WHITE PAPER

Orientarsi nella cybersecurity con un Security Operations Center efficace

Scopri il modello SOC ideale
per la tua organizzazione.

SOPHOS

Riepilogo

L'evoluzione del panorama della cybersecurity è inarrestabile, con minacce che diventano sempre più sofisticate e dilaganti. In un ambiente simile, i Security Operations Center (SOC) sono essenziali per aiutare le organizzazioni a rilevare, analizzare e rispondere rapidamente agli incidenti informatici. Le aziende devono scegliere quale modello SOC sia maggiormente in grado di soddisfare le loro esigenze: interno, ibrido o esterno (in outsourcing). Inoltre, devono assicurarsi di misurarne la performance con le giuste metriche, per garantire una sicurezza continua e perfettamente allineata con i loro obiettivi aziendali.

Il 63% delle aziende

Viene colpito dal ransomware per via della mancanza di personale o delle competenze necessarie[1].

Il ruolo di un SOC nell'attuale panorama della cybersecurity

L'era digitale ha portato con sé un aumento delle minacce informatiche, con cybercriminali e autori degli attacchi sponsorizzati da governi che sfruttano tecniche sempre più sofisticate. Le tendenze attuali indicano un preoccupante calo del tempo che intercorre tra la violazione iniziale dei sistemi e distribuzione del ransomware, che ora è in media pari a 2 giorni[2]. Come se non bastasse, il settore della cybersecurity continua ad affrontare il problema della mancanza significativa di talenti, il che rende ancora più difficile formare e mantenere un SOC interno.

Carenza di talenti

Il settore della cybersecurity continua ad affrontare una carenza significativa di personale specializzato.

Un SOC è un'unità organizzativa dedicata alla gestione dei processi di identificazione, indagine e correzione degli incidenti di sicurezza. Le responsabilità specifiche che può assumere includono la gestione delle risorse, dei cambiamenti, delle vulnerabilità, degli eventi di sicurezza e degli incidenti, nonché l'integrazione di dati di intelligence sulle minacce e varie attività di DevOps quali l'automazione e il controllo qualità. Anche se i SOC non controllano tutti gli aspetti della protezione di un'azienda, svolgono un ruolo cruciale nel coordinamento della risposta ai problemi di sicurezza. La mission e gli obiettivi specifici di un SOC possono essere molto diversi, poiché dipendono da fattori quali la tolleranza al rischio dell'organizzazione, il settore in cui opera, il livello di maturità informatica e gli strumenti e i processi utilizzati.

Tipi di modelli SOC

Esistono vari modelli SOC, ognuno dei quali presenta un set distintivo di caratteristiche e vantaggi:

I SOC interni sono tipici delle aziende con ampie risorse finanziarie, che possono permettersi di mantenere un'operatività continua con un team dedicato. Questi SOC potrebbero affidare a team esterni alcune funzioni specialistiche come i penetration test, il threat hunting a cura di esperti o l'intelligence sulle minacce. Le imprese di grandi dimensioni o con sedi in vari paesi possono utilizzare un modello a più livelli, con SOC diversi che operano nell'ambito di un'unica struttura di comando.

I SOC ibridi stanno diventando sempre più diffusi: si basano sulla combinazione di risorse interne e servizi esterni per creare una funzione di sicurezza personalizzata, con un modello basato sulla partnership. Normalmente, il provider di questi servizi di sicurezza è operativo 24/7 e si occupa del monitoraggio e della valutazione degli avvisi, indaga sugli incidenti, svolge attività di threat hunting e offre supporto a cura di esperti. Questo permette al team interno di ottimizzare le proprie risorse attraverso l'architettura e la progettazione della sicurezza, la gestione delle policy e della conformità, la mitigazione del rischio, nonché corsi di formazione e sensibilizzazione sulla sicurezza e azioni di risposta dirette, se l'azienda preferisce gestire la correzione internamente. Due aspetti particolarmente vantaggiosi di questo scenario sono la flessibilità che offre, e la possibilità di risolvere i problemi legati alle limitazioni del budget e alla mancanza di personale dotato di competenze elevate.

Un SOC gestito da un provider esterno è un servizio di terze parti che offre capacità complete di monitoraggio della cybersecurity e risposta alle minacce. Possono optare per questo modello le organizzazioni che hanno bisogno di creare rapidamente un SOC di base, ma che non hanno personale interno dotato di competenze adeguate. In questo scenario, l'azienda si affida completamente a un provider di servizi di Managed Detection and Response (MDR) già consolidato. L'azienda può poi attivare l'integrazione delle soluzioni del vendor esterno con le proprie tecnologie informatiche e di sicurezza attuali, per garantire massima visibilità sull'intero ambiente e per coordinare le attività di incident response.

Sapevi che...

L'88% degli attacchi ransomware ha inizio al di fuori del normale orario lavorativo[2].

Qual è il modello giusto per te?

Stabilire qual è il giusto modello per la tua organizzazione dipende da vari fattori, tra i quali il profilo di rischio complessivo. Devi ponderare qual è il livello di rischio considerato accettabile per la tua organizzazione, tenendo in considerazione il budget di cybersecurity disponibile. Ci sono diverse questioni importanti da considerare, tra cui:

1. Le limitazioni in termini di risorse interne (la disponibilità di competenze o di personale/capacità)
2. L'equilibrio tra gli ambiti che devono essere gestiti internamente e quelli da affidare in outsourcing
3. La maturità attuale delle tue Security Operations
4. La difficoltà del dover assumere, formare e fidelizzare talenti fondamentali, con competenze specialistiche
5. L'esigenza di stare al passo con le tecnologie emergenti, con un panorama delle minacce in continua evoluzione e con la crescente complessità delle tecniche utilizzate dagli active adversary
6. Le interdipendenze dei vari dipartimenti per le funzioni di natura informatica, legale o relative al rischio e alla conformità, nonché quelle che riguardano altri reparti aziendali

Qualsiasi sia il modello che scegli di implementare, è importante sviluppare un business case in grado giustificarne la necessità e specificare le risorse necessarie per renderlo sostenibile a lungo termine. Anche valutare regolarmente le capacità del tuo SOC è un aspetto fondamentale per assicurarti che sia in linea con la struttura e gli obiettivi operativi previsti.

La maggior parte delle aziende si trova attualmente ad affrontare una carenza di talenti di cybersecurity, e molti budget di sicurezza sono talmente limitati da precludere la possibilità di formare e mantenere un SOC interno dotato del giusto numero di membri del team per renderlo operativo 24/7. I CISO più esperti comprendono anche l'importanza del conservare il controllo strategico sulle proprie Cybersecurity Operations, e per estensione sulla sostenibilità a lungo termine della loro organizzazione, attraverso supervisione e governance.

I vantaggi di un modello SOC ibrido

Il modello SOC ibrido offre una combinazione estremamente favorevole di tutti i vantaggi dell'approccio interno e di quello esterno. Permette alle organizzazioni di sfruttare il pieno potenziale delle competenze e dell'efficienza di un provider esterno, pur mantenendo un certo grado di personalizzazione e controllo sulle proprie Security Operations.

Uno dei vantaggi principali di un SOC ibrido è l'accesso e la scalabilità che offre a tecnici di sicurezza esperti e a dati di intelligence sulle minacce dall'efficacia comprovata. Questi professionisti fanno parte di un team più ampio di talenti che affrontano continuamente un'ampia selezione di minacce. Gli incarichi in cui sono regolarmente coinvolti permettono a questi esperti di tenersi aggiornati sugli ultimi sviluppi nell'ambito della cybersecurity. Data la rapida evoluzione del panorama delle minacce, nessun team interno indipendente riuscirebbe mai a ottenere questo livello di esposizione ed esperienza.

Inoltre, collaborare con un vendor esterno garantisce protezione e monitoraggio ininterrotti (24/7, 365 giorni all'anno), anche di notte, nel fine settimana e durante i giorni festivi, quando i tuoi team interni potrebbero essere off-line.

Un SOC ibrido può ridurre significativamente lo stress dovuto all'eccessiva quantità di avvisi, in quanto aiuta le organizzazioni a ottimizzare i propri sistemi di rilevamento e di conseguenza ad accorciare il tempo medio di risposta agli incidenti. Oltre a questo, permette alle aziende di evitare gli elevati costi normalmente associati al dover mantenere un team completamente dedicato alla ricerca sulle minacce, visto che il partner esterno svolgerà queste attività per conto loro, aggiungendo continuamente nuove capacità di rilevamento man mano che vengono sviluppate e rilasciate.

Un ulteriore vantaggio è la possibilità di poter assegnare le risorse interne alla gestione delle principali strutture IT, delle tecnologie più critiche e dei problemi di conformità, mentre il partner SOC si concentra sugli incidenti di sicurezza. Questa ripartizione del lavoro permette di assegnare risorse e personale esperto in maniera più efficiente. Può anche permettere agli altri reparti di dedicare più tempo alle loro altre responsabilità di sicurezza.

In un modello ibrido, i corsi di formazione, che possono essere un investimento ingente di tempo e denaro, sono più semplici e brevi. Il provider di servizi esterno si assicura che il suo intero team sia al passo con le novità di tutti gli aspetti della cybersecurity, dalle analisi forensi, all'incident response e alla sicurezza del cloud. Questo solleva il team interno dell'organizzazione dal peso di dover mantenere competenze aggiornate in ogni ambito della cybersecurity, permettendogli di concentrarsi sulle questioni aziendali di maggiore pertinenza.

Il modello SOC ibrido offre anche la flessibilità di organizzare le attività operative per livelli, in base alla tolleranza al rischio dell'azienda, e di ottimizzare le metodologie di risposta a seconda del caso. Il risultato sono misure di sicurezza più efficaci e mirate. Oltretutto, i risparmi associati all'impiego di un SOC ibrido lo rendono un'opzione estremamente convincente non solo per le piccole e medie imprese, ma anche per le aziende più grandi che desiderano affidare certe funzioni di sicurezza a un provider esterno.

Come misurare l'efficacia di un SOC

Qualsiasi sia il modello che più si addice alle tue esigenze, per misurare l'efficacia di un SOC occorre impiegare un set di metriche in grado di riflettere sia il panorama di sicurezza, che l'efficacia delle risorse del SOC. Le metriche suggerite di seguito, insieme ad altre, possono essere riassunte e presentate in una dashboard che indichi il conteggio in tempo reale, più statistiche settimanali, mensili e trimestrali per monitorare le tendenze nel tempo, concentrandosi sulla velocità di risposta e sulla qualità delle indagini.

Per quanto riguarda il panorama di sicurezza, le metriche devono fornire approfondimenti sulla portata e sul volume delle potenziali minacce; inoltre devono indicare i punti vulnerabili dell'organizzazione e il livello totale di esposizione ai rischi. Alcuni esempi possono essere la quantità di e-mail sospette o dannose ricevute, il numero di scansioni e tentativi di exploit di sistemi esterni, e il volume di incidenti di sicurezza in base all'origine.

Quando si valuta l'efficacia di un SOC, le metriche devono monitorarne la performance rispetto a policy e obiettivi di sicurezza predefiniti, legati ai risultati aziendali desiderati, ad esempio la riduzione del rischio e la conformità normativa. Le statistiche includono anche la velocità di risposta e la qualità delle indagini, nonché la ripartizione del tempo che il personale di sicurezza trascorre svolgendo le varie attività, il numero di incidenti in base alla categoria di conformità, e le ore impiegate dal team di engineering per limitare la superficie di attacco. Tra le metriche più importanti ci sono inoltre il tempo richiesto per la valutazione delle indagini, la quantità di indagini nelle quali sono state intraprese azioni correttive, il numero di azioni correttive applicate in base ai risultati del threat hunting proattivo, e il volume di vulnerabilità a cui sono state applicate patch, in ordine di gravità.

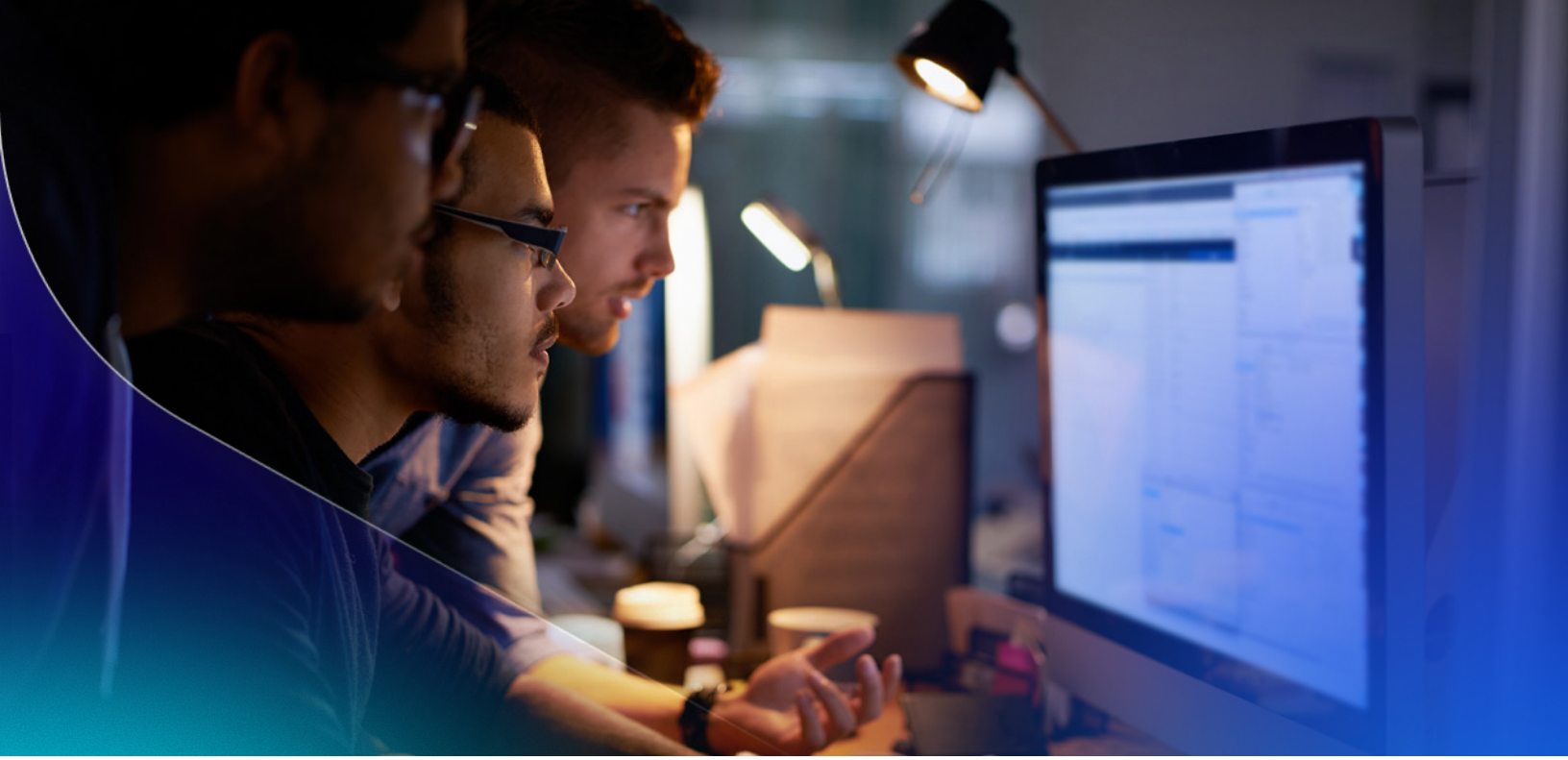
Monitorando regolarmente queste metriche, le organizzazioni possono non solo assicurarsi che il loro SOC stia funzionando in modo efficiente, ma anche contribuire a migliorare il profilo di sicurezza complessivo e raggiungere i propri obiettivi aziendali.

Le metriche devono:

- Fornire approfondimenti sulla portata e sul volume delle potenziali minacce
- Individuare i punti vulnerabili di un'organizzazione
- Indicare il livello totale di esposizione al rischio
- Monitorare la performance rispetto a policy e obiettivi di sicurezza predefiniti

Metriche principali:

- Tempo di valutazione delle indagini
- La quantità di indagini nelle quali sono state intraprese azioni correttive
- Il numero di azioni correttive applicate in base ai risultati del threat hunting proattivo
- Il volume di vulnerabilità a cui sono state applicate patch



Trova una soluzione SOC avanzata

Ogni azienda è diversa dalle altre, e tutte hanno livelli variabili di maturità di sicurezza. Con un panorama delle minacce in continua evoluzione, poter contare su un SOC di qualità è fondamentale per qualsiasi organizzazione disposta a prendere sul serio la propria cybersecurity. Sia che un'azienda scelga di formare una struttura interna, collaborare con un provider esterno o adottare un approccio ibrido, la giusta partnership può fornire sia un sistema di difesa efficace, che l'allineamento con gli obiettivi commerciali.

Molte imprese stanno optando per modelli SOC ibridi o completamente gestiti per risolvere i problemi legati alla mancanza di personale specializzato, alle limitazioni del budget e a minacce informatiche sempre più complesse. Questi modelli offrono flessibilità, analisi a cura di esperti e copertura 24/7. I team interni avranno così la possibilità di concentrarsi sulle iniziative più strategiche, mentre la gestione scalabile delle Security Operations viene affidata al proprio partner di fiducia.

Sophos MDR è l'esempio perfetto di questo approccio. Sophos offre varie opzioni con livelli diversi di servizio, progettate per venire incontro alle esigenze delle organizzazioni, qualsiasi sia la fase del percorso di cybersecurity in cui si trovano. Queste aziende potranno così contare su capacità avanzate di rilevamento, indagine e risposta, personalizzate in base ai propri requisiti specifici. Sia che si tratti di offrire supporto a un team SOC interno, o di svolgerne tutte le mansioni in outsourcing come partner esterno, Sophos MDR ottimizza la visibilità sulle minacce e le azioni di risposta, aiutando le organizzazioni a potenziare le proprie difese e a proteggere le risorse più importanti.

[1] Sophos, Report La vera storia del ransomware 2025
[2] Sophos, Active Adversary Report 2025

SOPHOS

Scopri di più sui nostri servizi di Managed Detection and Response, visitando la pagina sophos.it/mdr.

Vendite per Italia
(+39) 02 94 75 98 00
E-mail: sales@sophos.it