kaspersky BRING ON THE FUTURE

Comparación entre XDR, SIEM y SOAR

¿Muchas siglas le generan confusión? Averigüemos qué se oculta detrás de estas letras.

Introducción

SIEM, SOAR, MDR, EDR, EPP, XDR... ¿Siente desconcierto y no comprende todas estas siglas de ciberseguridad? Es lógico, y por eso elaboramos esta guía útil para determinar las diferencias entre tres de las principales siglas: SIEM, SOAR y XDR. ¿Cuál es la historia detrás de estas siglas? ¿Cómo es que la industria desarrolló estos términos confusos y superpuestos? ¿Significan algo distinto o solo son trucos de marketing? ¿Cuáles son sus similitudes y diferencias? ¿Pueden complementarse o compiten entre sí?

Acompáñenos en esta búsqueda. Revivamos nuestro conocimiento e investiguemos estas siglas y la jerga, para comprender con claridad qué significa cada una.

SIEM

La Seguridad Informática y Administración de Eventos, también conocida como SIEM, es un conjunto de herramientas y servicios que combina la administración de eventos de seguridad (SEM) Y la administración de seguridad informática (SIM) en una sola plataforma. SIEM recopila, agrega, analiza y almacena los datos de registro de toda la infraestructura de TI para diversos casos de uso, como el control y cumplimiento normativo, así como la detección y correlación basadas en reglas de actividad sospechosa.

¿Cómo funciona SIEM?

Los primeros servicios de SIEM se desarrollaron en 2005 con el propósito original de agregar y almacenar registros y eventos de toda la infraestructura de TI de una organización, incluyendo endpoints, aplicaciones y dispositivos de red, para generar informes de cumplimiento. El sistema SIEM ejecuta correlaciones en este conjunto de datos, busca cualquier patrón o evento que pueda indicar un comportamiento sospechoso y genera una alerta para el centro de operaciones de seguridad (SOC). Los analistas de seguridad no tardaron en ver la posibilidad de usar estas alertas no solo para fines de cumplimiento y control, sino también para identificar y detener de forma más proactiva el desarrollo de cualquier actividad maliciosa en el ecosistema.

Limitaciones de SIEM

El problema era que los servicios de SIEM no se diseñaron para el propósito específico de detectar incidentes y responder ante ellos. Esto dificultó el trabajo con estos servicios por varias razones:

- Demasiadas alertas: El enorme conjunto de datos que brinda el sistema SIEM tiene que filtrarse, procesarse y analizarse manualmente, lo que no es conveniente para los analistas de seguridad que intentan prevenir los ataques en un panorama de amenazas en constante evolución.

- Sin contexto: Para hacer frente a los ataques nuevos, complejos y sofisticados, los analistas de seguridad necesitan una imagen contextualizada y coherente del panorama de amenazas de la organización, en lugar de los flujos de datos desconectados que brinda el sistema SIEM.

- Demasiado pasivo: El bloqueo de procesos sospechosos, la puesta en cuarentena de archivos y otras capacidades de respuesta no están dentro de sus competencias. Es básicamente una herramienta pasiva y analítica.

Los profesionales de la seguridad intentaron resolver estos problemas superponiendo herramientas adicionales a la SIEM o desarrollando nuevas generaciones con complementos de aprendizaje automático y análisis del comportamiento. Sin embargo, la demanda por una herramienta que ofrezca alertas de mejor calidad y facilite procesos más rápidos y automatizados persistió.

SOAR

Las herramientas de organización de seguridad y respuesta automatizada (SOAR) surgieron en 2015 para resolver algunas de las fallas mencionadas anteriormente en los sistemas SIEM. Las plataformas SOAR reciben datos de diversas fuentes en toda la infraestructura, incluidos los sistemas de administración y las plataformas de inteligencia de amenazas, y brindan un análisis prioritario. Luego, los equipos de seguridad pueden configurar respuestas automatizadas de varias etapas y soluciones ante amenazas entrantes gracias a la integración de la plataforma SOAR con ecosistemas de seguridad conectados a través de API.

¿Cómo funciona SOAR?

Esta vez, el nombre es bastante útil. A continuación, le explicamos los motivos:

Las herramientas SOAR automatizan. Aunque suelen ser más conocidas por su capacidad para optimizar los procesos de respuesta ante incidentes, estas herramientas pueden en realidad simplificar una amplia gama de flujos de trabajo, como el análisis de vulnerabilidades, el análisis de registros, la administración del acceso de los usuarios, la evaluación de amenazas y mucho más.
Para ello, usan "manuales" o conjuntos de reglas preconfiguradas que se activan a partir de eventos específicos y que indican al sistema los pasos que deben seguir en un flujo de trabajo concreto. La mayoría de las soluciones SOAR vienen con cientos de manuales listos para usar, que abarcan las tareas más comunes a las que se enfrentan los equipos del SOC. De este modo, los equipos pueden configurar sus propios manuales para automatizar otros procesos repetitivos más particulares que puedan tener.

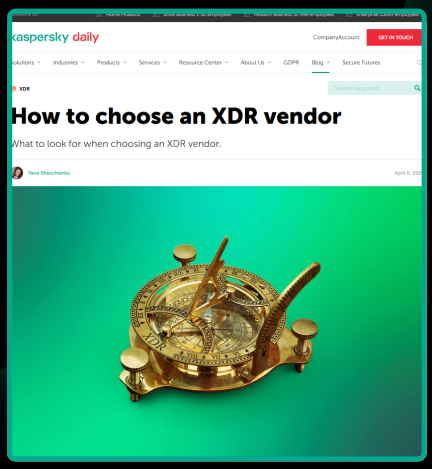
Después de esto, organizan. Mientras que la automatización hace referencia a la ejecución automática de tareas individuales dentro de un único flujo de trabajo, la organización hace referencia a la coordinación de diversas herramientas y procesos dispares en un flujo de trabajo más amplio, que recopila todos los datos relevantes en una única plataforma para obtener información útil y coherente.

La relación entre SIEM y SOAR

Por lo general, un sistema SIEM se usa junto con las herramientas SOAR en algo parecido a una relación de asistente y gerente: el sistema SIEM recopila todos los registros, los correlaciona para encontrar alertas y luego envía esta información a las herramientas SOAR, que a su vez pueden llevar a cabo las acciones de respuesta.

¿Cómo elegir un proveedor de XDR?

Muchos proveedores de ciberseguridad se sumaron a la tendencia de XDR con sus propias soluciones. ¿Cómo puede saber si está recibiendo un producto aceptable? Consulte nuestra guía útil: https://latam.kaspersky.com/blog/choosing-xdr-vendor/24646/



Limitaciones de SOAR

Todo suena muy bien, ¿no? La cuestión es que el mantenimiento de una plataforma SOAR bien configurada que se integre con las herramientas de los socios requiere el esfuerzo continuo de un SOC altamente capacitado y experimentado. Lamentablemente, es un recurso con el que muchas organizaciones no cuentan en el momento debido a la actual brecha de habilidades en materia de ciberseguridad.
Sin este mantenimiento especializado y minucioso, los analistas de SOAR pueden terminar con demasiadas alertas de baja prioridad, falsos positivos y un conjunto de datos generalmente incoherente como resultado de todas las diferentes herramientas aisladas que integran la plataforma. Justamente, lo que intentaban evitar.

XDR

XDR es una solución de seguridad que puede ser implementada localmente o en la nube y se divide en dos grandes categorías: nativa e híbrida. La solución XDR nativa consiste en un conjunto unificado de herramientas de un solo proveedor, mientras que la XDR híbrida integra otras soluciones de terceros en su ecosistema. El término 'XDR' se utilizó por primera vez en 2018, donde la "X" inicial representa la palabra 'eXtendido', sugiriendo desde el principio que esta herramienta iría más allá de las funciones tradicionales, como detectar, responder y proteger los endpoints (EDR y EPP). De hecho, esta solución permite recopilar y correlacionar datos de varias capas de seguridad, como el correo electrónico, la nube y la red, para ofrecer una protección integral en toda la infraestructura de TI.

Por lo tanto, se trata de una sola plataforma que coordina una serie de herramientas y usa el aprendizaje automático y la automatización para permitir que los equipos de seguridad protejan todo el ecosistema de seguridad. Suena como SOAR, ¿no le parece? Sin embargo, existen algunas diferencias fundamentales. Echemos un vistazo.

Comparación entre XDR y SOAR: ¿Cuál es la diferencia?

1. Las soluciones de XDR dependen de los datos y la optimización de los endpoints, lo que significa que la detección de incidentes y la respuesta ante estos es una función central del diseño, lo que les permite tener capacidades de análisis avanzadas que las herramientas de SOAR no suelen tener. Las herramientas de XDR son expertas en la detección de amenazas desconocidas y de día cero. De hecho, aprovechan la inteligencia artificial, los algoritmos de aprendizaje automático y la inteligencia de amenazas para proteger una organización más allá de sus límites. Por otro lado, las herramientas de SOAR pueden ofrecer una variedad mucho más amplia de casos de uso, ya que pueden organizar y automatizar cualquier proceso en toda la infraestructura, no solo la respuesta ante incidentes.

2. XDR puede considerarse algo así como un SOAR lite: una interfaz optimizada que ofrece respuestas automatizadas con un solo clic ante las amenazas y alertas entrantes. Esto puede ser mucho más conveniente para una organización que no tiene los recursos para mantener la complejidad de una plataforma SOAR bien configurada.

3. XDR permite una integración fluida entre diferentes productos, tanto si se trata de una pila de herramientas de un solo proveedor como de productos de terceros; es decir que XDR se caracteriza por una interoperabilidad sin interrupciones. Por otro lado, las herramientas SOAR a menudo se enfrentan a una difícil tarea al tratar de integrar todas las herramientas dispares y aisladas en su pila. En cambio, XDR rompe estas barreras para obtener una respuesta eficaz y completa ante las amenazas.

Entonces, ¿XDR reemplazará a SIEM y SOAR?

El jurado aún no ha emitido su veredicto ya que XDR es una tecnología relativamente nueva que se desarrolla todo el tiempo. Hoy en día, la mayoría de los expertos recomiendan un enfoque integrado debido a que cada solución ofrece ventajas que complementan a las demás:

- SIEM: Tiene casos de uso más allá de la detección de amenazas, como la administración de registros, el cumplimiento y el análisis de datos no relacionados con amenazas.
- SOAR: Posee manuales útiles y personalizables que permiten organizar y automatizar procesos en toda la infraestructura de la organización.
- XDR: Ofrece análisis avanzados que proporcionan una protección mejorada e incomparable cuando se trata de detectar y responder ante amenazas.

¿Busca una solución comprobada y adaptable para sus expertos?
Kaspersky Expert Security, una solución XDR basada en EDR nativa de nube, proporciona a su organización una mejor visibilidad y funcionalidad en la detección de amenazas basándose en la inteligencia artificial (IA) y la lógica de respuestas automáticas de la red y en todos los endpoints, lo cual facilita una amplia gama de situaciones de respuesta automatizada a incidentes. La tecnología avanzada e integrada de la plataforma para la detección y el análisis se complementa con la inteligencia de amenazas líder en el mundo. La arquitectura unificada de Kaspersky XDR brinda una administración centralizada desde una única consola web. Para obtener más información, visite go.kaspersky.com/es_mx_expert.

latam.kaspersky.com