HWG Sababa

Security Operations Center: in-house o in outsourcing?



Di fronte alla rapida evoluzione del panorama delle minacce, molte organizzazioni si trovano davanti ad un bivio nel decidere il destino del proprio Security Operations Center (SOC). La scelta strategica tra mantenere le funzioni del SOC all'interno dell'azienda o esternalizzarle richiede un'attenta riflessione. Questo whitepaper si propone di fare luce sui fattori che influenzano questa decisione, fornendo una guida preziosa ai Chief Information Officer (CIO) e ai Chief Information Security Officer (CISO) per compiere scelte consapevoli e adatte alle loro specifiche esigenze.

Se tra il 2018 e il 2023 il numero degli attacchi a livello globale è cresciuto del 61%, l'Italia ha registrato una crescita pari al 300%[1]. Inoltre, anche il ritmo degli attacchi cyber più complessi è notevolmente aumentato: il "dwell time" tra la violazione e la fase attiva di un attacco si è drasticamente ridotto, passando da oltre 2 mesi a poco più di 3 giorni[2].

Ciò spinge le aziende a cercare soluzioni di sicurezza in grado di fornire un monitoraggio continuo delle infrastrutture interconnesse, l'analisi degli alert, l'identificazione dei modelli di attacco nelle loro fasi iniziali, nonché una risposta e remediation rapide e accurate.

Confronto crescita % Italia vs. Global 2018 - H1 2023

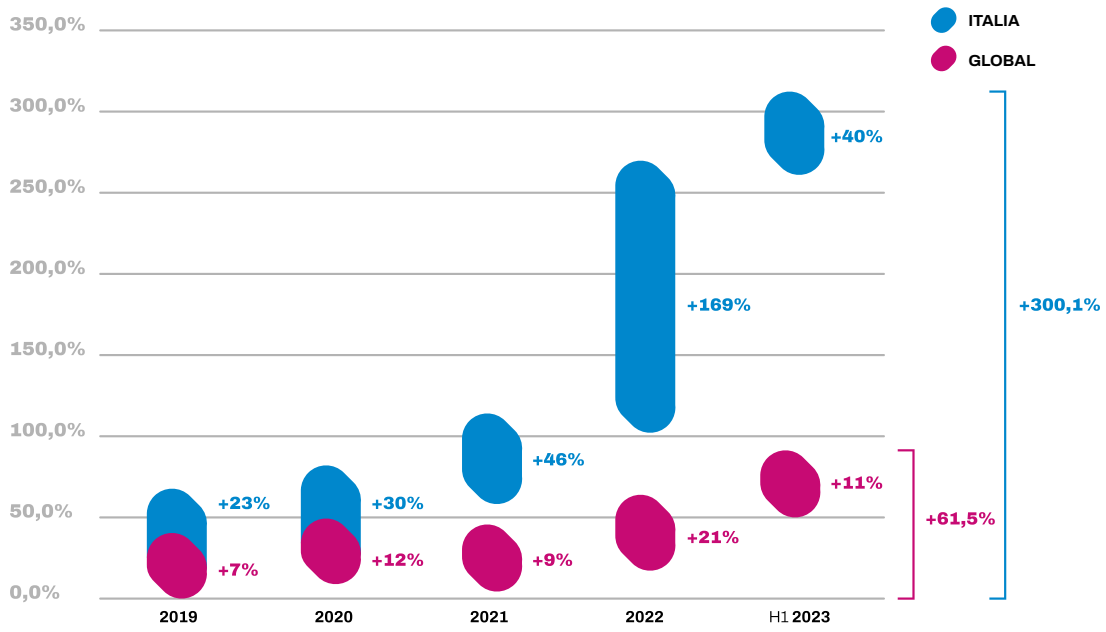


Immagine 1 *- Crescita dei cyberattacchi 2018-2023, Clusit*

[1]Rapporto Clusit 2023

[2]X-Force Threat Intelligence Index 2023, IBM

Anche il profilo dell'utente tipico di un SOC si sta modificando, variando a seconda dei verticali. Oltre al settore finanziario e alle infrastrutture critiche - che sono tra i primi fruitori del SOC - e ai settori governativo e manifatturiero - che sono stati maggiormente colpiti rispetto ad altre imprese italiane nel primo semestre del 2023[3]- anche le aziende che operano nell'utility, nei trasporti, nel retail, nella moda e nelle telecomunicazioni stanno considerando e adottando diverse strategie SOC per aumentare la resilienza delle proprie infrastrutture. Oltre alla sicurezza in ambito IT, i loro obiettivi includono la salvaguardia dei sistemi OT (Operational Technology), delle reti interconnesse, delle comunicazioni, dei dispositivi IoT e IIoT e delle infrastrutture smart, garantendo una protezione completa delle operazioni finanziarie e della supply chain, della proprietà intellettuale e dei dati dei clienti, attraverso il controllo costante e la combinazione di varie soluzioni di sicurezza.

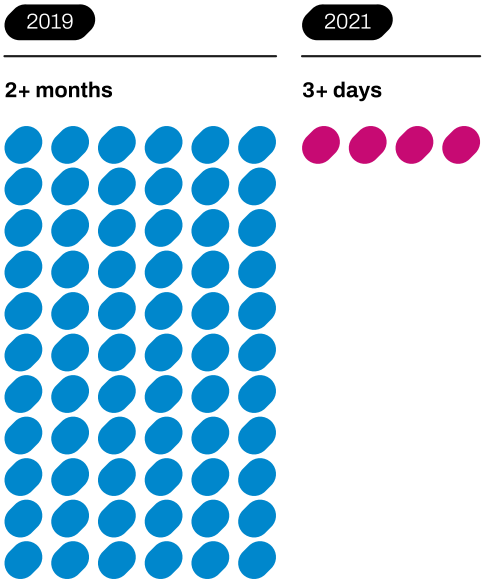
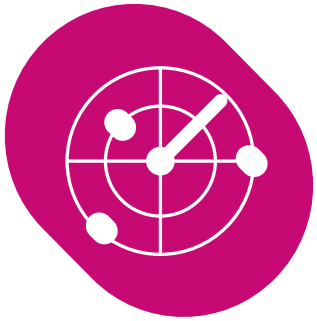


Immagine 2 - *Durata media degli attacchi ransomware, 2019-2021, IBM*

Questa varietà di verticali che scelgono il SOC come investimento strategico per il proprio piano di cybersecurity porta alla luce molteplici aspetti che influiscono sui requisiti richiesti ai provider di managed security. Le soluzioni di sicurezza devono infatti essere personalizzate in funzione delle normative di settore, dell'infrastruttura esistente, della maturità della sicurezza, degli obiettivi aziendali e delle risorse disponibili per la gestione delle stesse.

Quale tipo di SOC scegliere?



Non esiste un unico modello di Security Operations Center in grado di svolgere le funzioni di un SOC moderno. I SOC variano in base al loro scopo e ai loro obiettivi, che sono condizionati da fattori quali la propensione al rischio, il verticale in cui operano le aziende, il livello di maturità, le capacità e le competenze, i processi e le procedure, gli strumenti impiegati e il modo in cui vengono utilizzati i servizi di sicurezza.
A tal proposito, Gartner definisce 3 modelli principali di SOC: in-house, in outsourcing (a più livelli) e ibrido[4]. Finora il SOC in-house è stato largamente adottato da grandi imprese con cospicue disponibilità economiche ed asset critici da proteggere. Tuttavia, la situazione sta cambiando, poiché la complessità e le esigenze in materia di SOC stanno aumentando.

[3]Rapporto Clusit 2023

[4]Use the Gartner SOC HIT Model, 2021

Entro il 2025, il 33% delle organizzazioni che attualmente dispongono di funzioni di sicurezza interne tenterà di sviluppare un SOC in-house, ma senza risultati, a causa di risorse limitate in termini di budget, competenze e personale. Allo stesso tempo, entro il 2025, il 90% dei SOC del G2000 utilizzerà un modello ibrido, esternalizzando almeno il 50% del carico di lavoro[5].

L'adozione di modelli SOC completamente esternalizzati o ibridi, in cui professionisti esterni di cybersecurity diventano un'estensione dei team di sicurezza interni, ha molteplici motivazioni. Tra queste troviamo:

1. Capacità limitate dei team di sicurezza interni.

Mentre nel 2022 la carenza di esperti di cybersecurity era pari a 3,4 milioni a livello globale, nel 2023 questo divario ha raggiunto i 4 milioni[6]. Poche aziende dispongono di team di sicurezza estesi e i professionisti che ne fanno parte spesso soffrono di pressioni troppo elevate e di conseguente burnout[7]. L'efficacia in termini di costi - non dovendo assumere e mantenere esperti che lavorino 24x7 - e la più facile scalabilità nei casi in cui un'organizzazione cresca, si innovi, modifichi i propri obiettivi e debba essere conforme alle normative, spingono le aziende a scegliere questo modello di SOC.

2. Scarsa varietà di ruoli.

Non solo il numero di esperti di sicurezza, ma anche la loro diversificazione gioca un ruolo importante. Quando si cerca di capire quante funzioni di sicurezza vengono effettivamente svolte internamente, molte aziende si rendono conto che le loro competenze interne sono limitate. Per affrontare al meglio ogni singolo aspetto dell'intero ciclo di vita della sicurezza, le organizzazioni hanno bisogno di *diverse funzioni* e ruoli all'interno dei loro team che, lavorando a stretto contatto, possano garantire un'elevata resilienza informatica.

3. Cybersecurity oltre l'IT.

Con il processo di digitalizzazione in atto in tutti i settori, il raggio d'azione della sicurezza si estende oltre l'IT. Entro il 2027, si prevede che il 75% dei team di security avrà adottato almeno cinque strumenti per gestire la sicurezza dei sistemi cyber-fisici (CPS) in ambienti operativi, di produzione o mission-critical, il che rappresenta un notevole aumento rispetto a uno o due strumenti utilizzati oggi[8]. Questo fa sì che le aziende preferiscano fornitori di SOC che abbiano esperienza e competenze in ambito OT e IoT/IIoT per poter rispondere ad esigenze specifiche e garantire la conformità agli standard di sicurezza del settore.

4. Efficienza.

I SOC in outsourcing gestiscono ingenti volumi di dati ed eventi di sicurezza, spesso dell'ordine di milioni di eventi al secondo (EPS). Essi implementano ampie serie di regole e playbook, superando di gran lunga le offerte out-of-the-box dei provider di sicurezza e i risultati derivanti da attività interne. Questo livello elevato di automazione ed efficienza garantisce che l'organizzazione sia meglio equipaggiata per rilevare e rispondere tempestivamente alle minacce.

[5]SOC Model Guide, Gartner, 2021

[6]ISC2 Cybersecurity Workforce Study: Looking Deeper into the Workforce Gap, 2023

[7]We Need To Talk More About Burnout In Cybersecurity, Forrester, 2023

[8]Market Guide for Operational Technology Security, Gartner, 2023

5. Distribuzione della forza lavoro.

Con una forza lavoro distribuita in tutto il mondo, i SOC in outsourcing dispongono di un numero sufficiente di persone per lavorare su turni e operare 24 ore su 24. Mentre i dipendenti interni reperibili durante la notte dormono, i professionisti del SOC in outsourcing rimangono vigili, proteggendo la vostra organizzazione e i suoi asset dalle minacce informatiche, indipendentemente dalla loro origine. Questa copertura su scala globale è fondamentale per le aziende che hanno clienti e partner in tutto il mondo.

6. Sicurezza e sostenibilità dei dati.

Uno degli argomenti più convincenti per l'esternalizzazione del SOC è la sicurezza dei dati. Un fornitore di SOC affidabile infatti, essendo strutturato in diversi livelli, aderisce a rigidi protocolli di sicurezza. Essi sono ben attrezzati per salvaguardare i vostri dati sensibili, spesso in modo più efficace di un team interno, che potrebbe essere più suscettibile a minacce provenienti dall'interno o a data breach accidentali.

7. Accesso alle più recenti tecnologie di sicurezza.

Infine, il livello di protezione fornito da un SOC in outsourcing può essere un deterrente significativo contro le Advanced Persistent Threat (APT) o gli attacchi ransomware accidentali. La mancanza di un contesto relativo a ciò che viene individuato, l'automazione del rilevamento e della risposta e l'orchestrazione della sicurezza sono le maggiori sfide per il pieno utilizzo delle funzionalità di un SOC in-house[9]. I fornitori di SOC esterni sono dotati delle tecnologie più recenti, di strumenti di Threat Intelligence e di strategie di Incident Response che vanno al di là di quanto possa offrire un fornitore indipendente, riducendo le probabilità di successo degli attacchi cyber.

Quali sono gli altri fattori da tenere d'occhio quando si sceglie un fornitore di SOC?

Qualunque sia il modello di SOC più adatto alla tua organizzazione, ci sono altri fattori e tendenze che potrebbero influenzare la tua decisione nel 2024:

Consolidamento dei fornitori di sicurezza.

Dovendo garantire la protezione in tutti i settori IT, OT e IoT, le aziende si trovano a lavorare con più fornitori di sicurezza. Con l'obiettivo di trovare il giusto equilibrio nel numero di partner con cui collaborare, nel 2023 il 75% delle aziende ha consolidato il numero dei propri fornitori, rispetto al 29% del 2020[10], preferendo provider con un'offerta più ampia.

[9] SANS SOC Survey 2023

[10] Integrating SASE, XDR and Other Security Vendor Consolidation Trends in Security Strategy, Gartner 2022

Le attuali sfide della supply chain.

I cyberattacchi, compresi quelli di matrice statale, aggiungono pressione alle supply chain, accanto all'aumento dei costi, alla mancanza di manodopera e ad alcuni ritardi e carenze di prodotti[11]. Le supply chain più ridotte sono più facili da proteggere end-to-end, mentre la predilezione verso i fornitori locali, compresi quelli di sicurezza, garantisce una più facile conformità agli standard.

Generative AI.

L'intelligenza artificiale si sta rivelando uno strumento formidabile per identificare e prevenire gli attacchi informatici. Le organizzazioni integrano l'IA per ottenere SOC più efficienti e scalabili, con algoritmi generativi destinati a trasformare i processi decisionali, la comunicazione aziendale e la gestione delle minacce. Questa evoluzione promette di snellire i processi esistenti, migliorare le capacità di rilevamento e automatizzare le attività di Threat Hunting. Nel medio termine, si prevede che l'integrazione dell'IA sostituirà gradualmente gli analisti di livello inferiore, consentendo loro di reindirizzare la propria attenzione verso attività a più alto valore aggiunto. La scelta del cliente ricadrà quindi sui fornitori di SOC con anni di esperienza e molteplici certificazioni.



Valutare, pianificare, agire

La scelta del giusto SOC per la tua organizzazione richiede un approccio strategico e personalizzato. Tenendo a mente la continua evoluzione del panorama delle minacce, la diversità dei modelli di SOC e alcune considerazioni chiave che influenzano il processo decisionale, è possibile migliorare la postura di sicurezza della propria organizzazione.

Considera il seguente piano d'azione per un'autovalutazione completa:

1. **Valutare lo stato attuale della sicurezza.**
Valuta l'efficacia delle misure, dei processi e delle procedure di sicurezza esistenti. Identifica eventuali gap o vulnerabilità che potrebbero esporre la vostra organizzazione a potenziali minacce informatiche. Sii pronto ad accettare che la maturità dei processi IT e la consapevolezza delle più comuni minacce di sicurezza informatica possono essere superiori a quelle dei domini OT o IoT.

2. **Definire i requisiti ideali del SOC.**
Stabilisci requisiti specifici per il SOC, tenendo conto degli aspetti unici della tua organizzazione. Definisci obiettivi e aspettative chiare per i potenziali fornitori di SOC, tenendo conto anche della collaborazione con i team interni.

[11] European supply chain update – refocusing on reliability - August 2023

3. **Stabilire i requisiti per i fornitori di SOC.**
Definisci fattori critici come il monitoraggio 24x7, la portata delle mansioni di sicurezza svolte internamente (IT/OT/IoT) e il volume previsto di eventi di sicurezza. Considera l'integrazione di playbook e il grado di automazione necessario alle tue operazioni di sicurezza.

4. **Valutare le capacità interne.**
Poniti questa domanda: "Quante funzioni di sicurezza siamo davvero in grado di svolgere e gestire internamente in modo efficace?".
Sii onesto sui limiti e sui punti di forza del tuo team di sicurezza.

5. **Allineamento con gli obiettivi aziendali.**
Assicurati che il modello di SOC scelto si allinei perfettamente con i tuoi obiettivi aziendali. Considerane la scalabilità, l'economicità e la capacità di adattarsi ai futuri cambiamenti del panorama aziendale.

Tieni presente che la soluzione SOC ideale non è uguale per tutti, ma sarà personalizzata in base alle sfide, agli obiettivi e alle complessità operative uniche della tua organizzazione.

Il SOC di HWG Sababa

HWG Sababa è un'azienda italiana che offre una suite completa di soluzioni strategiche, servizi gestiti e consulenza in materia di cybersecurity. I suoi SOC di Verona e Vilnius garantiscono un monitoraggio proattivo delle infrastrutture digitali in ambienti IT, OT e IoT per prevenire, rilevare, analizzare e rispondere alle minacce informatiche. Il SOC di HWG Sababa si rivolge a imprese di diversi settori, tra cui banche centrali, impianti di produzione di energia, telco, sanità e altre infrastrutture critiche in tutto il mondo.

Sebbene non sia possibile trovare due progetti SOC identici, in quanto ciascuno di essi viene personalizzato per ogni cliente, le aree funzionali chiave del SOC sono pressoché uguali:

- **Rilevamento e risposta**
  Un team di esperti di cybersecurity monitora l'infrastruttura 24 ore su 24, 7 giorni su 7, identificando anche gli attacchi più complessi in ambienti IT, OT e IoT già nelle loro fasi iniziali e implementando immediatamente le azioni di risposta per garantire una protezione completa.

Intelligence & Threat Hunting

Fornisce preziose informazioni sulle minacce informatiche e sui loro attori.
In particolare, queste attività ci permettono di rintracciare l'origine degli attacchi e di raccogliere prove sostanziali per indagini approfondite sugli incidenti in ambito open source, deep web e darknet.

Exposure Management

Potenziali rischi e vulnerabilità che possono essere sfruttate dagli attaccanti vengono analizzati attentamente e mitigati per prevenire il verificarsi di attacchi reali, grazie a una combinazione di tecniche di threat modelling, vulnerability scanning e risk analysis.

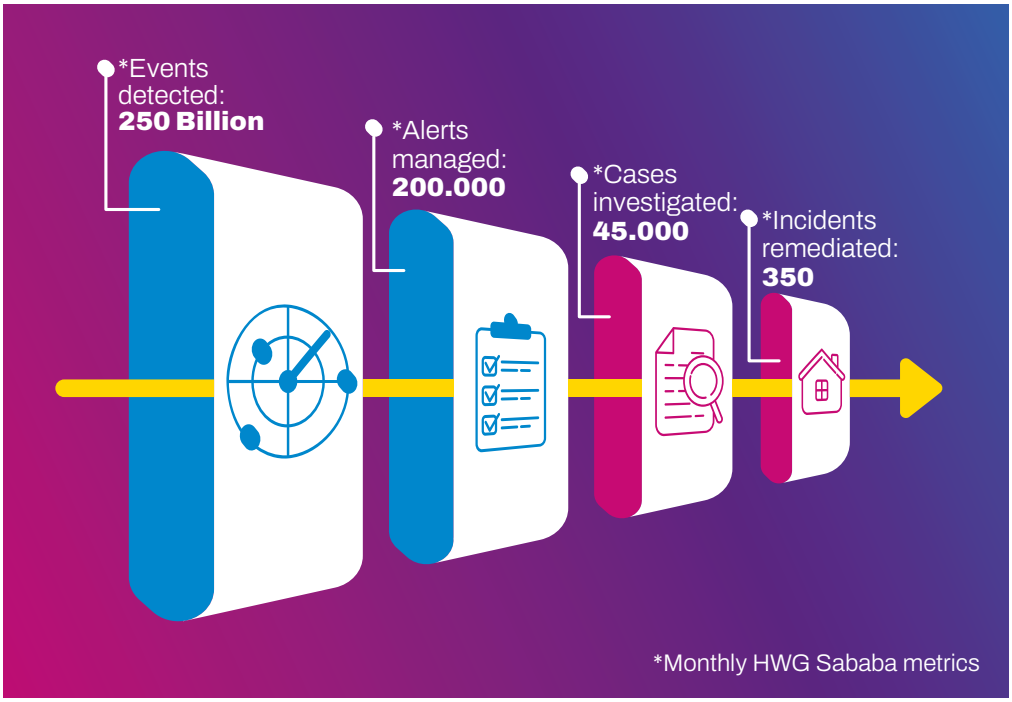
Security automation

Quando i tentativi di cyberattacco si ripetono, c'è la possibilità di mitigarli automatizzando le operazioni. Accelera il rilevamento e riduci i tempi di risposta grazie a un'orchestrazione automatizzata delle operazioni di sicurezza, lasciando che gli esperti di security si concentrino su aree più prioritarie per l'azienda.

Observability

Integra le metriche di security con KPI non legati alla sicurezza attraverso l'analisi comportamentale delle risorse nell'intera infrastruttura aziendale. Ciò consente di rilevare le anomalie e gli attacchi cyber nelle loro fasi iniziali.

Elaborando milioni e milioni di eventi di sicurezza ogni mese, il SOC di HWG Sababa li trasforma in 45.000 casi investigati e 350 casi risolti per i propri clienti.

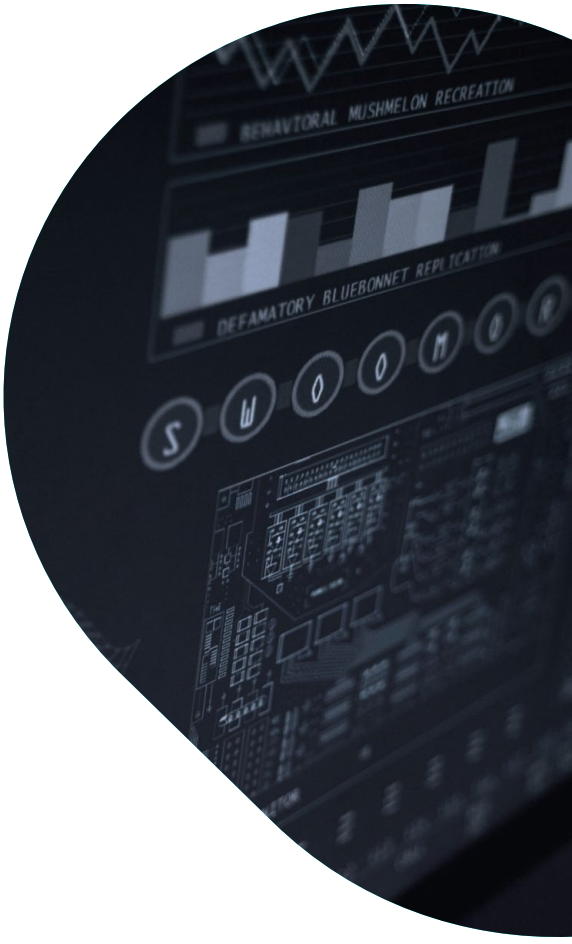


- Operativo dal 2008
- Clienti 125+/verticali
- IBM EPS gestito 100.000/mese
- Playbook personalizzati 200+
- 98% sotto SLA
- 70 esperti, raggruppati in 3 livelli
- 2 sedi
- 24x7x365
- Oltre 300 certificazioni, tra cui GPEN, GWAPT, CISSP, CCIE, PMP e altre ancora.

Scopri alcune storie di successo reali e cross-verticali in ambito SOC:

- Ansaldo Energia (Energia)
- Selda Informatica (Pubblica Amministrazione / Sanità)
- Unit Plus (Trasporto)

Contattaci per approfondire il nostro SOC o per chiedere una consulenza.



HWG Sababa

Follow us on:

www.hwgsababa.com