza rivoluzionare le infrastrutture esistenti.

A differenza di molti SOC tradizionali che si limitano all'attività di avviso, HWG Sababa offre di più. Il suo modello di servizio modulare, che spazia dall'Essential all'Ultimate, supporta un onboarding graduale e implementazioni gestite in modo congiunto, consentendo ai clienti di iniziare con servizi di consulenza o integrazione ed espandere la protezione

con la crescita della propria maturità informatica. Questo approccio "*grow with you*" offre benefici immediati e, al tempo stesso, un allineamento costante con gli obiettivi strategici di lungo periodo.

Visibilità unificata tra diversi domini

Uno dei principali elementi distintivi di HyperSOC è la capacità di fondere in un unico framework operativo il monitoraggio degli ambienti IT e OT. In un'epoca in cui la digitalizzazione industriale annulla i confini tra officina e data center, le aziende devono avvalersi di un partner che garantisca una visibilità trasversale. HyperSOC risponde a questa esigenza con integrazioni indipendenti dal produttore, regole di rilevamento personalizzabili e un potente motore di threat intelligence costruito su rischi specifici di settore.

Il risultato è una visione unificata che accelera il rilevamento e la risposta alle minacce, elimina i punti ciechi, semplifica la compliance e rafforza la postura complessiva di sicurezza dell'organizzazione.

Efficienza attraverso l'iperautomazione

Alla base di HyperSOC troviamo un concetto cardine: l'iperautomazione. L'intelligenza artificiale, il machine learning e i workflow automatizzati vengono uniti per eliminare il rumore di fondo, alleggerire il lavoro degli analisti e accelerare drasticamente i tempi di risposta. Grazie alla piattaforma Pulse, i clienti HWG Sababa potranno sfruttare una correlazione intelligente degli avvisi, l'arricchimento contestuale e la prioritizzazione automatizzata, offrendo un triage snello e decisioni più precise fin dal primo segnale.

Ciò si traduce in una riduzione concreta dei due indicatori che contano di più per ogni CISO: il Mean Time to Detect (tempo medio per il rilevamento, MTTD) e il Mean Time to Respond (tempo medio per la risposta, MTTR). In questo modo, i team di sicurezza potranno agire più rapidamente e con maggiore efficacia. Le capacità avanzate di arricchimento rendono gli avvisi precisi e realmente utilizzabili, riducendo i falsi positivi e portando all'attenzione le minacce che richiedono un intervento immediato.

L'automazione è un alleato strategico che aumenta la precisione, riduce il carico operativo e libera i team interni, consentendo al personale di concentrarsi sulle decisioni sui rischi ad alto valore e non sulle attività manuali e ripetitive.

Portata globale, rilevanza locale

Il modello di HWG Sababa è particolarmente adatto per le organizzazioni delle regioni EMEA e Asia Centrale in cerca di un'alternativa ai tradizionali MSSP globali. La presenza locale e l'approccio consulenziale favoriscono la creazione della fiducia, offrendo soluzioni flessibili e su misura per realtà con esigenze complesse in termini di approvvigionamento, normative o integrazione tecnologica.

Ciò che distingue HWG Sababa è la collaborazione sinergica tra le sue unità principali, Consulting, Engineering, Threat Intelligence e Managed Services, che offre un approccio unificato alle sfide del cliente. Questo allineamento garantisce percorsi di escalation fluidi, risoluzione efficace degli incidenti e una guida strategica costante lungo l'intero percorso del cliente.

Grazie a diversi hub operativi, analisti certificati e una profonda competenza verticale, HWG Sababa non offre solo un servizio, ma una vera e propria partnership strategica nell'ambito della sicurezza informatica, fondata sulla prossimità locale e guidata da una visione globale.

Dai segnali alle informazioni: trasformare i dati in azioni

HyperSOC offre una reale difesa end-to-end lungo tutto il ciclo di vita, dal rilevamento e contenimento fino all'indagine, al reporting e all'analisi post-incidente. Ciò consente alle organizzazioni di rispondere più rapidamente per poi apprendere e adattarsi rafforzando in modo continuo la propria postura di sicurezza.

Alla base dell'efficacia di HyperSOC troviamo l'integrazione nativa della Cyber Threat Intelligence (CTI) nell'architettura. Grazie ad un mix sinergico di ricerca proprietaria, feed sulle minacce in tempo reale e partnership strategiche a livello internazionale, HWG Sababa rende le attività di rilevamento e risposta sempre contestualizzate, tempestive e pertinenti rispetto alle minacce più rilevanti per ciascun settore. Questo approccio basato sui dati offre una prioritizzazione più accurata, un contenimento più rapido e una comprensione più profonda del comportamento dei criminali.

Guardando al futuro, la roadmap di HWG Sababa prevede una convergenza sempre più stretta con le aree di governance, rischio e compliance (GRC), consentendo ai clienti di unificare sicurezza informatica e gestione del rischio in un unico framework intelligente.

Una capacità strategica per un futuro resiliente

HyperSOC di HWG Sababa non rappresenta solo un'evoluzione del SOC, ma una trasformazione strategica del modo in cui le operazioni di sicurezza vengono erogate, gestite e scalate. Basato su una logica indipendente dal produttore, alimentato da informazioni in tempo reale e in grado di offrire visibilità interdominio, HyperSOC trasforma la sicurezza da una funzione reattiva a un elemento abilitante e proattivo della continuità operativa e resilienza del business.

Più che fornire semplici avvisi o risposte di base agli incidenti, HyperSOC consente alle organizzazioni di assumere il pieno controllo della propria postura di rischio informatico, ridurre la complessità e integrare la sicurezza nei processi centrali dell'azienda. Essa supporta un rilevamento e una risposta più rapidi e la crescita continua della maturità difensiva nel tempo.

Per le organizzazioni che intendono guardare al futuro, allineare la sicurezza agli obiettivi strategici e restare un passo avanti rispetto alle minacce emergenti, HyperSOC rappresenta molto più di un servizio, trattandosi di una capacità strategica essenziale.

Sfide

L'offerta HyperSOC di HWG Sababa è interessante, in quanto propone un servizio di sicurezza gestita più olistico rispetto a quanto sia disponibile nel mercato EMEA. Tuttavia, il mercato MDR sta iniziando a colmare il divario, con un numero crescente di provider che stanno ampliando la propria offerta con servizi di risposta agli incidenti orientati ai risultati e con supporto multilingue. In questo contesto, HWG Sababa dovrà misurarsi con una concorrenza crescente, mentre l'aumento delle capacità dei concorrenti potrebbe esercitare pressione sui margini di un mercato in forte accelerazione.

VI. Conclusioni

Gli economisti concordano sul fatto che un'auto nuova perda dal 10% al 20% del proprio valore una volta uscita dal concessionario. Allo stesso modo, molti acquirenti delle soluzioni di sicurezza informatica percepiscono un rapido deprezzamento degli strumenti impiegati per proteggere le proprie infrastrutture IT e OT. Per questo motivo, sempre più CISO e CIO scelgono partner come HWG Sababa, capaci di proteggere l'infrastruttura esistente, continuando a investire, nelle aree trattate in questo documento per salvaguardare gli asset anche in futuro.

IDC prevede una crescita costante del mercato MDR e, più in generale, del SOC-as-a-Service, grazie a provider come HWG Sababa. Questo documento ne evidenzia i fattori chiave del successo: investire con continuità nei cinque elementi rappresenta la strada più efficace per ottenere risultati duraturi.

I CISO della regione EMEA devono scegliere un MSSP in grado di offrire tutti i componenti necessari per proteggere le esigenze di oggi e quelle di domani.

Profilo dell'analista

Craig Robinson, Research VP

Craig Robinson dirige il reparto di ricerca di IDC dedicato ai servizi di sicurezza. Si occupa in particolare di *Managed Detection and Response* (risposta e rilevamento gestiti, MDR), servizi di preparazione e risposta agli incidenti, resilienza informatica e del rapporto tra C-suite, consigli d'amministrazione e sicurezza informatica.

MESSAGGIO DALLO SPONSOR

Potenziare le operazioni di sicurezza con HyperSOC

Con l'aumento dei rischi informatici e della pressione normativa, i SOC tradizionali non sono più sufficienti. L'HyperSOC di HWG Sababa nasce per rispondere a questa sfida, offrendo operazioni scalabili e basate sull'intelligence ideate per le esigenze di settori complessi e regolamentati.

HyperSOC integra il monitoraggio di IT, OT e IoT in un'unica piattaforma, sfruttando iperautomazione, threat intelligence avanzata e modelli di servizio flessibili. Il motore proprietario Pulse gestisce in maniera intelligente rilevamento, triage e risposta, aumentando visibilità, precisione ed efficienza.

HyperSOC va oltre la semplice generazione degli avvisi e offre risultati concreti come ad esempio la riduzione di MTTD e MTTR, rafforzamento della postura di rischio e percorso di crescita continua della maturità informatica.

Scopri di più su HyperSOC: https://www.hwgsababa.com/en/defense-center-soc/

IDC Custom Solutions

Il contenuto di questo documento è stato adattato da ricerche IDC già pubblicate su www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com