Accelerare l’efficienza delle operazioni di sicurezza nel Security Fabric con una risposta rapida

Sommario

Panoramica preliminare 3

Introduzione all'automazione della sicurezza nel Security Fabric 4

Livello 1: raggiungere la visibilità sfruttando le analisi del Security Fabric 5

Livello 2: migliorare la visibilità multivendor con SIEM 5

Livello 3: integrare la risposta automatica con SOAR 6

Sfruttare il modello di automazione del SOC per affrontare in modo intelligente la complessità del SOC 8

Panoramica preliminare

Solo nel 2019, sono stati spesi oltre 124 miliardi di dollari per la sicurezza informatica;[1] tuttavia, i team di sicurezza di molte organizzazioni faticano a tenere il passo. Le problematiche includono un numero eccessivo di console, il sovraccarico di avvisi, la dipendenza da processi manuali e la carenza di personale di sicurezza informatica.

Il modello di maturità del SOC (Security Operations Center) è progettato per aiutare i team di sicurezza a identificare le capacità del Fortinet Security Fabric sulla base degli investimenti esistenti in termini di persone e processi nei loro team SOC; quindi, guidando le imprese con le soluzioni necessarie per risolvere le problematiche affrontate dalle organizzazioni ad ogni livello di maturità.

Le soluzioni Fortinet, come FortiAnalyzer (analisi e automazione del Security Fabric), FortiSIEM (gestione delle informazioni di sicurezza e degli eventi) e FortiSOAR (orchestrazione, automazione e risposta della sicurezza), sfruttano l'automazione della sicurezza per risolvere le principali problematiche affrontate dagli architetti della sicurezza e far progredire l'automazione del SOC. Il Security Fabric collega tutte queste soluzioni, consentendo ai team di sicurezza di aumentare al massimo la propria capacità di proteggere l'impresa.

Introduzione all’automazione della sicurezza nel Security Fabric

La complessità operativa è una sfida per i team di sicurezza di qualsiasi dimensione. Il modello di automazione del SOC aiuta il team di sicurezza di un’organizzazione a identificare l’attuale livello di maturità e a scegliere le soluzioni di sicurezza Fortinet più appropriate per l’ambiente.

Il modello di automazione del SOC è suddiviso in tre aree principali: persone, processo e prodotto. All’interno di ciascuna area, un’organizzazione può essere classificata a un livello di maturità 1–3 in base alla sua posizione di sicurezza in quell’area. Ad esempio, un’organizzazione valutata con un livello 1 in tutte le categorie ha un piccolo team IT senza personale di sicurezza (persone), playbook di risposta agli incidenti “best-effort” (processo) e nessuna soluzione di sicurezza dedicata (prodotto). All’altro estremo, un’organizzazione può avere un grande team di sicurezza con analisti SOC esperti, playbook ben definiti e aver distribuito e misurato l’efficacia delle proprie soluzioni SIEM e SOAR.

Con un deficit di competenze in materia di sicurezza informatica di oltre 4 milioni di persone, una tendenza che è destinata ad aumentare,[2] migliorare la componente “persone” dell’automazione del SOC di un’organizzazione può essere impossibile. Tuttavia, implementando i processi corretti e selezionando i prodotti giusti, è possibile compensare un team di sicurezza sottodimensionato.

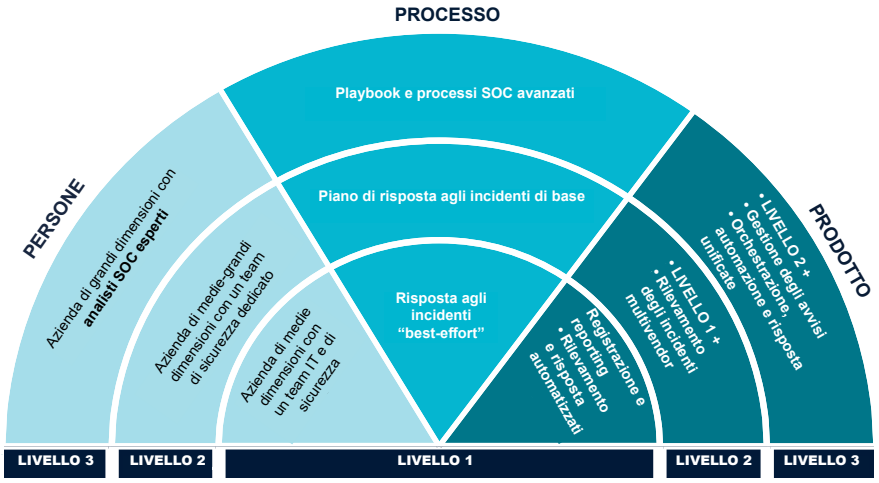


Figura 1: modello di automazione del SOC.

Livello 1: raggiungere la visibilità sfruttando le analisi del Security Fabric

Al livello 1 del modello di automazione del SOC, un team di sicurezza non dispone di personale di sicurezza dedicato o di processi per affrontare potenziali incidenti. Inoltre, l'impresa media riceve oltre 10.000 avvisi al giorno,[3] il che significa che gli analisti SOC hanno un sovraccarico di lavoro, con poco tempo per identificare e porre rimedio alle reali minacce alla rete.

Senza soluzioni dedicate, il team di sicurezza di un'organizzazione non ha visibilità sulle potenziali minacce alla propria rete. Tutti i dati dei registri devono essere raccolti manualmente e correlati prima che l'analisi possa essere eseguita. Molti SOC di livello 1 non sono dotati delle conoscenze o delle risorse necessarie per identificare le reali minacce, lasciando l'organizzazione a rischio.

FortiAnalyzer è una soluzione facile da implementare che consente di centralizzare la visibilità e il rilevamento delle minacce nell'intero Fortinet Security Fabric di un'organizzazione, incluse le distribuzioni sia on-premise che nel cloud. FortiAnalyzer mette in relazione i dati dei registri provenienti da più dispositivi Fortinet, fornendo un contesto prezioso agli analisti della sicurezza. Analizzando questi dati utilizzando il machine learning (ML) e gli IOC (Indicator of Compromise) forniti tramite un feed globale di threat intelligence, FortiAnalyzer può aiutare anche il più piccolo team di sicurezza a individuare e rispondere rapidamente alle minacce all'interno della propria rete.

Livello 2: migliorare la visibilità multivendor con SIEM

L'impresa media dispone di 75 diverse soluzioni di sicurezza specifiche distribuite nella propria rete.[4] Sebbene ciascuna di queste fornisca informazioni preziose sulle potenziali minacce alla rete dell'organizzazione, spesso non hanno il contesto necessario per distinguere tra una vera minaccia e un falso positivo. Inoltre, una serie di soluzioni di sicurezza standalone rende difficile applicare policy di sicurezza coerenti e garantire la conformità con le nuove e rigorose normative in materia di protezione dei dati, come il Regolamento generale sulla protezione dei dati (RGPD) dell'Unione Europea o il California Consumer Privacy Act (CCPA).

Un sistema SIEM è la soluzione logica alla complessità della sicurezza causata da un ambiente multivendor. Una soluzione SIEM raccoglie i dati recuperati da prodotti creati da diversi fornitori ed esegue correlazioni e analisi automatizzate per fornire un quadro più chiaro dello stato complessivo dell'ambiente protetto.

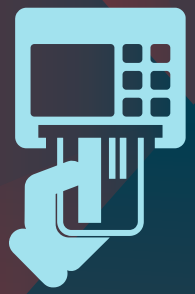
FortiSIEM consente ai team di sicurezza di mappare le operazioni secondo le best practice e gli standard di sicurezza del settore, come quelli pubblicati dal National Institute of Standards and Technology (NIST) e dal Center for Internet Security (CIS). In questo modo, FortiSIEM amplia la visibilità che FortiAnalyzer garantisce al Fortinet Security Fabric.

Livello 3: integrare la risposta automatica con SOAR

Il panorama delle minacce informatiche è in continua evoluzione, poiché i criminali informatici si affidano sempre più all'automazione per accelerare i loro attacchi. Sebbene la visibilità di una singola console di gestione aumenti la velocità con cui un team di sicurezza può identificare una potenziale minaccia, l'adozione di processi di risposta manuali agli incidenti presuppone che i difensori saranno sempre un passo indietro rispetto agli aggressori.

Le soluzioni SOAR consentono al team di sicurezza di un'organizzazione di sfruttare l'automazione per accelerare la risposta agli incidenti. Creando un framework automatizzato per unire l'intera architettura di sicurezza di un'organizzazione, è possibile intraprendere azioni difensive in contemporanea da più sistemi eterogenei, riducendo al minimo il cambio di contesto richiesto al personale di sicurezza, diminuendo l'eccessivo numero di avvisi e velocizzando la risposta agli incidenti.

FortiSOAR consente inoltre di ottimizzare i processi di sicurezza grazie a playbook di sicurezza ben definiti. Automatizzando le attività ripetitive e le risposte alle minacce comuni, FortiSOAR consente ai team di sicurezza di concentrare i propri sforzi e le limitate risorse su attività di livello superiore.



L’automazione può ridurre i tempi di risposta, passando da giorni a minuti.

Sfruttare il modello di automazione del SOC per affrontare in modo intelligente la complessità del SOC

Il panorama delle minacce alla sicurezza informatica sta diventando sempre più affollato, eppure molte organizzazioni devono far fronte a una carenza di risorse adeguate e di personale qualificato. La difesa contro le crescenti minacce informatiche richiede soluzioni di sicurezza che allevino il carico di lavoro dei team SOC sovraccarichi e sottodimensionati.

Il modello di automazione del SOC aiuta gli architetti della sicurezza a identificare l'attuale livello di maturità e i passi che devono compiere per raggiungere il livello successivo. Le soluzioni Fortinet, ad esempio FortiAnalyzer, FortiSIEM e FortiSOAR, sono progettate per aiutare a compiere questa transizione.

Sfruttando l'automazione intelligente della sicurezza, questi strumenti riducono il tempo medio di rilevamento (MTTD, Mean Time To Detection) e il tempo medio di risposta (MTTR, Mean Time To Response), diminuendo l'esposizione di un'organizzazione alle minacce informatiche.

In un anno in 65 paesi:[5]

- **2.216 violazioni di dati segnalate**
- **53.000 incidenti di sicurezza informatica segnalati**

[1] Lawrence Pingree, et al., "Forecast: Information Security and Risk Management, Worldwide, 2017-2023, 3Q19 Update", Gartner, 3 ottobre 2019.

[2] "(ISC)² Finds the Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap and Better Defend Organizations Worldwide", (ISC)², 6 novembre 2019.

[3] "How Many Daily Cybersecurity Alerts does the SOC Really Receive?", Bricata, 2 ottobre 2019.

[4] Kacy Zurkus, "Defense in depth: Stop spending, start consolidating", CSO, 14 marzo 2016.

[5] Gil Press, "60 Cybersecurity Predictions For 2019", Forbes, 3 dicembre 2018.

www.fortinet.com

616492-0-0-IT

settembre 22, 2020 8:36 AM