

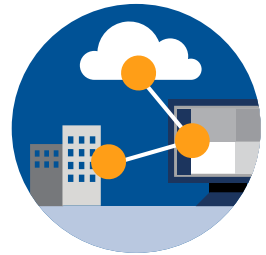
Come configurare il tuo SOC per il successo

Stai valutando di configurare o riconfigurare il tuo centro operativo di sicurezza (SOC) per raggiungere l'efficienza ottimale?

Un SOC ben progettato è cruciale per salvaguardare l'organizzazione da minacce in evoluzione, sia fisiche che informatiche. Qui analizziamo gli aspetti principali suddividendoli in sette categorie fondamentali: configurazione, collaborazione, contesto, chiarezza, coordinamento, conformità e cybersecurity.

✓ Configurazione: ampliare la portata e la flessibilità

- **Pianifica la disposizione dell'hub:** disponi il SOC, per facilitare il lavoro di squadra e rendere i monitor facilmente visibili a tutti gli operatori.
- **Prediligi ambienti senza finestre:** la sala non dovrebbe avere finestre e dovrebbe avere un accesso limitato per garantire la sicurezza e ridurre al minimo le distrazioni.
- **Valuta l'infrastruttura IT:** quale tipo di infrastruttura IT possiedi? On-premise, basata su cloud o ibrida? In che modo influisce sull'efficienza del tuo SOC?



Scopri perché le organizzazioni stanno adottando una sicurezza cloud ibrida

[Scopri come](#)

✓ Collaborazione: migliorare il lavoro di squadra all'interno e all'esterno del SOC

- **Installa video wall:** utilizza videowall per mostrare flussi in tempo reale e migliorare la visibilità complessiva.
- **Investi in tool di comunicazione:** sfrutta soluzioni di comunicazione basate su SIP, come Sipelia™, per facilitare lo scambio di informazioni e il coordinamento tra i team.
- **Configura un indirizzo e-mail dedicato:** migliora le comunicazioni creando un indirizzo e-mail specifico per gestire tutte le richieste.
- **Smista e assegna task:** valuta l'implementazione di sistemi collaborativi per la gestione delle decisioni, come Mission Control™, per un'assegnazione efficiente delle attività.



✓ Contesto: ottenere una visione unificata

- **Sfrutta funzionalità di mappatura avanzate:** utilizza tool di mappatura nel SOC per visualizzare e comprendere facilmente gli eventi nelle varie strutture.
- **Connetti dispositivi IIoT:** migliora la percezione situazionale del contesto collegando dispositivi IIoT e aggregando i dati in un'unica piattaforma unificata.
- **Aggiungi finestre del browser ai pannelli di controllo:** integra trasmissioni di notizie e aggiornamenti dei social media per migliorare la percezione situazionale degli eventi esterni.



✓ Chiarezza: digitalizzare le informazioni per ricavare indicazioni operative immediate

- **Crea regole:** definisci regole facili da usare che eliminino i falsi allarmi e riducano il carico operativo degli operatori.
- **Automatizza i task:** crea flussi di lavoro automatizzati che gli operatori possano seguire durante i momenti critici per garantire che le notifiche siano gestite in conformità alle procedure di sicurezza.
- **Filtra i dati:** implementa tool di automazione per filtrare i dati, consentendo agli operatori di affrontare rapidamente le potenziali minacce.



✓ Coordinamento: gestire l'escalation e rispondere agli eventi in modo efficiente

- **Configura procedure operative dinamiche:** introduci procedure operative dinamiche con Mission Control™ per fornire risposte personalizzate alle diverse fasi dell'incidente.
- **Valuta diritti di escalation basati sulla workstation:** assegna diritti di escalation basati sulla workstation per reazioni più rapide ed efficienti durante le emergenze.



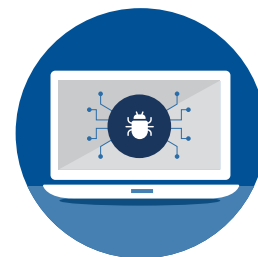
✓ Conformità: rispettare le normative

- **Assegna privilegi dell'utente:** ottimizza i privilegi dell'utente per garantire la conformità normativa.
- **Configura la generazione di report:** agevola le indagini forensi grazie a report sugli incidenti completi e ben organizzati.



✓ Cybersecurity: anticipare le minacce informatiche

- **Automatizza gli aggiornamenti di manutenzione:** configura task automatizzati per ricevere notifiche sugli aggiornamenti di manutenzione dei dispositivi e sullo stato di salute del sistema, al fine di mantenere un adeguato livello di cybersecurity.
- **Mantieni un registro-audit trail:** scegli un software che faciliti l'esportazione in formato nativo e la condivisione dell'archivio, mantenendo uno storico dettagliato.



Ottimizza il tuo centro operativo di sicurezza con l'aiuto di un sistema collaborativo di gestione delle decisioni

Scopri di più su Mission Control