Security Operation Center… oltre la norma!

di Francesca Balducci, Security Assessment e Data Analysis Account Securesat

Analisi della capacity, organizzazione delle risorse ed attività di data detective sono le basi per creare un luogo di gestione tecnologica. Francesca Balducci, Security Assessment e Data Analysis Account all'interno del team di Business Development di Securesat condivide un approccio innovativo per l'organizzazione e la gestione di un Security Operation Centre.

L'idea che ha accompagnato il percorso di crescita di Securesat nel corso degli ultimi anni è che il processo di costruzione di una security governance strutturata e capace di inserirsi nei processi decisionali e aziendali e dunque, di fornire un contributo primario nella garanzia della continuità del business, affonda le sue radici in un terreno ancora fortemente condizionato da idee e strutture di sicurezza tradizionali.

Se da un lato, l'obiettivo di chi "fa sicurezza" e si occupa di gestione dei rischi, rimane ancora quello di garantire una gestione degli eventi - intesi in senso ampio del termine - in grado di fornire risposte rapide, dall'altro si fa sempre più presente la necessità e, conseguentemente, la richiesta da parte delle aziende di comprendere nel dettaglio le dinamiche insite nell'operatività di un Security Operation Centre (SOC), anche in chiave analitica.

Attraverso progetti di analisi della capacity dei SOC dei nostri clienti nel settore dell'energia, nell'industria, nei trasporti ed attività di data detective, con il team di Business Development di Securesat , siamo giunti all'idea che **il SOC sia un luogo di raccolta di dati ed informazioni utili per l'analisi gli scenari di evoluzione del rischio, nonché per avviare azioni di ottimizzazione che consentano di supportare operativamente la costruzione di una Security Governance aziendale *business oriented*.**

Abbiamo dunque sviluppato un modello dedicato ai Security Operation Centre che parte dallo studio dei processi operativi e gestionali all'interno di un SOC, per essere in grado di fornire risposte utili per la rimodulazione di piani strategici, per ottimizzare le risorse ed implementare efficacemente soluzioni tecnologiche e procedure operative.

In questo senso, progettare un SOC non significa più solamente pensare e definirne la struttura architettonica rispettando i requisiti di layout e le caratteristiche infrastrutturali previste dalla norma UNI CEI EN 50518:2020 ma anche, e soprattutto, avviare attività di riorganizzazione delle risorse a disposizione e investimenti in tecnologie mirati e tarati sulle esigenze aziendali per costruire un modello di sicurezza aziendale unico.

Se l'obiettivo è quello di garantire una gestione degli eventi in grado di fornire risposte rapide, dall'altra si fa sempre più strada la consapevolezza che i dati e le informazioni rimandate dai sistemi e dalle tecnologie in campo, nonché le modalità gestionali dei processi e delle procedure in essere possano fornire un valore aggiunto e supportare la ridefinizione degli investimenti e delle strategie di business.

"Il contributo che il team di Business Development offre è quello di analizzare le logiche di funzionamento dei sistemi tecnologici presenti, condurre un Vulnerability Assessment per fornire un quadro completo relativo alla capacity - tecnologica, infrastrutturale ed operativa - del SOC"

Il contributo che il team di Business Development offre è quello di analizzare le logiche di funzionamento dei sistemi tecnologici presenti, condurre un *Vulnerability Assessment* per fornire un quadro completo relativo alla capacity – tecnologica, infrastrutturale ed operativa - del SOC.
Il nostro obiettivo è comprendere le modalità di gestione tecnologica e dei sistemi, la loro adeguatezza rispetto alle caratteristiche strutturati e gestionali (numero e tipologia di impianti gestiti, numero e tipologia di segnalazioni e allarmi presi in carico, competenze degli operatori e delle risorse impiegate nel SOC), nonché rispetto ai target e alle esigenze aziendali, ma anche quello di avviare percorsi di *data detection* e analisi dei dati tecnologici provenienti dai sistemi di supervisione e di gestione integrata dei sistemi di security e safety, per identificare quelli utili per ottimizzare le scelte e le decisioni aziendali.
Ciò che ci consente di fare il salto di qualità e di definire la nostra una "consulenza operativa", sono il mix di esperienza tecnico-tradizionale, la conoscenza dei meccanismi tipici dell'operatività di un SOC e le competenze gestionali, organizzative ed analitiche.
A fare la differenza in questo processo non è tanto la capacità di elaborare e analizzare questi dati, quanto essere in grado di definire la struttura del data-lake ottimale per il raggiungimento dei KPI e delle metriche aziendali nonché definire le modalità attraverso le quali utilizzare questi dati in chiave operativa: i dati elaborati e analizzati nel corso di progetti strutturati di consulenza, rimandando quasi sempre ad una serie di informazioni spesso disarticolate, proposte secondo modalità eterogenee e difficilmente interpretabili ai non addetti ai lavori. Quello che le aziende ricercano è, infatti, la possibilità di disporre di dashboard interattive, aggiornate in *real time*, capaci di monitorare KPI *(Key Performance Indicator)* e individuare KRI *(Key Risk Indicator)*.

E l'obiettivo del team di Business Development di Secursat è proprio quello di analizzare i dati *raw*, provenienti dai database a disposizione, aiutare il cliente a comprendere come standardizzarli e strutturarli in maniera organizzata e fornire suggerimenti e indicazioni relativamente alle modalità attraverso cui analizzare le informazioni attraverso sistemi di business intelligence.
Lo step successivo, e che spesso si tende a tralasciare, è che le implementazioni e le ottimizzazioni tecnologiche e a livello di sistemi, da sole non bastano a garantire il raggiungimento degli obiettivi e dei risultati aspettati: è la modalità attraverso cui la tecnologia e i servizi vengono gestiti che consente poi di raggiungere risultati misurabili.
In questa prospettiva, Secursat pone con molta enfasi l'attenzione sulla necessità e sull'importanza di formare e informare operatori, addetti e risorse dedicate alla gestione e all'organizzazione della sicurezza a qualsiasi titolo. Attraverso questo approccio innovativo, abbiamo dunque creato un modello per sdoganare la tradizionale concezione di un Security Operation Center come luogo ove si gestiscono gli allarmi, dissociandoci da un'idea di passività, ma pensandolo come hub tecnologico dove si costruisce e dove fondano le radici per implementare una governance tecnologica della sicurezza. Progettare e costruire una security governance per rimodulare gli interventi di security e ottimizzare i processi aziendali secondo un'ottica di integrazione e flessibilità è certamente, infatti, la finalità e la richiesta di molti clienti anche se, soprattutto negli ultimi tempi, viene spesso richiesto anche di avere un occhio di riguardo alle sempre più emergenti tematiche relative all'ambiente ed allo sviluppo di politiche sostenibili.
Per questo per il prossimo futuro, come team di Business Development, stiamo sviluppando un approccio che consente di misurare, attraverso la gestione della security, anche gli obiettivi di sostenibilità aziendale, con la consapevolezza che le tematiche relative alla sostenibilità si sono ormai poste come *driver* dei meccanismi e dei processi aziendali guidando la definizione delle strategie dei più grandi gruppi e compagnie nazionali ed internazionali ed è in questa prospettiva che, a nostro avviso, la gestione tecnologica ed il fattore umano possono e devono acquisire un ruolo di primaria importanza.

SECURSAT
Build your security

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