Automation & Orchestration:

l'evoluzione dei Servizi MDR

SecurityLab
Prevent and protect

ALERT MANAGEMENT

I Team di Security si trovano a dover affrontare una sfida quotidiana legata alla rilevazione, smistamento e gestione di enormi quantitativi di alerts

TRIAGE

ALERT MANAGEMENT

È il processo che si trova esattamente tra le fasi di TRIAGE e generazione dell'ALERT. Molti strumenti di AM sono integrati all'interno di un SIEM, ma nessuno di questi applica **l'AUTOMATION** a supporto del SOC

ALERT

Quando il numero degli alert aumenta in modo significativo, è necessario un diverso approccio alla loro gestione

LA NOSTRA ESPERIENZA

Veicolare ogni singolo alert all'interno di un canale Slack, non era più sufficiente con l'aumento drastico del numero si segnalazioni

COME GESTIRE L'ASSEGNAZIONE DEGLI ALERT?

COME CREARE FOLLOW-UP?

COME TRATTARE GLI ALERT DUPLICATI?

COME VELOCIZZARE I TEMPI DI PRESA IN CARICO E REAZIONE?

REQUIREMENTS

Sono state chiare quali fossero le caratteristiche indispensabili per il sistema di alert management del quale avevamo bisogno

ALERT INGESTION DA OGNI SISTEMA DI DETECTION

SOPPRESSIONE E DEDUPLICA DEGLI ALERT

TRIAGE AUTOMATIZZATO E GESTIONE DISTRIBUITA DEGLI ALERT

METRICA E CATEGORIZZAZIONE DEGLI ALERT

Nessuno dei Vendor con i quali collaboriamo aveva una soluzione integrata con queste caratteristiche

REALIZZIAMO UN SISTEMA DI ALERT MANAGEMENT EFFICIENTE

SOAR

Piattaforma con funzionalità di orchestrazione, automazione e risposta agli eventi di sicurezza, è il cuore pulsante sul quale è costruito il nostro sistema

INCIDENT MANAGEMENT

Servizio di gestione degli alert e collecting degli incident che consente al Team di veicolare in maniera chiara le segnalazioni sugli analisti di competenza e coinvolgere direttamente l'enduser in caso di escalation

COLLABORATION

Piattaforma operativa a supporto del Team per l'interazione diretta con i sistemi. Riceve gli alert normalizzati e standardizzati per consentire al Team un processo di intervento rapido ed efficace

CONTESTUALIZZAZIONE E DEDUPLICA

Nel nostro sistema di Alert Management, il "contesto" è l'informazione derivata dal payload dell'allarme che viene utilizzata come metadati per la soppressione, la deduplica e le metriche. La riduzione del rumore è principalmente attribuita alla sua capacità di utilizzare il contesto per impedire che gli allarmi inutili arrivino al SOC, secondo il principio di »poco rumore -> alto valore»

SOPPRESSIONE

disattivazione automatica di alert di scarso valore o importanza

DEDUPLICA

Eliminazione di alert duplicati o simili tra loro

Ciò è possibile perché viene generato un contesto per ogni alert a partire da due informazioni: il Nome e i campi del Payload dell'alert. Tutti i campi del Payload vengono utilizzati, inclusi quelli multipli

SecurityLab
Prevent and protect

AUTOMATION Qualsiasi processo che interpreta e elabora un alert prima che venga assegnato

Raccolta e razionalizzazione delle informazioni

Opzioni di automated response

Workflow specifico per singoli alert

Logiche di deduplica per gruppi di alert ricorrenti

PERCHÉ AUTOMATION & ORCHESTRATION PER IL NOSTRO MDR

- La cybersecurity è un settore in continua **evoluzione** e richiede un costante monitoraggio delle minacce in tempo reale
- L'automazione può aiutare a gestire in modo efficiente un alto volume di allarmi, **migliorare e supportare le prestazioni del Team**
- Grazie all'automazione, il 20% degli alert è stato gestito senza alcun intervento umano consentendo un **risparmio medio di 16 h lavorative**
- Solo 5 alert rappresentavano il 56% di tutte le attività del SOC. Con l'introduzione dell'alert management è stato possibile **ottimizzare il rendimento del Team**