

L'Hub tecnologico Secursat: dalla security alla gestione del rischio

intervista a Maura Mormile, Business Development Manager di Secursat

A quasi un anno dall'inaugurazione dell'Hub Tecnologico dedicato alla gestione del rischio, presso Torre Monforte nel cuore di Milano, **Maura Mormile**, Business Development Manager di **Secursat** racconta il percorso di creazione dell'Hub e le basi del modello innovativo.

Come è nato questo progetto?

Alla luce delle evoluzioni degli scenari internazionali e delle dinamiche che interessano la gestione del rischio che hanno reso la velocità di azione e la capacità di adattamento indispensabili per rispondere alle nuove minacce, chi si occupa di sicurezza può mettere in campo la capacità di lavorare in emergenza e di gestione delle crisi.

Ma l'*expertise* della sicurezza tradizionale non basta più, i confini fisici e virtuali sempre più sfumati e l'interconnessione tra le dinamiche economiche e quelle tecnologiche hanno reso necessario lo sviluppo di nuove competenze, nuovi approcci e nuovi modelli. È per questo che noi di Secursat abbiamo investito nel nostro Hub tecnologico, realizzato nel cuore di Milano, per creare un polo di gestione tecnologica di una security capace di essere lo strumento di prevenzione e gestione dei rischi, e per trasformarci da esperti a professionisti.

Cosa è l'Hub Tecnologico Secursat?

L'Hub Tecnologico Secursat è innanzitutto un MARC, come lo definisce la norma 50518:2020, ma non solo. È stato, infatti, pensato e strutturato per rispondere a tutti i requisiti della certificazione necessaria per lo svolgimento delle nostre attività, ma noi nell'idea che la gestione remota possa estendere il concetto di sicurezza tradizionale ad una governance tecnologica completa e quindi ad una gestione dei rischi anche operativi, abbiamo cercato di fare molto di più.

Abbiamo creato un centro di supervisione e gestione delle tecnologie, dove l'allarme, per noi, è "solo" un evento straordinario, di un insieme di processi molto più ampi e che nel loro insieme possono garantire la gestione dei rischi in senso completo, e non solo quelli fisici. Non ci piace parlare di "sicurezza" perché ci sentiamo più affini ad un concetto di "gestione dei rischi". La sicurezza, troppo spesso, rimanda ad un concetto tradizionale, racchiuso nella sfera fisica o piuttosto in quella digitale mentre noi riteniamo di essere per i nostri clienti un partner completo che può accompagnare nella gestione di



una serie di processi che alle volte possono sembrare marginali rispetto ai modelli tradizionali e che, invece, oggi a nostro avviso diventano prioritari. La capacità di ridurre attività reiterate, la capacità di ridurre attività on-site non necessarie con impatti misurabili sulla riduzione di Km non percorsi e CO2 non emessa o, ancora, il monitoraggio dei consumi energetici unito a quello delle tecnologie di security. Si parla di "società liquida", per noi oggi anche la security è diventata liquida, con perimetri fisici e virtuali sempre più labili e dove strategiche diventano, se gestite e integrate in un modello più ampio, le attività di *maintenance* e della gestione del *facility* come necessarie parti integranti di un unico modello.

L'Hub per noi è però anche una sorta di *showroom* della sicurezza, un luogo dove vedere, fare, sperimentare, testare, progettare, pensare, analizzare. Non un luogo nascosto, ma un punto di riferimento dove poter anche ripensare modelli di gestione complessiva, effettuare test operativi. Perché se i prodotti oramai sono *commodities* molto spesso tecnologicamente affini per varie fasce di prezzo, è la capacità di gestione, a fare la differenza. E abbiamo creato l'Hub per dire non solo che questo modello siamo riusciti a realizzarlo, ma che lo facciamo anche vedere, testare.

Quali sono stati gli elementi principali alla base di questo progetto?

In primis chiaramente quelli tecnici legati alla struttura e soprattutto all'infrastruttura di rete. Su questo punto oltre all'Hub di Milano abbiamo un secondo MARC sempre certificato

50518:2020 per garantire *disaster recovery e business continuity*. In secondo luogo, ci siamo concentrati sulle tecnologie e soprattutto su quelle di integrazione. Ad oggi non siamo ancora riusciti a trovare sul mercato un'unica piattaforma capace di rispondere alle esigenze dei nostri clienti e quindi abbiamo messo insieme una serie di competenze e tecnologie per essere flessibili e poliedrici.

Il cuore del modello è stata l'analisi della *capacity*, ovvero un'analisi del mix di competenze, tecnologie e numero di risorse necessarie per gestire un certo numero di siti, di impianti e di attività. Un percorso che abbiamo sperimentato su di noi e che è poi diventato un prodotto per altri clienti che, come noi, hanno centri di gestione SOC/NOC certificati o meno, e che si domandano: ma quante persone servono per gestire il perimetro dei siti? Noi oggi, grazie ad un modello strutturato e un team con competenze multifunzionali, siamo in grado di rispondere a questa domanda, partendo dai dati.

Un altro aspetto, non meno importante, è stato quello del *design*, abbiamo anche scelto partner importanti presenti soprattutto in ambito internazionale dalla Spagna alla Germania, per avere un insieme di strumenti che potessero, da un lato trasmettere l'idea di un polo tecnologico all'avanguardia e, dall'altro, rendere confortevole l'attività degli operatori, che per noi sono figure tecniche preziosissime. Dalle luci dimmerabili, per rendere l'ambiente da un "bunker" senza finestre ad un'area accogliente, e agevolare il lavoro in turnazione, a scrivanie di design personalizzate che, oltre a essere ad alto valore estetico, consentono una gestione ottimale dei cavi / delle tecnologie, fino alla più evoluta tecnologia di matrice video per gestire i video con una molteplicità di scenari molto complessa.

Quali competenze sono state necessarie?

Le competenze necessarie sono state molte, a partire da quelle "tradizionali" di security perché, per gestire da remoto i sistemi, abbiamo avuto bisogno di persone che hanno lavorato sul campo tecnicamente, per anni e che conoscono le dinamiche di gestione di prodotti anche oramai datati, fino a quelle informatiche. Abbiamo peraltro aggiunto alcune piattaforme di monitoraggio anche delle reti per sancire il nostro passaggio da "SOC" a "NOC" e pensato la struttura per garantire la protezione dei dati e delle informazioni. Oltre alle competenze tecniche, tradizionali o informatiche, è stato necessario fare scendere in campo anche i nostri security manager certificati che, parte del team Secursat, hanno aiutato a realizzare un luogo idoneo alla gestione del rischio cercando di andare oltre ai concetti



tradizionali, lavorando su procedure e regole di comportamento, oltre quelle previste chiaramente dalle normative.

Quanto contano i dati?

I dati contano moltissimo, ma quello che abbiamo imparato è che conta maggiormente la capacità di comprendere nella oramai infinita moltitudine di dati a disposizione, quali sono quelli utili per indirizzare i comportamenti e prendere delle decisioni. Da questo punto di vista noi ci ispiriamo a settori anche apparentemente molto lontani dalla security, dove l'automazione e la prevenzione sono concetti oramai diffusi e trasversali e completamente integrati all'interno dei processi decisionali, e ci siamo orientati sull'utilizzo di *dashboard* di sintesi perché per noi rappresentano uno dei migliori valori aggiunti del nostro servizio.

Per il futuro, qual è la sfida più grande?

Sicuramente una riflessione è verso il mercato ed il generale approccio alla security. La sicurezza, purtroppo, in generale, è spesso poco comunicata o comunicata in maniera tradizionale sia all'esterno che all'interno delle organizzazioni e quindi percepita come un costo. Il valore aggiunto che cerchiamo di dare è reinterpretare questo scenario tradizionale e pensare ad un insieme di processi che, se strutturati, possono dare grande valore aggiunto all'interno delle organizzazioni in termini di controllo (non delle persone ma delle tecnologie), in termini di ottimizzazione, di miglioramento dei livelli di efficacia e di efficienza. Per noi, guardando al futuro, la sfida più grande è quella di trovare o sviluppare sul mercato delle vere piattaforme di integrazione e gestione automatizzata capaci di non guardare solo al piccolo universo tecnologico della security e di trovare presso i clienti interlocutori "illuminati" capaci di cogliere il valore innovativo di questo progetto.



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