kaspersky BRING ON THE FUTURE

Confronto tra XDR, SIEM e SOAR

Troppi acronimi vi fanno girare la testa? Scopriamo cosa si nasconde dietro queste lettere...

Introduzione

SIEM, SOAR, MDR, EDR, EPP, XDR... vi sentite persi in una giungla di acronimi di cybersecurity? È comprensibile. Ecco perché abbiamo preparato questa guida, utile per capire le differenze fra i tre sistemi principali: SIEM, SOAR e XDR. Cosa si cela dietro questi acronimi? Perché a livello di settore sono stati sviluppati questi termini confusi e sovrapposti? Hanno un significato specifico o sono solo espedienti di marketing? Quali sono le somiglianze e le differenze? Possono completarsi a vicenda o sono in competizione tra loro?

Unitevi a noi in questa ricerca! Attraversiamo la foresta degli acronimi e del gergo tecnico per raggiungere una radura dove tutto sarà più chiaro.

SIEM

SIEM (Security Information and Event Management) è un set di strumenti e servizi che combinano la gestione degli eventi di sicurezza (SEM) e la gestione delle informazioni di sicurezza (SIM) in un'unica piattaforma. Il sistema SIEM raccoglie, aggrega, analizza e archivia i dati dei log dell'intera infrastruttura IT per le specifiche esigenze di vari casi d'uso (come governance/conformità e correlation matching basato su regole per il rilevamento delle attività sospette).

Come funziona il SIEM?

I primi servizi SIEM sono stati sviluppati nel lontano 2005, con lo scopo originale di aggregare e archiviare log ed eventi provenienti dall'intera infrastruttura IT di un'organizzazione, inclusi endpoint, applicazioni e dispositivi di rete, per scopi di reporting di conformità. Il SIEM esegue correlazioni su questo set di dati, cercando eventuali modelli o eventi che potrebbero indicare comportamenti sospetti, quindi genera un avviso per il SOC. Gli analisti della sicurezza hanno presto visto la possibilità di utilizzare questi avvisi non solo per scopi di conformità e governance, ma anche per identificare e arrestare in modo più proattivo l'avanzamento di qualsiasi attività dannosa nell'ecosistema.

Limiti del SIEM

Il problema era che i servizi SIEM non erano progettati con lo scopo specifico di rilevare e rispondere agli incidenti. Ciò rendeva piuttosto difficile lavorare con loro, per una serie di motivi:

- Troppi avvisi: l'enorme set di dati fornito dal SIEM deve essere filtrato, elaborato e analizzato manualmente, cosa non facile per gli analisti della sicurezza che cercano di prevenire gli attacchi in un panorama di minacce molto dinamico.

- Nessun contesto: per gestire attacchi nuovi, complessi e sofisticati, gli analisti della sicurezza necessitano di un quadro contestualizzato e coerente del panorama delle minacce per l'organizzazione, anziché dei flussi di dati disconnessi forniti dal SIEM.

- Troppo passivo: il blocco dei processi sospetti, lo spostamento dei file in quarantena e altre funzionalità di risposta non rientrano nel suo mandato. È fondamentalmente uno strumento passivo e analitico.

I professionisti della sicurezza hanno tentato di risolvere questi problemi sovrapponendo strumenti aggiuntivi al SIEM o sviluppando soluzioni di nuova generazione con plug-in di machine learning e analisi del comportamento. Tuttavia, rimane l'esigenza di uno strumento che fornisca avvisi di migliore qualità e strutture più rapide e automatizzate.

SOAR

Gli strumenti SOAR (Security Orchestration & Automated Response) sono emersi nel 2015 per risolvere alcuni dei problemi menzionati in precedenza nei sistemi SIEM. Le piattaforme SOAR acquisiscono dati da una varietà di fonti nell'infrastruttura, inclusi sistemi di gestione e piattaforme di threat intelligence, e forniscono analisi delle priorità. I team di sicurezza possono quindi configurare risposte automatizzate multi-fase e multi-soluzione alle minacce in arrivo, utilizzando l'integrazione della piattaforma SOAR di un ecosistema di strumenti di sicurezza connesso tramite API.

Come funziona la piattaforma SOAR?

Questa volta il nome è realmente utile! Ecco perché:
Gli strumenti SOAR consentono l'automazione. Sebbene siano noti soprattutto per la loro capacità di automatizzare i processi di risposta agli incidenti, questi strumenti possono in realtà automatizzare un'ampia gamma di flussi di lavoro, tra cui la scansione delle vulnerabilità, l'analisi dei log, la gestione degli accessi degli utenti, la classificazione delle minacce e altro ancora.

Lo fanno utilizzando "playbook": set di regole preconfigurate attivate da eventi specifici, che indicano al sistema quali passaggi devono essere eseguiti successivamente in uno specifico flusso di lavoro. La maggior parte delle soluzioni SOAR è dotata di centinaia di playbook pronti all'uso, che coprono le attività più comuni affrontate dai team SOC. I team possono quindi configurare i propri playbook per automatizzare altri processi ripetitivi più particolari.

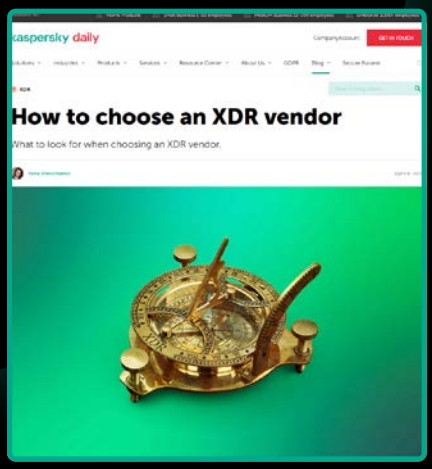
In secondo luogo, eseguono l'orchestrazione. Mentre l'automazione si riferisce all'esecuzione automatizzata di specifiche attività all'interno di un singolo flusso di lavoro, per orchestrazione si intende il coordinamento di più strumenti e processi in un flusso di lavoro più ampio, raccogliendo tutti i dati rilevanti in un'unica piattaforma per informazioni consolidate e utilizzabili.

Il rapporto tra SIEM e SOAR

In genere, un SIEM viene utilizzato insieme agli strumenti SOAR in una relazione simile a quella tra assistente e manager: il SIEM raccoglie tutti i log, li correla per trovare gli avvisi e fornisce queste informazioni al SOAR, che può quindi gestire le azioni di risposta.

Come scegliere un fornitore XDR?

Molti fornitori di cybersecurity sono saltati sul carro dell'XDR con le proprie soluzioni. Come potete capire se state utilizzando un prodotto adeguato? Consultate la nostra guida: https://www.kaspersky.com/blog/choosing-xdr-vendor/44063/



Limiti del SOAR

Sembra tutto fantastico, vero? Il fatto è che mantenere una piattaforma SOAR ben configurata che si integra con gli strumenti dei partner richiede l'impegno continuo di un SOC maturo e altamente qualificato, una risorsa di cui molte organizzazioni attualmente non dispongono, dato l'attuale gap di competenze in materia di cybersecurity.
Senza una manutenzione così qualificata e attenta, gli analisti SOAR possono ritrovarsi con troppi avvisi a bassa priorità, falsi positivi e un set di dati generalmente incoerente come risultato di tutti i vari strumenti isolati che forniscono dati alla piattaforma: esattamente quello che stavano cercando di evitare.

XDR

XDR è una soluzione di sicurezza on-premises o basata su cloud, che rientra in due ampie categorie: nativo e ibrido. XDR nativo è una suite unificata di strumenti di un unico fornitore, mentre XDR ibrido integra altre soluzioni di terze parti nell'ecosistema del cliente. Il termine "XDR" è stato utilizzato per la prima volta nel 2018. La "X" sta per "eXtended": XDR "si estende" oltre i tradizionali strumenti di rilevamento, risposta e protezione degli endpoint (EDR ed EPP) raccogliendo e correlando dati da più livelli di sicurezza, tra cui e-mail, cloud e rete, per fornire una protezione completa per l'intera infrastruttura IT.

Quindi, è un'unica piattaforma che coordina una gamma di strumenti e utilizza il machine learning e l'automazione per aiutare i team di sicurezza a proteggere l'intero ecosistema di sicurezza. Sembra simile a SOAR, no? Ma ci sono alcune differenze fondamentali. Diamo un'occhiata...

Confronto tra XDR e SOAR: qual è la differenza?

1. Le soluzioni XDR sono incentrate sui dati e sull'ottimizzazione degli endpoint: ciò significa che il rilevamento e la risposta agli incidenti sono una caratteristica di progettazione centrale, che offre loro capacità di analisi avanzate che gli strumenti SOAR in genere non hanno. Gli strumenti XDR sono eccellenti per rilevare minacce sconosciute e zero-day, sfruttando l'intelligenza artificiale, algoritmi di machine learning e la threat intelligence per proteggere un'organizzazione oltre i suoi confini. D'altra parte, gli strumenti SOAR possono offrire una varietà molto più ampia di casi d'uso, poiché possono orchestrare e automatizzare qualsiasi processo nell'infrastruttura, non solo la risposta agli incidenti.

2. XDR può essere considerato qualcosa di simile a una versione "light" di SOAR: un'interfaccia semplificata che offre risposte automatizzate con un solo clic alle minacce e agli avvisi in arrivo. Questo può essere molto più pratico per un'organizzazione che non dispone delle risorse per mantenere la complessità di una piattaforma SOAR ben configurata.

3. XDR consente un'integrazione fluida tra i prodotti: sia attraverso lo stack di strumenti di un singolo fornitore che tramite prodotti di terze parti, XDR eccelle in termini di interoperabilità senza soluzione di continuità. Gli strumenti SOAR spesso hanno difficoltà nell'integrare tutti gli strumenti eterogenei e isolati nel loro stack. XDR abbatte questi silos per garantire una risposta alle minacce efficiente e completa.

L'XDR sostituirà il SIEM e il SOAR?

Su questo aspetto il giudizio è ancora aperto, poiché XDR è una tecnologia relativamente nuova che viene continuamente sviluppata. Attualmente, la maggior parte degli esperti consiglia un approccio integrato, poiché ciascuna soluzione offre vantaggi complementari alle altre:

- SIEM: il SIEM presenta casi d'uso che vanno al di là del rilevamento delle minacce, come la gestione dei log, la conformità e l'analisi dei dati non correlati alle minacce.
- SOAR: l'ampia possibilità di personalizzazione dei playbook SOAR è utile per orchestrare e automatizzare i processi nell'infrastruttura dell'organizzazione.
- XDR: quando si tratta di rilevare e rispondere alle minacce, l'analisi avanzata di una soluzione XDR offre una protezione superiore che non è seconda a nessuno.

Cercate una soluzione collaudata e adattabile per i vostri esperti?

Kaspersky Expert Security, un sistema XDR basato su una soluzione EDR cloud-native, assicura alla vostra organizzazione una visibilità e funzionalità migliorate per il rilevamento basato sull'intelligenza artificiale e la logica di risposta automatica per tutti gli endpoint e la rete, facilitando un'ampia gamma di scenari di risposta automatizzata agli incidenti. La tecnologia avanzata integrata nella piattaforma per il rilevamento e l'analisi è completata da una threat intelligence leader di livello superiore. L'architettura unificata di Kaspersky XDR consente una gestione centralizzata da un'unica console Web. Per ulteriori informazioni, visitate la pagina go.kaspersky.com/expert.

www.kaspersky.it