Security Operations: dal perimetro alla resilienza operativa



La crescente sofisticazione delle minacce informatiche e la dissoluzione dei perimetri tradizionali impongono un ripensamento radicale delle strategie difensive. Le *Security Operations* (SecOps) rappresentano oggi molto più di un approccio metodologico: sono il tentativo di tradurre principi difensivi in processi operativi scalabili, misurabili e adattivi, capaci di rispondere a un panorama delle minacce in continua evoluzione.

La convergenza tra Security e Operations: una sfida culturale e strutturale

Quando si parla di *SecOps*, si fa riferimento a una convergenza strategica tra security e IT operations, nata dalla necessità di superare i silos organizzativi che hanno tradizionalmente separato chi protegge da chi sviluppa. Questa integrazione, apparentemente ovvia sulla carta, si scontra nella pratica con tensioni culturali profonde e sfide strutturali significative.

Il problema non è esclusivamente culturale, sebbene l'attrito tra sviluppatori orientati alla velocità e professionisti della sicurezza focalizzati sui controlli sia tangibile. La questione è architettonica: i cicli di sviluppo moderni, caratterizzati da rilasci continui e *pipeline* automatizzate, operano a velocità incompatibili con le prassi tradizionali di *security assessment*. Come evidenziato nel panorama dei Security Operations Center contemporanei, non si tratta di

rallentare lo sviluppo per implementare controlli di sicurezza, ma di riprogettare la sicurezza stessa perché diventi parte integrante e nativa dei processi di sviluppo.

Un SOC tradizionale, con analisti che monitorano *dashboard* alla ricerca di anomalie, non scala in contesti dove quotidianamente vengono rilasciati centinaia di microservizi. La telemetria deve essere raccolta diversamente, gli *alert* contestualizzati con maggiore granularità, le risposte orchestrate con automazione intelligente che i *playbook* statici non possono offrire.

Automazione intelligente: tra efficienza e nuove fragilità

L'automazione rappresenta il mantra degli ultimi anni in ambito cybersecurity, promettendo di trasformare rilevamento, risposta e *remediation* in processi scalabili. Gli strumenti di *Security Orchestration, Automation and Response* hanno effettivamente ridotto i tempi di reazione da ore a minuti in molti scenari. Tuttavia, l'automazione è efficace solo quanto sono accurati i modelli su cui si basa.

Il rischio concreto è quello di automatizzare la mediocrità: sistemi che rispondono rapidamente ma in modo inadeguato, che classificano minacce secondo schemi rigidi facilmente aggirabili dagli attaccanti, che generano volumi di *alert* tali da desensibilizzare gli analisti che dovrebbero supervisionarli. L'*intelligenza artificiale* e il *machine learning*, pur promettenti, introducono nuove vulnerabilità: modelli che possono essere ingannati, *bias* che amplificano errori umani, opacità decisionale che complica la spiegazione delle classificazioni.

Il fattore umano nelle Security Operations

Il vero valore di un *Security Operations Center* maturo risiede nella capacità degli analisti di andare oltre gli *alert* automatici, correlare informazioni da fonti eterogenee,

intuire *pattern* che nessun algoritmo ha ancora imparato a riconoscere. È l'analista che identifica una sequenza di accessi apparentemente legittimi che nasconde un *living off the land attack* – tecnica in cui gli attaccanti utilizzano strumenti legittimi del sistema per condurre attività malevole rimanendo sotto il radar dei controlli tradizionali.

Emerge qui una tensione critica: come mantenere competenze umane di alto livello in un contesto che spinge verso l'automazione massiva? Come trattenere talenti quando la routine quotidiana rischia di ridursi alla gestione di falsi positivi? Le organizzazioni che eccellono nelle *SecOps* sono quelle che investono non solo in stipendi competitivi, ma in ambienti dove la curiosità intellettuale viene premiata, dove esiste tempo e spazio per approfondire, sperimentare, apprendere.

Il contesto normativo europeo: NIS2 e resilienza operativa

Il quadro normativo europeo, con l'implementazione della Direttiva NIS2 entrata in vigore nel ottobre 2024, sta ridefinendo gli standard di resilienza operativa. La normativa impone requisiti stringenti sulla gestione degli incidenti: le organizzazioni devono notificare gli incidenti significativi entro 24 ore dalla loro rilevazione (*early warning*), fornire un report dettagliato entro 72 ore e un report finale entro un mese.

Questi obblighi rendono esplicito ciò che molti professionisti della sicurezza sostengono da tempo: non è più accettabile scoprire una compromissione mesi dopo il fatto, non è più sostenibile affidarsi a controlli *spot* e verifiche annuali. La NIS2, con il suo focus sulla resilienza operativa e sulla capacità di risposta tempestiva, sta di fatto imponendo l'adozione di capacità *SecOps* anche a organizzazioni che finora le consideravano un lusso per *enterprise* di grandi

dimensioni.

Security Operations modulari per organizzazioni di ogni dimensione

Implementare *SecOps* efficaci in contesti con risorse limitate richiede pragmatismo e creatività. Non tutte le organizzazioni possono permettersi un SOC attivo 24/7 con team dedicati o le piattaforme più sofisticate. Tuttavia, è possibile costruire capacità operative di sicurezza significative se si hanno chiari gli obiettivi e si è disposti a fare scelte strategiche su dove concentrare gli investimenti.

Le *SecOps* moderne devono essere pensate come sistemi modulari e componibili, dove diverse organizzazioni possono combinare capacità interne con servizi gestiti, strumenti commerciali con soluzioni *open source*, competenze specialistiche con formazione continua del personale esistente. L'essenziale è avere una visione d'insieme, una comprensione chiara dei rischi specifici che si affrontano e delle capacità necessarie per gestirli. L'integrazione di *threat intelligence* e l'adozione di approcci basati sul rischio diventano fattori abilitanti fondamentali.

SIEM e gestione centralizzata degli eventi

I sistemi di *Security Information and Event Management* (SIEM) costituiscono il cuore tecnologico delle operazioni di sicurezza moderne, aggregando e correlando eventi da fonti eterogenee. Tuttavia, la loro efficacia dipende criticamente dalla qualità della configurazione, dalla capacità di *tuning* continuo e dall'integrazione con altri strumenti dell'ecosistema di sicurezza.

Un SIEM mal configurato genera più problemi di quanti ne risolva: falsi positivi che saturano i team, falsi negativi che permettono agli attaccanti di operare indisturbati, complessità operativa che richiede competenze specialistiche difficili da trovare e trattenere. L'evoluzione verso

piattaforme di *Extended Detection and Response* (XDR) promette di superare alcune di queste limitazioni attraverso maggiore automazione e correlazione intelligente.

Vulnerability Management e approccio proattivo

La gestione proattiva delle vulnerabilità rappresenta un pilastro fondamentale delle *Security Operations* efficaci. Non si tratta semplicemente di applicare *patch* quando disponibili, ma di comprendere il panorama delle vulnerabilità nella propria infrastruttura, prioritizzarle in base al rischio effettivo, e implementare *remediation* in modo coordinato che non comprometta la continuità operativa.

L'approccio *Continuous Threat Exposure Management* sta emergendo come paradigma evolutivo, superando i tradizionali *vulnerability assessment* periodici a favore di una valutazione continua della superficie di attacco e dell'esposizione al rischio.

Il futuro delle Security Operations: resilienza adattiva

Se esiste una caratteristica distintiva delle *Security Operations* è la loro natura perpetuamente incompiuta. Non si arriva mai a un punto in cui il lavoro è fatto, i processi sono perfetti, la sicurezza è garantita. Ogni miglioramento nelle capacità difensive viene rapidamente incorporato dagli attaccanti nei loro modelli di attacco. Ogni nuova tecnologia adottata introduce nuove superfici di attacco da proteggere.

Il concetto di *cyber resilience* – la capacità non solo di prevenire gli incidenti ma di resistere, adattarsi e recuperare rapidamente quando si verificano – sta diventando centrale. Le organizzazioni più mature stanno evolvendo da un modello incentrato sulla prevenzione verso uno che bilancia prevenzione, rilevamento rapido, contenimento efficace e

recupero resiliente.

Conclusioni: Security Operations come percorso continuo

Forse è proprio in questa tensione continua, in questa necessità di evolvere costantemente, che le *Security Operations* trovano il loro senso più profondo. Non sono una destinazione ma un percorso, non sono una soluzione ma un approccio per navigare la complessità irriducibile della sicurezza informatica moderna. In un panorama dove le certezze sono sempre più rare e le minacce sempre più sofisticate, l'umiltà operativa e la capacità di apprendimento continuo rappresentano forse le competenze più preziose.

Le organizzazioni che eccellono nelle *SecOps* non sono quelle che hanno eliminato ogni rischio – obiettivo irrealistico – ma quelle che hanno costruito la capacità di rilevare rapidamente le anomalie, rispondere efficacemente agli incidenti, apprendere da ogni evento e adattare continuamente le proprie difese. In questo senso, le *Security Operations* rappresentano meno una funzione tecnica e più un paradigma organizzativo che permea cultura, processi e tecnologie.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/security-operations/