# Secursat: Le linee guida per la progettazione di un Security Operation Centre

**Un *Security Operations Center* (SOC) può essere il cuore nella gestione della sicurezza e può essere pensato e progettato come luogo di raccolta di dati e di informazioni utili alla protezione del business, tanto quanto al management aziendale, per orientare scelte e decisioni. Non sempre l'aumento dei perimetri comporta il necessario aumento di risorse per la gestione, la tecnologia deve essere orientata guardando al futuro ed ai possibili cambiamenti di scenario. Alessio Cino, security project & design account all'interno del team di Business Development Secursat, condivide l'approccio da seguire nella progettazione di un SOC pensato come hub di governance tecnologica.**

***Quali sono le linee guida che regolano la progettazione di un Security Operation Center ed in che modo può essere pensato come un hub tecnologico?***

La struttura, il guscio, i sistemi di protezione, la o le piattaforme di integrazione e gestione, risorse e postazioni di lavoro, sono a grandi linee le scelte che le aziende si trovano ad affrontare per la progettazione di un Security Operation Center (SOC), o come viene definito dalla norma UNI CEI EN 50518:2020, Alarm Receiving Centre (ARC). Nel dettaglio la normativa di riferimento regola e guida le aziende nella scelta delle caratteristiche infrastrutturali e tecniche, dei sistemi di allarme ed alimentazione elettrica, nonché nelle modalità operative attraverso le quali devono essere gestiti gli allarmi e le segnalazioni, al fine di realizzare un luogo idoneo, e certificabile, per la gestione ed il monitoraggio dei sistemi di safety e security.

Secondo Secursat la necessità di rispettare queste linee guida deve essere orientata da un approccio integrato con gli obiettivi non solo della security ma del management in generale, per seguire il percorso di digitalizzazione ed innovazione nella gestione dei processi già ampiamente diffuso nelle organizzazioni. La risposta alla pandemia ha, infatti, reso ancora più evidente la necessità di accelerare l'adozione di modalità di gestione dei processi snelle ed efficaci, di sistemi capaci di collezionare dati ed informazioni puntuali per superare l'incertezza e stabilizzare il business attraverso un'azienda "più "intelligente" e, nel nostro caso, anche attraverso una security "più intelligente".

Una security intelligente secondo Secursat, in questa fase, implica più che l'adozione di nuove tecnologie, il revamping dei sistemi in campo o la ricerca di nuovi prodotti, un cambio di direzione radicale nella gestione dei processi di security ripensando il Security Operation Centre come luogo chiave nella gestione dei sistemi. Il SOC deve dunque essere progettato per essere agile, resiliente e capace di cambiare continuamente. Non una struttura rigida basata sul controllo ma un luogo di gestione dinamica di eventi di security e safety e di segnalazioni tecniche ed operative.

L'obiettivo è dunque progettare un "ARC" certificabile ai sensi della normativa, laddove necessario, uscendo dalla tradizionale concezione di gestione generica degli allarmi da parte di guardie particolari giurate, per invece progettare un SOC strategico dove attraverso competenze tecniche, di security e di analisi è possibile monitorare e gestire, da un lato, segnalazioni tecnologiche ed operative e attività legate all'infrastruttura IT (rete, sistemi ed applicazioni) e dall'altro eventi ed informazioni di security e safety per garantire la protezione dei siti, dei beni e delle persone dell'azienda o dei clienti. Secondo questo approccio il SOC diventa non solo il luogo dove monitorare in real-time eventi e situazioni, ma anche un centro di raccolta dati ed informazioni utili per prevenire scenari di evoluzione del rischio, studiare modelli di automazione dei sistemi, fornire risposte per ottimizzare le risorse ed implementare l'efficacia delle attività.

Adottare un modello diverso di gestione della sicurezza attraverso il SOC può aiutare piccole e grandi organizzazioni a mitigare i rischi, automatizzare le attività di routine attraverso modelli *human+machine* ma anche a ridurre i costi tradizionalmente associati alle attività extra, rivedendo il ruolo della security nell'organizzazione aziendale.

Per realizzare questo modello, secondo il nostro approccio, utilizzato sia nella progettazione dei nostri *Security Operation Center* certificati e sia in progetti di supporto alla progettazione di SOC o alla scelta delle piattaforme da parte dei nostri clienti, in primo luogo è necessario partire dall'analisi della *capacity*. Il nostro team si basa sull'analisi de dati relativi alle segnalazioni dei sistemi presenti in campo, classificandole e studiandone il comportamento, nonché analizza e comprende la tipologia dei siti da connettere per uscire dall'equivoco che un numero maggiore di siti e collegamenti debba necessariamente comportare un aumento degli investimenti in risorse. Il team Secursat, grazie ad un mix di competenze di analisi, tecniche dei sistemi tradizionali e IT, aiuta dunque a comprendere le migliori scelte tecnologiche e definisce la *road-map* per rimodulare le caratteristiche delle piattaforme di integrazione. L'obiettivo è consentire un monitoraggio evoluto dei sistemi e delle segnalazioni con un impatto diretto sulla riduzione dei costi associati alle attività extra, nonché standardizzare il modello di gestione degli eventi, classificandone la tipologia, per disporre di dati da fornire al management per monitorare KPI e processi.

Un altro aspetto, non meno importante interessa invece la capacità del SOC di garantire la *business continuity* nella gestione delle attività nonché *backup* e *disaster recovery*, tutte attività rivelatesi strategiche soprattutto durante la pandemia dove il SOC, nel nostro caso, è diventato il luogo per continuare a garantire la continuità operativa dei nostri clienti da remoto. Il nostro team, parallelamente alle scelte infrastrutturali e relative alle piattaforme, contribuisce a ripensare l'infrastruttura di rete ed i modelli di collegamento, basandosi su soluzioni cloud-based e guardando agli standard di sicurezza internazionale, nonché includendo nei ragionamenti complessivi anche valutazioni relative alla protezione dei server e degli apparati hardware necessari per garantire il buon funzionamento del SOC e anche la sicurezza delle informazioni processate.

Per ultimo, nel pensare alla realizzazione di un SOC, occorre analizzare risorse e competenze necessarie nonché definire procedure e regole di comportamento delle persone come dei sistemi, in modo da garantire da un lato il rispetto delle procedure aziendali e dall'altro ridurre la discrezionalità degli operatori. Seguendo il percorso tracciato nella progettazione di un SOC, secondo Securesat, pensare alle risorse in maniera innovativa significa abbandonare i tradizionali processi decisionali *top-down*, e formare team con un mix di competenze tecniche e tecnologiche, relative ai più diffusi sistemi di security e safety presenti sul mercato per monitorare gli eventi ma anche gestire le segnalazioni operative, e con competenze di security e di analisi per l'utilizzo di piattaforme utili per il monitoraggio degli scenari internazionali come dei viaggiatori dell'azienda o dei clienti. Il SOC dovrebbe dunque essere popolato da team responsabilizzati con obiettivi e regole chiare nella gestione dei sistemi, guidati e supportati dai dati e dalla tecnologia, secondo logiche *end-to-end*, per una maggiore e migliore velocità di risposta e gestione. In questo senso il team Securesat aiuta dunque a definire le modalità di implementazione delle piattaforme di gestione dei sistemi, di travel security, di localizzazione, etc. e le modalità di utilizzo delle stesse da parte degli operatori. L'obiettivo è garantire che la gestione degli eventi garantisca a sua volta risposte rapide, prevedendo la formazione delle risorse, per identificare nuovi talenti e competenze capaci di rispondere alle esigenze di gestione degli eventi, nonché l'affiancamento delle stesse nelle fasi di avvio e start-up del progetto.

In conclusione le *guide-lines* brevemente rappresentate definiscono un modello dove gli investimenti in tecnologia e nelle modalità di applicazione della stessa garantiscono una reale riduzione dei costi fissi e delle attività extra, privilegiando la qualità delle risorse umane alla quantità. Secondo questo approccio il SOC diventa un luogo dove monitorare i rischi legati alla *business continuity*, gestire gli improvvisi cambiamenti nelle necessità, prendere decisioni real-time prevedendo e mitigando i rischi di sicurezza, fornire dati ed informazioni utili all'intera organizzazione, grazie ad un insieme di tecnologie e competenze che garantiscono una buona reazione alle crisi, oggi, e che saranno utili anche nel prossimo futuro per una vera capacità di resilienza da parte della security.

Una progettazione che segue le esigenze e le normative attualmente in essere, cercando allo stesso tempo di prevedere un punto di rottura definitiva in cui la linea di demarcazione tra sicurezza fisica e virtuale sarà completamente intangibile, ponendo le basi per consentire la futura evoluzione dei nostri "tradizionali" centri di monitoraggio in *Network Operation Center* (NOC) o *Global Security Control Room (GSCR)* capaci di superare i confini territoriali, sincronizzare le esigenze della *physical-security* con quelle IT ed adottare logiche di *machine-learning*.