

SOC o NOC?

Gli scenari evolutivi nella gestione remota della security

di Maura Mormile, Business Development Manager di Secursat

Security Operation Centre o Network Operation Centre?

È una domanda alla quale possiamo rispondere condividendo una concreta ed attuale visione della possibile evoluzione dei modelli di gestione delle Control Room.

Security Operation Centre, Control Room o, come li definisce la norma UNI CEI EN 50518:2020, *Monitoring Alarm Receiving Centre*, possono diventare il centro nevralgico nella gestione dei servizi di sicurezza.

Le tecnologie e gli apparati di security possono difficilmente fare la differenza nella costruzione e la gestione di un moderno modello di sicurezza complesso, che può essere completo solo attraverso lo sviluppo di adeguati processi di gestione tecnologica, locale o remota, che consentano di realizzare una governance della sicurezza.

Secursat, in considerazione del sempre più rapido allineamento tra le tematiche di sicurezza fisica e sicurezza logica, e della sempre crescente importanza della rete nello sviluppo dei processi aziendali a tutti i livelli, sta attuando modelli di gestione della sicurezza che evolvono in questa direzione.

Stiamo infatti realizzando progetti innovativi con la consapevolezza che, all'interno di una Control Room, piattaforme di integrazione, di gestione tecnologica o di gestione video non sono più sufficienti a fare del SOC un luogo adeguato per un'organizzazione a progettare modelli di sicurezza efficaci.

Così, da un lato i nostri tecnici, nell'approccio alla progettazione di luoghi di gestione tecnologica remota, hanno studiato quali sono le caratteristiche tecniche che consentono di rispettare i requisiti previsti dalle normative, quali sono le soluzioni tecnologiche e di layout (postazioni



ergonomiche, matrici video, monitor, etc.) più efficaci per rispondere ai bisogni di gestione; dall'altro, i nostri analisti, pensando alle evoluzioni di sviluppo del business, hanno studiato come poter garantire business continuity e disaster recovery per noi e per i nostri clienti, e come gestire la trasmissione dei dati consentendo la sicurezza delle informazioni, rispetto della privacy e data collection. L'infrastruttura di rete che regola il processo di scambio dati ed informazioni e la ridondanza dei sistemi - nel nostro caso garantita anche dalla presenza di due *Security Operation Centre* certificati - diventano quindi il principale punto di attenzione nello sviluppo dei progetti di security. In questo senso, nella nostra visione il SOC, nella sua accezione tradizionale già da oggi ed ancor più nei prossimi anni, tende ad evolversi verso un modello più assimilabile ad un Network Operation Centre, ovvero un luogo dove monitorare anche lo stato di funzionamento della rete, delle connessioni e dei collegamenti di comunicazione.



La progressiva evoluzione da SOC a NOC e l'integrazione tra piattaforme di gestione eventi derivanti dai sistemi di sicurezza tradizionali, come telecamere, sensori, etc. e piattaforme per il monitoraggio dello stato della rete e delle comunicazioni, renderà possibile dunque affrontare le sfide imposte dal prossimo futuro.

Il SOC dev'essere concepito come luogo, fisico e virtuale, dove approfondire da remoto guasti e malfunzionamenti, indagare sullo stato di apparati, sensori e sistemi, indirizzando gli sforzi in maniera mirata e utilizzando la rete come strumento per consentire manutenzione remota e, quindi, ridurre gli impatti degli interventi onsite non necessari.

Dunque, non solo come luogo dove gestire eventi e segnalazioni che rappresentano "un di cui" di un processo molto più ampio, ma l'elemento base di un percorso volto a costruire per aziende ed organizzazioni una governance tecnologica della sicurezza; dove garantire la business continuity, in caso di emergenza, per dare supporto nella ricostruzione di eventi e situazioni critiche mediante l'analisi

dei dati dei sistemi tecnologici; dove identificare, tra la grande mole di dati ed informazioni a disposizione, quelli utili per migliorare i processi di sicurezza ed ottimizzare le risorse.

Un mix di competenze di progettazione tradizionale ed informatica, investimenti in tecnologie di monitoraggio evolute e conformi agli standard di sicurezza oramai diffusi nel mercato internazionale, insieme ad una visione volta a rendere, anche fisicamente, il SOC un luogo idoneo ad una gestione tecnologica evoluta.

Tra *Security Operation Centre* e *Network Operation Centre*, a noi di Secursat piace parlare di Hub Tecnologico, aperto all'innovazione concreta, capace di operare secondo le logiche tradizionali di un SOC ed in conformità con le normative. Allo stesso tempo, un luogo dove le piattaforme ed i modelli di servizio vengono gestiti su cloud e vengono programmati per raccogliere e analizzare dati e informazioni, utili anche al management aziendale per orientare scelte e decisioni, e dove la rete diventa la condizione essenziale per la garanzia della continuità del servizio.



Contatti:
Secursat
Tel. +39 0141 33000
www.secur-sat.com