Presentado por

Detección y respuesta extendida (XDR)

para dummies®

Edición especial de Cisco

- Explora el valor de una plataforma de XDR
- Experimenta una mejor detección de amenazas
- Reduce la complejidad para tu equipo de seguridad

James Sullivan

Acerca de Cisco Secure

Como la empresa de ciberseguridad corporativa más grande del mundo, lideramos el camino con soluciones que impulsan la industria en SASE, XDR y confianza cero. La integración se realiza gracias a Cisco SecureX, nuestra plataforma de seguridad que brinda simplicidad, visibilidad y eficiencia en toda tu infraestructura de seguridad.

cisco.com/go/securex

El enfoque XDR de Cisco se basa en la experiencia integrada de la plataforma nativa de la nube de SecureX. Conectar tus productos de Cisco Security con el resto de tu infraestructura, brinda simplicidad, los unifica en una ubicación para mejor visibilidad, y maximiza la eficiencia operativa para proteger tu red, aplicativos, endpoints y la nube. Reduce significativamente el tiempo de permanencia y las tareas impulsadas por humanos para contrarrestar los ataques y cumplir con las normas.

 www.twitter.com/ciscosecure

 www.facebook.com/ciscosecure

 www.linkedin.com/showcase/cisco-secure/

Detección y respuesta extendida (XDR)

Edición especial de Cisco

por James Sullivan

para dummies®

Detección y respuesta extendida (XDR) para Dummies®, Edición especial de Cisco

Publicado por
John Wiley & Sons, Inc.
111 River St.,
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-394-15626-9 (pbk); ISBN 978-1-394-15627-6 (ebk)

Agradecimientos del editor

Algunas de las personas que ayudaron con la publicación de este libro incluyen:

Gerente del proyecto: Jennifer Bingham

Editora de adquisiciones: Ashley Coffey

Director editorial: Rev Mengle

Especialista de ajuste del contenido: Vivek Lakshmikanth

Introducción

La seguridad de TI es uno de los ámbitos que cambia con mayor velocidad en el mundo de la tecnología. Hay nuevas herramientas, técnicas y tipos de ataques que aparecen todo el tiempo. Una de estas nuevas herramientas es la detección y respuesta extendida (*Extended Detection and Response*, XDR). Las plataformas de XDR incluyen herramientas para orquestación, monitoreo y análisis, automatización, visualización y más. Lo que lo une todo es una visión centralizada de toda tu infraestructura de seguridad.

Los entornos de seguridad corporativa se han vuelto tan complejos que los recursos de seguridad en silos ya no son una opción viable. Los atacantes explotan múltiples puntos de ataque, la actividad comercial regular se identifica erróneamente con demasiada facilidad como maliciosa y los equipos de seguridad están llenos de amenazas legítimas.

Las soluciones de gestión de eventos e información de seguridad (*Security Information and Event Management*, SIEM) y de orquestación, automatización y respuesta de seguridad (*Security Orchestration Automation and Response*, SOAR) comparten algunas características con las herramientas de XDR, pero existen algunas diferencias clave. SIEM con frecuencia no puede organizar y procesar correctamente todos los registros y alertas que genera. SOAR, por otro lado, no tiene las capacidades de integración que tienen las herramientas de XDR. Sin embargo, estas dos herramientas aún tienen su lugar en el panorama de la seguridad.

Este libro analiza qué son exactamente las herramientas de XDR, cómo se relacionan con otras soluciones de seguridad, cómo pueden integrarse con esas soluciones y qué desafíos intentan resolver.

Acerca de este libro

Las herramientas de XDR son una nueva incorporación al mundo de la seguridad de TI, por lo que aún no muchas personas las comprenden por completo. ¡Por eso existe este libro! Las guías *para Dummies* son fáciles de leer y contienen información fácil de digerir, pero también brindan al lector el conocimiento que necesita para tomar decisiones, hacer que las cosas funcionen o simplemente aprender algo nuevo.

Tal vez quieras aprender sobre una parte específica de las herramientas de XDR. ¡No hay problema! Aunque cada capítulo tiene algo que agregar

sobre las herramientas de XDR o la seguridad de TI en general, puedes omitirlos. Cada sección de este libro es independiente y se puede comprender sin leer las secciones anteriores.

Si realmente deseas una versión resumida de este libro, consulta el Capítulo 6. Allí encontrarás diez de los puntos más importantes sobre las herramientas de XDR que se cubren en el resto del libro. ¡Es una excelente manera de comenzar con el contenido del libro, o simplemente aprender cosas sobre las herramientas de XDR!

Íconos utilizados en este libro

Mientras lees, puede encontrar algunos símbolos especiales. Los usamos para señalar información especial o proporcionar recordatorios sobre puntos importantes del capítulo. Estos son los íconos que encontrarás en este libro:

RECUERDA

Este ícono se utiliza para resaltar un punto crítico del capítulo. Puede ser algo específico sobre una herramienta de seguridad o un concepto general. Esta información probablemente aparezca más de una vez.

CONSEJO

Este ícono está destinado a agregar algo adicional a una sección. Podría desarrollar un punto o agregar algo que no corresponda a la sección principal. Los consejos suelen ser específicos y no referirse a conceptos generales.

Más allá de este libro

Si todavía tienes preguntas o si deseas obtener más información sobre las herramientas de XDR y la seguridad de TI, ingresa a `cisco.com/go/xdr` o `blogs.cisco.com/security` para ver lo que piensa la gente de Cisco sobre el estado de la seguridad de TI.

EN ESTE CAPÍTULO

- Cómo han evolucionado las amenazas de seguridad
- Herramientas y técnicas modernas de seguridad
- Desglose de XDR
- Cómo lo hace Cisco

Capítulo 1
Operaciones de seguridad: tendencias y desafíos

El panorama actual de la ciberseguridad es desalentador. Surgen nuevas amenazas y actores aparentemente a diario, desde las naciones-estado, el ciberespionaje, las configuraciones erróneas, las vulnerabilidades y más. Además, el mercado actual ofrece una amplia variedad de proveedores y herramientas, que en ocasiones resultan caóticas al intentar que los productos "interactúen correctamente entre sí".

Este capítulo examina algunas de las herramientas de seguridad más destacadas disponibles en la actualidad, las diferencias entre ellas y lo que aporta el nuevo producto: la detección y respuesta extendida (*Extended Detection and Response*, XDR). Pero, en primer lugar, presentaremos información sobre la evolución de las amenazas a la seguridad en los años recientes.

La evolución del panorama de las amenazas

Con respecto a los ataques cibernéticos, debemos considerar el *ransomware*, los puntos de vulnerabilidad y el *malware*, entre otros. La cantidad de amenazas a la seguridad crece tan rápido como su complejidad.

Estas son algunas de las principales amenazas:

- **Ransomware:** Sí, aún está presente. El *ransomware* es un ataque que bloquea la información objetivo y la retiene como rehén. El ataque reciente a Colonial Pipeline es un ejemplo de alto perfil del poder de esta amenaza.
- **Ataques a nivel de país, estado y gobierno:** Son los ataques cibernéticos que se originan de los actores estatales. Con los ataques a Sony y al Departamento del Tesoro de Estados Unidos, los ataques patrocinados por el estado siguen siendo una amenaza relevante.
- **Malware y otros virus:** Otra estrategia de ataque comprobada y verdadera, el *malware* es cualquier software creado para interferir o dañar los sistemas internos. Estas amenazas siguen aumentando en complejidad, pero con frecuencia llegan a través de métodos simples de entrega. Por ejemplo, cada vez se observan más correos electrónicos "urgentes" que anuncian actualizaciones falsas del sistema operativo Windows.
- **Ataques internos:** Son ataques realizados por miembros de tu propia organización. Si bien no se suele hablar sobre este tipo de amenaza, es igual de importante. Incluso después de una verificación previa al empleo, una persona con malas intenciones puede filtrarse dentro de una organización. Un ataque interno común es la filtración de la información confidencial o privilegiada para la compraventa de acciones.

Es fácil verse abrumado por las inquietudes sobre la ciberseguridad, pero es el costo que conlleva operar de forma digital. En definitiva, la seguridad se trata de mantener el control de tus recursos e infraestructura. Las partes externas con frecuencia intentarán penetrar en tu red, robar o destruir tus datos, y tal vez incluso comprometer el hardware. Son riesgos que debes asumir, y prepararse para ellos, mientras aprovechas los beneficios de trabajar en el espacio digital.

Herramientas y técnicas de seguridad

Al igual que las amenazas de seguridad que enfrentan las organizaciones, las técnicas de protección y la seguridad misma también están evolucionando. Ya no alcanza con "prenderle una vela al *firewall*" para proteger los datos del cliente y la integridad de la red. (Esto no significa que no hace falta tener un *firewall*, aún lo necesitas).

Fieles al estilo del sector tecnológico, hay palabras de moda, abreviaturas y siglas por todas partes en el espacio de las soluciones de seguridad. Este libro analiza tres tipos de soluciones de seguridad que se utilizan para mejorar la automatización y la detección de amenazas: Gestión de eventos e información de seguridad (Security Information and Event Management, SIEM), orquestación, automatización y respuesta de seguridad (Security Orchestration Automation and Response, SOAR), y detección y respuesta extendidas (Extended Detection and Response, XDR). En primer lugar, veamos el problema de los silos.

Soluciones en silos y sus limitaciones

La práctica común de colocar partes diferentes de una infraestructura digital en silos ofrece numerosos beneficios. Mantiene las cosas organizadas, permite que los desarrolladores y administradores se concentren en la información relevante para ellos y, a menudo, es la forma en que se deben usar las soluciones y herramientas. Sin embargo, surgen problemas cuando los diferentes sistemas tienen información relevante para la función de otros sistemas en silos.

Este problema se puede observar especialmente al tratar con las soluciones de seguridad. La seguridad de los endpoints recopila y procesa diferentes tipos de información que la seguridad de la red o la del correo electrónico. Sin embargo, todos estos sistemas se benefician significativamente con una visión integral.

RECUERDA

Recientemente, se han generado innovaciones y soluciones para superar las limitaciones de los silos en las soluciones de seguridad. Los dos tipos más destacados de soluciones en los últimos cinco años son SIEM y SOAR.

Intentos iniciales de integración: SIEM

La gestión de eventos e información de seguridad (SIEM) es una versión bastante exitosa y probada de las soluciones de gestión de registros y eventos. En su esencia, SIEM trata de recopilar la mayor cantidad posible de información de registros de toda una organización.

Numerosas soluciones de SIEM pueden tomar los datos de registro de las herramientas de seguridad de la Internet de las cosas (*Internet of Things*, IoT), registros de eventos de *firewall* y todos los eventos intermedios. Este tipo de solución comienza a derribar las paredes del silo, se integra con múltiples soluciones y centraliza la información de seguridad importante.

Lo que SIEM no hace es brindar a los ingenieros de seguridad una mejora en el tiempo y eficacia en la respuesta a las amenazas. Poder tener una

vista panorámica de la seguridad de tu organización es excelente para muchos fines, pero responder a las amenazas es igual de importante.

Intentos iniciales de respuesta frente a las amenazas: SOAR

La orquestación, automatización y respuesta de seguridad (SOAR) toma gran parte de lo que hace que SIEM sea excelente y agrega capas adicionales para cubrir algunas de las debilidades de la solución anterior. Al igual que SIEM, las soluciones de SOAR toman datos de diferentes partes de la infraestructura de seguridad y los colocan en un solo lugar, que es la parte de "orquestación".

Las automatizaciones entran en escena con la capacidad de poner en uso esta información recopilada. Varias soluciones de SOAR ofrecen opciones para automatizar diferentes tareas de auditoría, registro y escaneo. Sin embargo, la automatización no puede encargarse de todo y, a veces, debe intervenir un ser humano.

La parte de la "respuesta" de SOAR se trata de organizar y gestionar la respuesta a una amenaza de seguridad. Este conjunto de características utiliza información de orquestación y automatización para ayudar al personal de seguridad a tomar decisiones y responder a las amenazas.

RECUERDA

La automatización de SOAR no automatiza las respuestas a las violaciones de seguridad. Automatiza las tareas simples de análisis para reducir las cargas de trabajo del personal de seguridad.

¿Qué es XDR?

La detección y respuesta extendida (XDR) es un agregado reciente al conjunto de siglas que invaden el espacio de la tecnología corporativa. Toma una gran parte de lo que hace que SIEM y SOAR sean útiles, e intenta agregar un poco más a cada función de los tipos de soluciones más establecidos.

Los aspectos básicos de XDR

Si bien SIEM y SOAR hacen énfasis en los registros y el análisis (que termina en manos del personal de seguridad) las soluciones de XDR se enfocan en los endpoints. Ahí está la acción. Eso es lo que atacan las partes externas.

En esto, XDR comparte mucho con las herramientas de detección y respuesta de endpoints (*Endpoint Detection and Response*, EDR), pero hay

una razón por la que XDR no podría llamarse EDR. Lo que hace XDR es *ampliar* las capacidades de una solución EDR tradicional, además de profundizar las funciones de una solución de SIEM o SOAR. Por ejemplo, XDR amplía la visibilidad y las detecciones disponibles con una solución de EDR con datos y detecciones de la solución de detección y respuesta de red (*Network Detection and Response*, NDR).

La metodología aquí es que el tiempo entre el registro de un comportamiento sospechoso y su reconocimiento como ataque, la creación de un plan de respuesta y su ejecución debe ser lo más reducido posible. Para comprender mejor las soluciones de XDR, vamos a desglosar su contenido.

Componentes de una solución de XDR

Las herramientas de XDR son nuevos participantes en el espacio de seguridad, y todavía hay algunas variaciones en lo que ofrecen estas soluciones. Sin embargo, hay algunas funciones clave que ofrecen las soluciones de XDR:

- **Integración flexible:** La cantidad y el método de integración con las soluciones de seguridad existentes depende de la propia solución de XDR, pero a menudo hay una forma de incorporar herramientas de seguridad, especialmente seguridad de los endpoints, en una plataforma de XDR.
- **Vista centralizada:** Las herramientas de XDR no serían gran cosa sin una vista centralizada de la información que recopilan. Estas examinan la mayor parte del entorno de seguridad, si no todo, y es necesario un *hub* central para analizar toda esa información.
- **Aprendizaje automático:** Las plataformas de XDR ofrecen análisis de datos de seguridad basados en el aprendizaje automático. Esto es especialmente útil para reducir los tiempos de respuesta, porque el personal de seguridad tiene menos trabajo que hacer antes de resolver un problema de seguridad.
- **Automatización:** Al igual que las soluciones SOAR, las herramientas de XDR utilizan la automatización para reducir las cargas de trabajo de Operaciones de Seguridad. Solo automatizan las tareas simples, pero todo ayuda.

En función del proveedor, puede haber accesorios adicionales conectados a una plataforma de XDR, pero estos puntos deberían ser la base de cada solución de XDR.

¿Por qué son importantes las herramientas de XDR?

SIEM, SOAR, NDR y EDR son útiles a su manera. Las herramientas de XDR son una nueva incorporación al mercado de soluciones de seguridad, por lo que deben aportar algo que no se pueda encontrar en ningún otro lugar. El beneficio real de esta nueva opción no son solo las nuevas funciones que trae, sino también cómo estas funciones responden al panorama de seguridad actual.

Nuevos desafíos de seguridad

Los ataques cibernéticos son cada vez más sofisticados, y no solo en la forma en que se cometen. El "lugar" también está cambiando. Con la IoT y la continua expansión a la nube, las redes son más numerosas y la cantidad de endpoints crece rápidamente, y las partes externas malvadas están al tanto.

Ahora, los ataques pueden llegar a múltiples redes y endpoints a la vez. Se producen ataques de múltiples frentes que necesitan nuevos tipos de seguridad de TI. Las soluciones de SIEM y SOAR simplemente no están diseñadas para procesar y administrar este tipo de ataques. Las herramientas de EDR y NDR tienen una mayor capacidad para manejarlos, pero no cuentan con el soporte de gestión necesario para responder rápidamente a las amenazas sofisticadas.

Diferentes fuentes de información

No solo los tipos de ataques son cada vez más sofisticados, sino que también lo son los entornos de TI donde trabajan las organizaciones. Todos los días se agregan nuevos sitios potenciales de ataque. La IoT, los aplicativos en la nube y el uso de bases de datos crecen rápidamente. La necesidad de trabajar desde casa es una preocupación especial en este momento. Este estilo de operar se extiende y aumenta la cantidad de dispositivos que tienen acceso a los recursos internos.

Estos son algunos de los desafíos que presenta el trabajo desde casa:

- La cantidad de dispositivos que necesitan protección ha aumentado, lo que significa más puntos de ataque para la explotación de terceros.
- La variedad de dispositivos de los empleados ha aumentado. Muchas organizaciones ya no utilizan únicamente las "computadoras del trabajo". Esto puede requerir un conjunto igualmente diverso de soluciones de seguridad.

» Las redes domésticas rara vez son tan seguras como las redes de la oficina. La mayoría de los empleados de una organización no son expertos en seguridad y no pueden garantizar una conexión de red segura y constante.

Todo esto se suma a un ecosistema complejo que requiere un conjunto complejo de soluciones de seguridad. Por este motivo, se hace obvio el deseo de colocar estas herramientas de seguridad y fuentes de información en silos. Las soluciones de XDR son importantes porque permiten que las organizaciones tengan herramientas de seguridad dispares en su entorno, sin que las operaciones de protección se ralenticen.

Personal de seguridad sobrecargado

Los profesionales de seguridad de TI están altamente capacitados y bien informados, pero lo que una persona puede hacer tiene un límite. La complejidad y amplitud de los ecosistemas de seguridad modernos a menudo lleva a que los ingenieros encargados trabajen demasiado, lo que, a su vez, conduce a errores en las operaciones de seguridad.

Las soluciones de SIEM y SOAR, si bien son útiles en el contexto adecuado, a menudo conducen a una sobrecarga de información debido a su naturaleza de "recopilar todo". SIEM es conocido por convertirse en una nueva forma de crear una gran cantidad de registros, sin herramientas para manejarlos. La cantidad y diversidad de información que generan las herramientas de seguridad es demasiado para que un ser humano la gestione sin la ayuda de una máquina.

CONSEJO

Puede parecer que somos demasiado negativos en cuanto a las soluciones de SIEM; sin embargo, es importante señalar que estas soluciones son muy útiles para las industrias que exigen un alto grado de cumplimiento donde las pilas registros son exactamente lo que necesitas.

Que el personal de seguridad esté sobrecargado y con exceso de trabajo es una garantía de que sucedan dos cosas: violaciones de seguridad y empleados descontentos. Es verdaderamente una situación en la que todos pierden. La forma en que las soluciones de XDR se enfocan en la seguridad de los endpoints y la automatización de tareas significa una carga de trabajo reducida para los profesionales de la seguridad.

Objetivo principal: reducir MTTD y MTTR

Reducir el tiempo medio de detección (*Mean Time To Detect*, MTTD) y el tiempo medio de respuesta (*Mean Time To Respond*, MTTR) son los objetivos de cualquier equipo de operaciones de seguridad. En realidad, son la razón por la que existen los equipos de seguridad de TI en primer lugar.

Los MTTD y MTTR son exactamente lo que su nombre indica: ¿Cuánto tiempo se necesita por lo general para encontrar y solucionar un problema de seguridad? La necesidad de filtrar alertas y registros para encontrar problemas de seguridad reales aumenta el tiempo de detección, mientras que la falta de herramientas de automatización y análisis aumenta el tiempo de respuesta.

Las soluciones de XDR son la entrada más reciente al panorama de la seguridad que intenta disminuir tanto el MTTR como el MTTD. La recopilación, el análisis, la automatización y la centralización (todas las facetas clave de las soluciones de XDR) ayudan a acelerar los tiempos de detección y respuesta. Al fin y al cabo, ¿no es eso exactamente lo que debería hacer una solución de seguridad?

El enfoque de Cisco Secure

El enfoque XDR de Cisco Secure se basa en una experiencia de plataforma integrada. Las soluciones de XDR se ocupan de la organización y el control, por lo que Cisco Secure ha desglosado lo que considera los componentes clave de cualquier solución exitosa de detección y respuesta extendida:

- **X:** La plataforma debe cubrir tantos puntos de control y fuentes de datos como sea posible. Una solución de seguridad es tan buena como las vulnerabilidades que puede cubrir.
- **D:** El análisis basado en el aprendizaje automático reduce el MTTD y permite que los profesionales de seguridad tomen mejores decisiones.
- **R:** La automatización y la información de seguridad centralizada implican tiempos de respuesta más rápidos e investigaciones optimizadas de las violaciones de seguridad.

Otra parte clave de la filosofía de Cisco Secure es que cada una de estas promesas de XDR son igualmente importantes. El alcance de una plataforma de XDR no significa mucho si no tiene una automatización que respalde las tareas de análisis de seguridad de rutina. Finalmente, Cisco Secure intenta que la integración con los productos de seguridad que ya se encuentran en su entorno sea lo más fácil posible. Las soluciones de XDR no intentan reemplazar estas herramientas de seguridad, sino fortalecerlas al derribar las paredes de los silos y optimizar las operaciones de seguridad.

EN ESTE CAPÍTULO

- Cómo las soluciones en silos crean obstáculos
- Problemas no resueltos para las operaciones de seguridad corporativa

Capítulo 2
El estado de la detección y la respuesta

El panorama actual de detección y respuesta a las amenazas comparte mucho con otros sectores de TI. Hay más herramientas de las que cualquier persona podría controlar, los proveedores tienen diferentes nombres para los mismos conceptos y la complejidad de los entornos de TI es tan grande que la creación de silos se ha convertido en una práctica común.

A pesar de la gran cantidad de herramientas disponibles para los profesionales de la seguridad, aún existen problemas sin resolver que enfrentan los equipos de SecOps. Mantener un tiempo medio de detección (*Mean Time To Detect*, MTTD) bajo y un tiempo medio de respuesta (*Mean Time To Respond*, MTTR) bajo es una lucha constante, y los falsos positivos sobrecargan a los equipos con trabajo innecesario.

Antes de analizar los problemas no resueltos, primero consultemos algunas formas en las que los silos afectan el trabajo de los equipos de seguridad.

Obstáculos de las soluciones en silos

Colocar soluciones en silos fue una respuesta a la intrincada y vasta red de ecosistemas y herramientas de seguridad que los protegen. La idea era que separar diferentes áreas de seguridad en sus propios entornos reduciría la complejidad y permitiría que fueran más manejables.

Por el contrario, estos silos resaltan los desafíos de administrar y proteger un ecosistema corporativo moderno. Son complejos por un motivo. Las redes, los aplicativos y las bases de datos son parte de un todo mayor, no agentes solitarios que pueden vagar por el desierto, viviendo de la tierra a medida que avanzan.

Cada una de estas secciones en silos enfrenta sus propios desafíos por estar en silos. Examinemos algunos ejemplos:

Seguridad de la red

La seguridad de la red es el candado en la puerta que protege todas tus cosas valiosas. Incluye:

- *Firewalls*
- Prevención de intrusiones
- Controles de acceso de red

Esta no es una lista exhaustiva de las funciones de seguridad de la red, pero incluye algunas de las herramientas más importantes. El silo de seguridad de la red incluye información sobre las direcciones IP que intentan unirse a la red, el volumen de tráfico de la red, la integridad del puerto y más.

RECUERDA

Lo que la seguridad de la red puede ver revela lo que no puede ver. Puede haber un aumento repentino y continuo en el tráfico que, desde la perspectiva de la seguridad de la red, parezca un ataque de denegación de servicio distribuido (*Distributed Denial of Service*, DDoS). Pero ¿qué sucede con una nueva carga de trabajo que se conecta y realiza algunas solicitudes iniciales altas a los servicios internos?

Bueno, la seguridad de la red ahora tiene que consultar con los equipos de aplicativos y con cualquier otro equipo que pueda estar causando el pico de tráfico. Esto requiere tiempo y otros recursos. El tiempo de seguridad se consume mientras ocurre un posible ataque. El MTTD y MTTR, en este caso, son mucho más largos de lo necesario.

Seguridad de los aplicativos

La seguridad de los aplicativos implica proteger los aplicativos y sus recursos, lo que incluye servidores, bases de datos, sistemas de mensajería y otra infraestructura de software. Este silo de seguridad cubre mucho terreno, como autorizaciones de bases de datos, monitoreo de uso de CPU, monitoreo de entrada/salida y más.

De manera similar a la forma en que la seguridad de la red puede verse afectada e interrumpirse al no tener toda la información sobre el comportamiento inusual, la seguridad de los aplicativos necesita ver más que solo su propio entorno.

Tomemos un pico de E/S como ejemplo. Digamos que ocurre un cambio extremo en la demanda de la red en medio de la noche. No ocurre durante el horario laboral normal, muchos datos entran y salen a través de un aplicativo, y se alerta a la seguridad de los aplicativos. Esto podría indicar algún tipo de violación de datos, o podría ser evidencia de un proceso de migración de datos por parte de un departamento separado.

¿Qué sucede si hay un gran salto en el uso de la CPU que parece inusual? Eso podría significar que hay software malicioso ejecutándose en una máquina virtual o explotando una vulnerabilidad del aplicativo. O podría ser algo inofensivo y parte de las operaciones comerciales habituales.

En ambos casos, el silo está creando pasos adicionales que deben atravesar los equipos de seguridad, en lugar de permitirles moverse de manera eficiente sin perder tiempo en la verificación una y otra vez para asegurarse de que toda la actividad esté en orden.

Seguridad de los endpoints

La seguridad de los endpoints también cubre una variedad de herramientas de seguridad. El *antimalware*, la prevención de pérdida de datos y la detección de amenazas de dispositivos endpoints se encuentran bajo el paraguas de la seguridad de los endpoints. El volumen de las herramientas de seguridad de los endpoints está aumentando, lo que se suma a la complejidad de esta área, con el impulso del trabajo remoto. Más dispositivos requieren acceso a los recursos internos, lo que significa que se necesita más seguridad para más dispositivos que nunca.

La seguridad de los endpoints en sí misma no presenta tantos inconvenientes del silo de seguridad como las demás áreas de seguridad, pero genera problemas para otros equipos, como la administración de identidades y la seguridad de la red.

Gestión de identidad y acceso

Esta zona es un poco engañosa. ¡Ni siquiera tiene "seguridad" en el nombre! Uno de los grandes trabajos de la gestión de identidad y acceso (*Identity and Access Management*, IAM) es administrar la autenticación. Es un término general que cubre:

- Autenticación de dos factores
- Certificados digitales
- Nombres de usuario
- Contraseñas

Según a qué se accede, las regulaciones de la industria y las políticas específicas de la organización, uno o más de estos puntos determinarán las necesidades específicas de autenticación de inicio de sesión.

Un ejemplo simple de silos que perjudican las operaciones son los intentos fallidos de inicio de sesión. Los intentos fallidos repetidos de inicio de sesión, ya sea una contraseña o un nombre de usuario mal recordado, o algo completamente diferente, pueden parecer un intento de ataque para los equipos de seguridad de aplicativos y redes.

Dado que la IAM cubre las identidades de cuentas de servicio, se cruza con la seguridad de los aplicativos en la autorización de uso de recursos. Para disminuir el MTTD y el MTTR, es especialmente importante eliminar la seguridad de la red del silo y de IAM.

Problemas no resueltos que desafían a las empresas

La esfera de la tecnología de negocios evoluciona a una velocidad vertiginosa, pero todavía hay muchos problemas que causan dolores de cabeza a los desarrolladores, administradores, profesionales de la seguridad y líderes empresariales. El MTTD, el MTTR, los falsos positivos de ciberataques y la ineficiencia en la clasificación de incidentes son problemas que aún enfrentan las empresas.

MTTD

El tiempo medio de detección (MTTD) es una parte fundamental de la seguridad corporativa. El MTTD es la cantidad de tiempo que suele tardar un equipo de seguridad en encontrar y confirmar que se ha producido una violación a la seguridad. Alcanzar un MTTD bajo es más que solo recibir una alerta y encontrar el sitio del ataque.

Detectar una amenaza o un ataque en curso implica observar múltiples sistemas entrelazados y coordinar la comunicación entre los equipos a cargo de esos sistemas. Por ejemplo, si un administrador de red nota una actividad que parece una infiltración en la base de datos, la actividad debe verificarse con los equipos de la base de datos para ver si realmente está ocurriendo.

El desafío aquí es coordinar la detección rápidamente, sin perder precisión. El exceso de velocidad para confirmar la validez de una amenaza conduce a una pérdida de tiempo y recursos aún mayor.

MTTR

El reloj del tiempo medio de recuperación (MTTR) comienza a correr justo después de que se haya identificado y confirmado un problema de seguridad. El MTTR es la medida promedio del tiempo que tardan los equipos de seguridad en detener o solucionar el problema. Las grandes preguntas para MTTR: ¿Qué se ha comprometido y cómo se soluciona?

El mayor desafío al responder a una amenaza suele ser que el alcance del entorno de TI es tan grande que es difícil ver todo el daño ocurrido. Es difícil por varias razones y depende del contexto:

- Tal vez sea necesario encontrar las direcciones IP y verificarlas con el equipo de seguridad de la red en el caso de un ataque basado en la red, pero si la violación ya ocurrió, ¿a qué otros lugares se dirigió el ataque?
- Si se violó una base de datos, puede ser difícil ver exactamente a qué tablas se accedió, si la información que obtuvo el atacante le permitió acceder a otras partes del sistema, etc.
- El ataque puede tener varios frentes, y el atacante viola varios puntos de entrada.

Cada uno de estos problemas requiere una solución diferente, y esta solución debe adaptarse a la situación específica. ¿Hay que impulsar una actualización de software rápida o reparar una biblioteca vulnerable? ¿Hay que bloquear un puerto de dirección IP para evitar más ataques? La respuesta puede ser una combinación de cosas, y decidir cuál es la opción correcta es tan importante como encontrar la violación en primer lugar.

Falsos positivos

En el contexto de la seguridad, los falsos positivos son actividades benignas que se identifican erróneamente como amenazas a la seguridad. Tal vez un administrador de la base de datos se marcha a la hora de almuerzo después de comenzar un gran trabajo de exportación. Mientras tanto, un empleado de seguridad de la red cancela su almuerzo porque ve un gran volumen de tráfico en la red que no esperaba. Para empeorar las cosas, se suponía que su almuerzo iba a ser un delicioso sándwich de pollo katsu. ¡Qué desperdicio terrible!

Las violaciones de seguridad que son falsos positivos no solo causan interrupciones innecesarias y pérdida de tiempo, sino que también dejan pasar inadvertidamente violaciones de seguridad reales. La fatiga de las alertas se asemeja al "Pastorcito mentiroso". Digamos que, en promedio, un equipo de seguridad de aplicativos recibe diez alertas de seguridad todos los días, pero solo dos de ellas son amenazas legítimas. Si esto pasa durante unos pocos días no es un problema, pero si hay semanas de alertas falsas, el equipo no prestará mucha atención a las alertas. Después de todo, lo más probable es que no sea una amenaza real.

Entonces, los falsos positivos son un desafío especialmente importante para los equipos de seguridad. No solo desperdician el tiempo valioso de los profesionales de seguridad, sino que también pueden ocasionar que más amenazas de seguridad atraviesen la línea de defensa.

Clasificación de incidentes

La clasificación de incidentes comparte muchos de los mismos problemas con el MTTR. Mientras que el MTTR se preocupa por el tiempo que lleva resolver un problema, la clasificación de incidentes se trata de priorizar los pasos para recuperarse del incidente.

Al igual que con todos los demás puntos de desafío en esta sección, aquí es clave el contexto. Tiene que haber una comprensión del impacto de la solución de seguridad para minimizar las consecuencias negativas. Como ejemplo, si se viola una base de datos, una opción es cerrarla. Sin embargo, es posible que se realicen actividades de negocios esenciales que utilicen esa base de datos. Si ese es el caso, tal vez haya una solución menos obvia pero igualmente efectiva.

Muchas violaciones de seguridad, como una violación a la base de datos, requieren respuestas inmediatas. En estos casos, los equipos de seguridad actuarán con la mayor rapidez posible. Sin embargo, si no tienen el contexto adecuado, la solución podría terminar siendo peor que el problema.

Lo que nos hace volver al problema de los silos. Como los equipos de seguridad solo ven lo que hay en sus respectivos silos, las respuestas de seguridad pueden ser lentas, ineficaces, ineficientes y, en última instancia, disruptivas.

RECUERDA

Cuando se trata de la seguridad, el contexto es muy importante. ¡Contexto, contexto, contexto!

EN ESTE CAPÍTULO

- Consolidación del análisis de detección
- Investigación de la remediación
- Beneficios de la orquestación y la automatización

Capítulo 3
XDR: Integrar la pila de seguridad

Una pila de seguridad desarticulada puede generar muchos problemas. Los profesionales de seguridad a menudo carecen del contexto que necesitan para enfrentar los problemas de seguridad de manera rápida y eficiente, la fatiga de las alertas hace que las preocupaciones de protección válidas queden desatendidas, y el personal de seguridad esté sobrecargado de trabajo persiguiendo falsos positivos.

Las soluciones de detección y respuesta extendida (*Extended Detection and Response*, XDR) brindan muchos beneficios, pero uno de los más importantes es cómo intentan integrar la pila de seguridad. Las tareas de análisis, remediación y automatización se simplifican cuando se les permite acceder y comprender el contexto completo de la pila de seguridad. Este capítulo examina cómo las soluciones de XDR reúnen estos elementos.

Análisis de detección

El análisis de detección no se trata solo de lo que se ve, sino de lo que se aprende. Las operaciones de seguridad (*Security Operations*, SecOps) exitosas implican enfrentar una amenaza y descubrir cómo enfrentar otras similares en el futuro. A menudo, es más que buscar vulnerabilidades de

software similares a las que has visto en el pasado o pensar en términos de cómo un *malware* específico podría infectar nuevamente tu sistema.

CONSEJO

Visualizar los patrones de ataque y las estrategias que utilizan los atacantes es información poderosa. Tanto los tipos de ataques como sus métodos están cambiando. Un buen análisis de detección trata de ocuparse de estos dos aspectos.

Las capacidades de análisis de detección de las plataformas de XDR se basan en la integración. Estas son las principales fuentes que las plataformas de XDR analizan y agregan:

- **Endpoints:** Incluye estaciones de trabajo para empleados, computadoras portátiles, teléfonos inteligentes, tabletas, dispositivos del Internet de las Cosas (*Internet of Things*, IoT) y más.
- **Redes:** Esto incluye redes públicas y privadas, nubes privadas virtuales y más.
- **Aplicativos:** Incluye el correo electrónico y cualquier software como servicio (*Software as a Service*, SaaS) que utilice el personal, como el acceso a través de un navegador web.
- **Nube:** Los servicios en la nube pueden incluir bases de datos en la nube, herramientas de administración y más.

Las herramientas de XDR permiten que los equipos de seguridad vean todas estas partes juntas: cómo se comunican entre sí, qué fue a dónde, etc. Veamos cómo esta integración cambia lo que los equipos de seguridad pueden ver y cómo operan.

Visualizaciones e inteligencia de amenazas agregadas

Una característica clave de muchas soluciones de XDR es una vista agregada de información sobre amenazas. Su aspecto cambia de una plataforma a otra, pero la base son visualizaciones legibles de información de seguridad relevante en caso de un problema de seguridad.

Debido a que las herramientas de XDR abarcan desde los endpoints hasta el equipo de seguridad, la plataforma puede mostrar a los profesionales de seguridad una visión integral del problema. Examina los endpoints que podrían ser el punto de violación, ve las alertas que te llamaron la atención, qué recursos podría estar afectando el ataque y más.

RECUERDA

Las plataformas de XDR analizan tanta información y pueden organizarla de manera accesible de forma tal que agregar inteligencia de amenazas en este contexto es casi una auditoría en tiempo real. Se puede ver la información de seguridad relevante justo después de que haya ocurrido el evento.

La forma en que se muestra toda esta información al personal de seguridad depende de la plataforma de XDR, pero existen algunos métodos comunes para visualizar la información de seguridad:

- **Paneles:** Muchas plataformas tienen un panel que puede equiparse con diferentes fuentes de información de seguridad, para una fácil referencia y monitoreo.
- **Mapas de amenazas:** Las plataformas de XDR con frecuencia cuentan con herramientas de visualización de infraestructura que permiten ver las relaciones entre servicios o recursos. Puede ser un gráfico de nodos, un mapa o alguna otra representación de información de seguridad relevante.
- **Personalización:** Las plataformas de XDR con frecuencia brindan opciones de personalización sobre cómo y dónde se representan todos estos recursos.

CONSEJO

Diferentes organizaciones requieren acciones diferentes de sus soluciones de seguridad, por lo que el monitoreo flexible y la inteligencia de amenazas son esenciales. Los componentes del panel a menudo visualizan problemas de seguridad a lo largo del tiempo. Por ejemplo, gráficos de líneas que muestran la cantidad de intentos de penetración en la red durante los últimos seis meses o los tiempos de respuesta para la detección y reparación de *malware*.

Las capacidades de mapeo de las herramientas de XDR permiten a los equipos de seguridad ver una violación de principio a fin, desde dónde comenzó hasta dónde está ahora, y qué podría afectar potencialmente en el camino. ¡Este punto es tan importante que muy pronto tendrá su propia sección!

Correlacionar y contextualizar

La visibilidad del contexto y la correlación son las armas no tan secretas de las plataformas de XDR. Antes de un análisis más detallado, estas son las definiciones de trabajo de los términos dentro del espacio de seguridad de TI:

- El **contexto** ayuda a responder el "por qué" de un problema de seguridad. Idealmente, coloca los problemas de seguridad en una perspectiva de pila completa, mostrando las ramificaciones potenciales de un ataque o una solución.
- La **correlación** debería responder el "dónde" de un problema de seguridad. Se trata de qué recursos se ven afectados y qué impacto pueden tener esos recursos comprometidos.

Las plataformas de XDR se enfocan en el endpoint y avanzan a partir de allí, por eso las herramientas de seguridad que conforman el ecosistema serán visibles. Sin una visión clara del alcance completo de un ataque, desde el endpoint hasta la red y los aplicativos, la evaluación y corrección de amenazas sufre. Hay tres razones principales por las que las brechas de seguridad de TI actuales son tan desafiantes:

- El número de posibles puntos de ataque ha aumentado en los últimos años.
- La complejidad y sofisticación de los ataques ha crecido.
- En respuesta a estos nuevos desafíos, las pilas de seguridad también se han vuelto más complicadas.

Una de las formas clave en que las plataformas de XDR ayudan a los equipos de seguridad a enfrentar estos nuevos desafíos es a través de la visualización. Las funciones de mapeo de amenazas de las plataformas de XDR muestran la correlación entre los diferentes sistemas que participan, directa o indirectamente, en un ataque. Por ejemplo, se encuentra un *malware*. Mediante un mapa de amenazas, el software malicioso se rastrea hasta una computadora portátil terminal, donde un empleado abrió el correo electrónico de un atacante.

¿Y un ejemplo de contexto? Supongamos que hay un gran pico de entrada o salida programado en medio de la noche: Un disparador de alerta simple no tendrá un contexto completo. Esta alerta puede activarse simplemente porque parece un comportamiento sospechoso, cuando en realidad es una operación esencial para el negocio. Con un contexto más amplio, los equipos de seguridad y sus sistemas de alerta tendrían más información sobre por qué suceden las cosas. Las amenazas de falso positivo son pérdidas de tiempo y energía, e incluso pueden hacer que los equipos pasen por alto amenazas legítimas debido a la fatiga de las alertas.

Por lo tanto, las capacidades de correlación y contextualización muestran a los equipos de seguridad el panorama general. La siguiente pregunta es: ¿Qué hacer con lo que se ve?

Identificar amenazas y formular una respuesta.

Gracias a la correlación y el contexto que brindan las herramientas de XDR, las amenazas son más fáciles de identificar. Las herramientas de XDR reducen el tiempo para encontrar la ubicación y las implicaciones más importantes de un ataque, pero también tienen un impacto directo en la forma en que los profesionales de la seguridad enfrentan una amenaza.

En primer lugar, el enfoque de pila completa de las herramientas de XDR, junto con los extensos historiales de seguridad que los equipos pueden generar, significa que las anomalías se pueden identificar como tales.

Un aumento de actividad en el servidor A, seguido de un aumento en el servidor B, podría ser una actividad comercial normal. Es un patrón que los sistemas de seguridad pueden reconocer, trabajando en conjunto, y esta información se puede aplicar a futuros ataques. ¿Qué sucede si el servidor B observa un aumento de actividad, pero el servidor A está en silencio? La plataforma de XDR lo reconocerá como un comportamiento anómalo y activará una respuesta.

Los análisis también aceleran la formulación de respuestas. Examina de nuevo el servidor B comprometido. El servidor B puede estar ejecutando un software que tenga una vulnerabilidad conocida. Como el equipo de seguridad ha identificado este servidor como el área del problema, puede buscar rápidamente vulnerabilidades conocidas en este software y aplicar parches según sea necesario.

El análisis de detección también ayuda a los equipos de seguridad a responder de manera más inteligente, no solo más rápida. El servidor B, mientras está siendo atacado, podría estar enviando datos esenciales para el negocio al servidor C. Debido a esto, el servidor B no puede apagarse ni interrumpirse. El personal de seguridad lo sabe porque tiene la imagen completa y puede formular un nuevo plan que no interrumpa las operaciones comerciales importantes.

Remediación de investigaciones

Puedes encontrar amenazas todo el tiempo, pero no significa mucho si no las solucionas. Hay muchos enfoques para la remediación, y las herramientas de XDR intentan ayudar a aliviar la carga de encontrar la correcta y aplicarla.

RECUERDA

Hay dos formas principales en que las herramientas de XDR mejoran la remediación de investigaciones: mediante el apoyo del personal del Centro de Operaciones de Seguridad (*Security Operations Center*, SOC) y mediante un impulso a las capacidades de seguimiento de incidentes.

El personal del SOC a menudo está sobrecargado de trabajo, y esto trae aparejadas consecuencias para la seguridad. Las herramientas de XDR pueden aligerar la carga al agilizar y simplificar muchas operaciones de seguridad necesarias. El seguimiento de incidentes también se mejora enormemente con los aportes que brindan las plataformas de XDR. El seguimiento del historial de ataques tiene implicaciones de seguridad que pueden ser excelentes herramientas para los equipos de seguridad.

Apoyo para el SOC

El personal del SOC tiene que trabajar duro y rápido para mantenerse actualizado con el panorama actual de amenazas. Desafortunadamente, muchas herramientas de seguridad no están actualizadas con las necesidades prácticas del SOC. Una pila de seguridad ineficiente no solo agrega estrés a los equipos de seguridad, sino que también puede inducir fatiga de las alertas y, como consecuencia, que se pasen por alto las amenazas.

La mayor ventaja individual para las operaciones del SOC que ofrecen las herramientas de XDR es el panel centralizado. El panel en muchas plataformas de XDR sirve como un único punto de acceso a los datos de seguridad integrados de toda la pila de seguridad. Esto a menudo incluye visualizaciones, historiales y registros de alertas, paneles de información personalizables y más.

CONSEJO

Puede parecer que esto solo transforma la fatiga de las alertas en fatiga del panel, pero la personalización de estas vistas centrales debería evitar que eso suceda. Solo debes alinear lo que necesitas ver.

Las herramientas de análisis personalizadas brindan contexto a un problema de seguridad, lo que significa facilidad de priorizar las respuestas a incidentes, reducción de falsos positivos y operaciones más eficientes del SOC.

Otro conjunto importante de herramientas que aportan las plataformas de XDR, desde una perspectiva del SOC, es la automatización de la orquestación. El SOC está formado por profesionales de seguridad competentes y bien capacitados, y abrumarlos con tareas que podrían automatizarse es solo una pérdida de su valioso tiempo.

Una computadora portátil terminal que está comprometida puede bloquearse rápidamente de la red si se activa la automatización correcta. Un ser humano tardaría más en hacerlo, y su tiempo estaría mejor invertido en otro lugar. El lado humano de las cosas, cuando sea posible, debe comenzar cuando se necesita la planificación y la toma de decisiones difíciles.

RECUERDA

La automatización no se trata solo de ahorrar tiempo. También es una forma de acelerar todo el proceso de respuesta.

Seguimiento de incidentes

Otra bendición para los equipos de seguridad de remediación: los historiales de ataques. Las plataformas de XDR incluyen módulos de panel personalizables o, a veces, paneles dedicados, para realizar un seguimiento y registrar violaciones de seguridad pasadas. En ocasiones se realiza un seguimiento por sistema, por ejemplo, mediante el listado de las infracciones de la base de datos y los ataques a la red por separado, o por tipo de ataque, por ejemplo, mediante una lista de todos los ataques de DDoS.

El reconocimiento de patrones de ataque brinda información útil sobre futuros ataques. Si se identifica una brecha y muestra un comportamiento que los equipos han visto antes, tal vez muchas veces antes, les resultará mucho más fácil enfrentar la amenaza.

Tener un historial de ataques anteriores es una forma de generar conocimiento institucional sobre tipos y patrones de ataques comunes. Es importante correlacionar la inteligencia de amenazas de fuentes internas y externas en su vista histórica e incluir fechas de vencimiento apropiadas para esa inteligencia, especialmente en el caso de IP, que pueden transferir la propiedad fácilmente y dejar un recurso crítico en la "lista de bloqueo". Los equipos del SOC pueden identificar amenazas comunes más rápido y responder a ellas de manera más eficiente, con el conjunto de conocimientos que crearon los equipos de seguridad.

Volviendo al ejemplo del pobre servidor B, supongamos que el pico de actividad en el servidor B se identifica como una amenaza. Los equipos de seguridad, utilizando el conocimiento de los historiales de ataques, pueden reconocer el tipo de actividad que está ocurriendo, sus patrones

anteriores y actuales, y saber exactamente qué tipo de ataque es, además de tener una buena idea de su origen.

Este tipo de información histórica se extiende a las propias respuestas. Si este tipo de ataque ha ocurrido antes, entonces los equipos de seguridad lo han tratado antes. El seguimiento de incidentes debe ser más completo que la identificación de problemas: también debe incluir averiguar una forma más eficaz de abordar estos problemas en el futuro.


CONSEJO

Cuando los atacantes te dan *malware*, prepara limonada. Exprime hasta la última gota de información de los historiales de violaciones de seguridad. Los ataques son malos cuando ocurren, pero se convierten en un poderoso recurso de seguridad.

Automatización de la orquestación

La automatización de la orquestación es la forma en que las plataformas de XDR admiten la automatización de trabajos que pueden requerir información de toda la pila de seguridad. Incluye la integración de herramientas de seguridad dispares para que las tareas de automatización puedan beneficiarse de los diferentes puntos de vista de seguridad, además de realizar los trabajos de automatización reales.

Integrar múltiples tecnologías de seguridad

La pila de herramientas de seguridad que componen una pila de seguridad es complicada; sin embargo, integrarlas a través de una plataforma de XDR puede simplificar los *scripts* y trabajos de automatización. Como muchas otras partes de las tareas del SOC, la falta de contexto hace que la vida sea mucho más difícil para la automatización. Una vista de la pila completa permite que las tareas de automatización tengan disparadores más complejos y sofisticados que respondan de manera más eficiente y consistente a las amenazas legítimas.

Es posible que la automatización dentro de una solución de endpoints en silos solo detecte una parte de las violaciones del endpoint, sin información sobre la seguridad de la red y el registro de respuesta a incidentes. Aprovechar las capacidades de orquestación solo aumenta la eficacia de las respuestas de seguridad en toda la pila.


CONSEJO

No hagas que la solución sea peor que el problema. Evita *scripts ad hoc* personalizados para cada nueva respuesta. Los profesionales de la seguridad no deberían tener que agregar el mantenimiento del software a su lista de responsabilidades.

También está la cuestión de encargarse de los propios *scripts* de automatización. Las tareas de automatización en entornos aislados con frecuencia necesitan cuidados. Las actualizaciones de software, los cambios de cumplimiento y los cambios de herramientas de seguridad pueden interrumpir el uso regular de *scripts ad hoc*.

Tener herramientas de seguridad integradas disponibles para las tareas de automatización significa que los equipos de seguridad pueden utilizar más información y un entorno más estable. Los casos marginales con *scripts* de automatización personalizados se pueden integrar en una solución de automatización más grande, lo que significa menos cuidados y menos *scripts* para seguir.

RECUERDA

¡La automatización *ad hoc* no es automatización!

Respuestas automatizadas

Tenemos la integración y el alcance, pero ¿qué puede hacer realmente la automatización?

Con las herramientas de XDR, los equipos de seguridad pueden realizar tareas de automatización más detalladas de lo que permitirían otros tipos de soluciones de seguridad. El alcance de la pila de seguridad y los historiales de ataques significan que las tareas de automatización de las herramientas de XDR son planos bien informados sobre cómo se realizarán los ataques.

Examina este ejemplo de un endpoint: Se identificó un endpoint en el que se está ejecutando un *malware*. Una tarea de automatización, creada por el personal de seguridad para responder a este tipo de amenazas, tiene una serie específica de acciones para realizar un paso preliminar de remediación. En este caso, podría incluir aislar el endpoint del resto de la red y luego ejecutar software *antimalware* en la máquina infectada.

En el caso de una violación de datos, puede haber un conjunto más complejo de respuestas automáticas necesarias para tratarlo adecuadamente. Algunas bases de datos no se pueden cerrar simplemente porque podrían participar en tareas esenciales para el negocio. En cambio, una respuesta automática podría, según ciertos criterios, decidir que no se puede cerrar una base de datos con una violación y, en cambio, cambiar una regla de *firewall* para detener la salida de datos de ese servidor.

EN ESTE CAPÍTULO

- *¿Qué es SIEM y qué examina?
- *¿Qué es SOAR y qué hace?
- Cómo SIEM y SOAR interactúan con las herramientas de XDR

Capítulo 4
XDR, SIEM, SOAR: ¿Amigos o enemigos?

No podemos hablar de detección y respuesta extendida (*Extended Detection and Response*, XDR) sin repasar también sus dos mayores predecesores: la gestión de eventos e información de seguridad (*Security Information and Event Management*, SIEM) y la orquestación, automatización y respuesta de seguridad (*Security Orchestration Automation and Response*, SOAR). Son dos de las herramientas de seguridad más destacadas del mercado que se anuncian como solucionadores de problemas generales.

SIEM y SOAR adoptan diferentes enfoques para fortalecer la pila de seguridad de TI y brindan diferentes resultados para el cliente. Si bien las herramientas de XDR están invadiendo sus espacios, los estándares antiguos no son del todo incompatibles con el producto nuevo.

SIEM

La gestión de eventos e información de seguridad (SIEM) es una solución de seguridad que se centra en recopilar datos de seguridad de toda una infraestructura de seguridad y proporcionar la mayor cantidad posible de registros y alertas. Esta concentración en la información de seguridad sin procesar tiene ventajas y desventajas.

RECUERDA

Por un lado, a veces tu organización necesita exactamente eso: pilas y más pilas de registros. Las industrias de cumplimiento intensivo, como la industria de atención médica o de finanzas, a menudo requieren grandes cantidades de información sobre sus sistemas internos. Por otro lado, muchas industrias simplemente no necesitan saber acerca de cada problema en el radar de seguridad. Muchas veces, estos destellos no son ataques. Las siguientes secciones analizan algunas de las capacidades de las soluciones SIEM y lo que significan para los equipos de seguridad.

¿Qué examina?

En resumen, las soluciones de SIEM examinan lo que se les dice que examinen. Como el tipo de producto evolucionó, las SIEM mejoraron cada vez más a la hora de recopilar información y colocarla en una ubicación central para su análisis. Las capacidades de recopilación de datos de SIEM dependen de los productos y herramientas que están monitoreando.

SIEM es una herramienta de seguridad comprobada que intenta integrar sistemas previamente aislados que necesitan monitoreo. Estas son algunas de las ubicaciones que las herramientas de SIEM pueden monitorear:

- Eventos del *firewall*
- Dispositivos de la Internet de las Cosas (*Internet of Things*, IoT)
- Dispositivos de seguridad
- Software antivirus
- Aplicativos

Los registros de eventos se recopilan en una ubicación centralizada para su procesamiento y análisis. Los agregados recientes al ámbito SIEM han sumado algunas características de procesamiento automatizado, herramientas de orquestación y otras capacidades que han sido exclusivas de las soluciones de SOAR.

Las soluciones de SIEM utilizan diferentes sistemas basados en reglas para determinar si la actividad en los recursos monitoreados es sospechosa. Si se determina que el comportamiento es potencialmente una violación de la seguridad, se envían alertas a un punto de acceso central para que el personal de seguridad lo revise y decida un curso de acción.

SIEM ha existido por un tiempo y ha demostrado su utilidad repetidamente. Sin embargo, existen algunas limitaciones para este tipo de solución de seguridad, que las nuevas soluciones están superando, manteniendo los principales beneficios de SIEM.

El resultado es una visibilidad limitada

La capacidad de SIEM para administrar las alertas de una pila de seguridad completa puede ser una herramienta poderosa. También puede, contrariamente a la intuición, generar una menor visibilidad de todo el ecosistema para los equipos de seguridad. La fatiga de las alertas y los falsos positivos ejercen una presión innecesaria sobre el personal de seguridad y pueden hacer que se pierdan de vista amenazas legítimas.

La fatiga de las alertas es el resultado de un sistema de seguridad que emite tantas alertas que los equipos de seguridad se ven abrumados al verificar la validez de las amenazas. Hay algunas razones por las que podrían generarse demasiadas alertas:

- Los sistemas en silos hacen que los equipos de seguridad interpreten incorrectamente cuál comportamiento es realmente sospechoso.
- Las alertas no tienen suficiente contexto para ser precisas.
- El sistema de alerta en sí mismo no proporciona el control de alerta detallado necesario para adaptar las alertas a necesidades específicas.

Cuando ocurre la fatiga de las alertas, es más probable que los equipos de seguridad pasen por alto las amenazas que deban abordarse. Están demasiado preocupados con alertas innecesarias que ocultan los problemas de seguridad legítimos.

Los sistemas en silos y los amplios criterios de alerta también conducen a eventos de seguridad falsos positivos. Sin un contexto del ecosistema de TI más amplio, las herramientas de alerta a menudo confunden lo que sucede en los sistemas o identifican falsamente las amenazas de seguridad. Un servidor puede ver un pico de actividad durante un fin de semana festivo que activa una alerta por comportamiento sospechoso, cuando esta actividad es un trabajo planificado que debe ejecutarse durante las horas que no son pico.

Los falsos positivos son una pérdida de tiempo para los equipos de seguridad y se suman a la fatiga de las alertas. Esto puede crear una cultura de esperar que una alerta sea de baja prioridad, pues probablemente no será una amenaza real. Las alertas deben tomarse en serio y proporcionar a los equipos la información que necesitan.

RECUERDA

Calidad sobre cantidad. Los equipos de seguridad necesitan buena información, no mucha.

SOAR

Las soluciones de orquestación, automatización y respuesta de seguridad (SOAR) están más del lado de la preparación y la acción de la seguridad y, a primera vista, parecen bastante similares a las plataformas de XDR. La diferencia principal entre ambas es la integración, que afecta lo que pueden hacer los equipos de seguridad y cómo lo hacen.

¿Qué hace?

Las soluciones de SOAR tienen como objetivo optimizar la orquestación y la respuesta por medio de herramientas de automatización. SOAR es una categoría de herramientas de seguridad que es relativamente nueva en el panorama de TI, acuñada por Gartner en 2017, y ha brindado a los usuarios nuevas formas de enfrentar las amenazas.

El núcleo de las plataformas de SOAR es el "manual". Es una herramienta de orquestación diseñada por equipos de seguridad para planificar una secuencia de acciones en respuesta a una amenaza. Partes de este plan pueden optimizarse mediante la automatización, que a menudo puede utilizar técnicas de aprendizaje automático para mejorar el desempeño.

Sin embargo, las soluciones de SOAR no pueden actuar de manera independiente, por lo que ofrecen integración con otras herramientas de seguridad, como las soluciones de detección y respuesta de red (*Network Detection and Response*, NDR). Entonces SOAR responde a la información generada por las otras herramientas utilizando los manuales y funciones automatizadas.

Estas plataformas son herramientas poderosas para orquestar respuestas de seguridad, pero tienen algunos inconvenientes. Si bien ofrecen integración con otras herramientas de seguridad, las plataformas de SOAR a menudo hacen que sea complicado ponerlas en funcionamiento y carecen de capacidades de detección integrales.

El resultado es carga sobre SecOps

Los equipos de operaciones de seguridad (*Security Operations*, SecOps) asumen el trabajo de proteger los recursos y los sistemas comerciales. Las redes, los aplicativos y los datos comerciales y de los clientes caen bajo su atenta supervisión. Es una gran carga para la que realizar un seguimiento, y los equipos de SecOps no necesitan un peso adicional que afecte su trabajo.

Las soluciones de SOAR con frecuencia tienen compatibilidad de integración con muchos tipos de herramientas de seguridad, muchas de las que ya forman parte de tu infraestructura de seguridad, pero a veces se requiere un trabajo adicional para que SOAR sea compatible con las otras herramientas. Muchas SOAR tienen un acceso mediocre a las API, lo que significa que la integración completa de las herramientas de observación de seguridad que necesitas es difícil, si no imposible.

Este desafío puede provocar interrupciones en el flujo de trabajo, limitaciones de detección y la necesidad de herramientas de seguridad adicionales para llenar los vacíos. Estos tres factores hacen que los equipos de SecOps trabajen más y con menos eficiencia. Cada nueva herramienta en la pila de seguridad es un nuevo punto de falla, una nueva solución para integrar y aprender, y una nueva carga para el profesional ya ocupado que tiene que vigilarla.

RECUERDA

Aunque SOAR es una poderosa herramienta de seguridad, puede sumarle a SecOps dolores de cabeza innecesarios. Este es especialmente el caso con los avances recientes en las capacidades de la plataforma de XDR.

Trabajo conjunto

Al igual que SIEM y SOAR, la plataforma de XDR no puede funcionar de manera independiente. Requiere otras herramientas de seguridad para respaldarla, brindarle la información que necesita para funcionar y llenar los vacíos en su conjunto de características. Tanto SIEM como SOAR son soluciones de seguridad competentes y han demostrado ser útiles para muchas organizaciones. Las plataformas de XDR son nuevas y prometedoras, pero no deben descartarse ni olvidarse las herramientas más establecidas.

SIEM y SOAR se incorporan en XDR

La plataforma de XDR ofrece mucho a las organizaciones, pero no es un remedio para todo. Una implementación exitosa de XDR necesita otras herramientas de seguridad para respaldarla y, según las necesidades específicas de la organización, podría ser beneficioso integrar las fortalezas de las soluciones SIEM o SOAR con tu herramienta de XDR.

Como SIEM es una herramienta tan sólida para el registro y las alertas, puede reforzar las capacidades de análisis de la plataforma de XDR al proporcionar datos de registro completos. Como la plataforma de XDR puede manejar grandes cantidades de información de seguridad, una

avalancha de registros de SIEM no debería provocar la pérdida de información esencial o la omisión de alertas. Las soluciones de SIEM también podrían ayudar a los equipos que usan herramientas de XDR a fortalecer sus requisitos de cumplimiento. Algunas organizaciones simplemente requieren grandes pilas de registros para cumplir con los estándares de la industria, y la XDR puede ser la herramienta de análisis y organización necesaria para manejarlo.

Sin embargo, la integración de SOAR con XDR es más bien un caso extremo. Las soluciones de XDR ofrecen herramientas integrales de orquestación y automatización, que es exactamente el gran punto de venta de SOAR. Sin embargo, la plataforma de XDR se puede usar por sus análisis y herramientas, mientras que una solución de SOAR complementaria se usa para muchas de las tareas de automatización y orquestación. Es una opción para aquellos a quienes simplemente les agrada usar el producto de SOAR que ya utilizan en su entorno de seguridad. Tal vez tus equipos de seguridad prefieren ajustarse al manual y las capacidades de automatización de SOAR, pero pueden beneficiarse con análisis y el punto de vista centralizado de la plataforma de XDR sin aprovechar sus otras herramientas.

RECUERDA

La plataforma de XDR no debe considerarse como un simple reemplazo de las soluciones de seguridad existentes, sino como un agregado favorable al panorama de la seguridad. Hay instancias en que las herramientas de XDR pueden reemplazar a las existentes, pero una de las fortalezas del tipo de producto es su capacidad para integrarse con entornos de seguridad existentes.

Centralizar la información de seguridad

Una de las formas en que la plataforma de XDR puede integrarse tan eficazmente con la infraestructura de seguridad existente es a través de su enfoque en la centralización de la información de seguridad. Estas son algunas características que permiten que las herramientas de XDR centralicen lo que los equipos de seguridad necesitan ver:

- **Tablero de control personalizable:** Las soluciones de XDR suelen tener al menos un tablero de control central con paneles de observación personalizables. Estas áreas se pueden mover para mostrar diferentes partes de tu infraestructura de seguridad, alertas, historiales de ataques y más.
- **Mapas de incidentes:** Son visualizaciones de incidentes de seguridad que muestran a qué sistemas afectó un ataque y con qué más pudo haber estado en contacto. Es similar a los mapas

epidemiológicos utilizados para estudiar la propagación de enfermedades y puede ayudar a los equipos a rastrear un ataque hasta su origen.

- **Acceso a herramientas de apoyo de seguridad:** La mayoría de las soluciones de XDR brindan fácil acceso a las otras herramientas de seguridad que alimentan la información de la plataforma. Por lo general aparece como parte del panel central o un menú de acceso rápido.

Las grandes promesas de integración de las plataformas de XDR no serían mucho sin una forma centralizada de acceder a toda esa información, por lo que los proveedores de herramientas de XDR desean que sus productos sean fáciles de leer y usar. La información centralizada reduce las cargas de trabajo en los equipos de seguridad, acorta los tiempos de identificación y respuesta, y brinda a los profesionales de la seguridad el espacio para mejorar las respuestas futuras en lugar de buscar en franjas de datos.

Otras tecnologías a tener en cuenta

Dos tecnologías a tener en cuenta al pensar en herramientas de XDR son la detección y respuesta de endpoints (*Endpoint Detection and Response*, EDR) y la detección y respuesta de red (*Network Detection and Response*, NDR). Estas dos herramientas pueden actuar como excelentes soportes para una implementación exitosa de la solución de XDR, al ayudar a los equipos de seguridad a navegar por las complejidades de los entornos de red y endpoints.

EDR, a veces llamado detección y respuesta de amenazas de endpoints (*Endpoint Threat Detection and Response*, ETDR), puede considerarse un pariente o precursor de XDR. Realiza algunas de las funciones principales de un producto de XDR, como centrarse en la supervisión y detección de endpoints, aunque por lo general no tiene muchas de las capacidades de análisis y punto de vista centralizado de las plataformas de XDR. Es importante tener en cuenta al EDR, porque es probable que sea el tipo de herramienta adecuado para alimentar tu solución de XDR centralizada con los datos de seguridad de endpoint que necesitas.

Las herramientas de NDR son similares a las de EDR, pero en su lugar monitorean la actividad y los recursos de la red. Las herramientas de NDR pueden ayudar a identificar las amenazas de la red y brindar respuestas automáticas aunque, nuevamente, estas soluciones a menudo

no cuentan con las herramientas integrales que proporcionan las plataformas de XDR. La ventaja de tener una herramienta de monitoreo de seguridad de red dedicada es que necesita visibilidad de los ataques a las redes, que son cada vez más complejos y múltiples. Con frecuencia existen múltiples puntos de ataque, y una herramienta de seguridad de red sumamente enfocada puede agregar mucho a una infraestructura de seguridad.

RECUERDA

¡Las soluciones de XDR no son ladronas que han venido a robar los éxitos de tu SIEM! Son plataformas que funcionan bien en conjunto con muchas herramientas de seguridad que ya estás utilizando.

EN ESTE CAPÍTULO

- La filosofía de XDR de Cisco
- Desglosar la plataforma SecureX

Capítulo 5
Enfoque de CISCO para las herramientas de XDR

Cisco Secure adopta un enfoque único para la detección y respuesta extendida (*Extended Detection and Response*, XDR), por medio de un conjunto de herramientas patentadas, múltiples técnicas de aprendizaje automático para el análisis de datos, capacidades de automatización, que son adecuadas no solo para acelerar los tiempos de respuesta, sino también para abordar de manera proactiva los posibles problemas de seguridad, y más.

El enfoque para las herramientas de XDR de Cisco Secure se construye sobre una solución de plataforma integrada; SecureX se basa en mantener una visibilidad completa de la pila de seguridad y amplias capacidades de integración con tu infraestructura de seguridad existente. Este capítulo también analiza cómo Cisco Secure desglosa lo que debería ser una plataforma de XDR.

Los tres pilares de una plataforma de XDR efectiva

Cisco Secure considera a las herramientas de XDR como una plataforma de seguridad que falla si alguno de sus componentes no cumple sus funciones. Después de todo, el "extendido" en XDR no sirve de mucho si

no hay un poderoso conjunto de herramientas de análisis para aprovecharlo. Cada una de las tres partes principales de la plataforma de XDR tiene que trabajar en conjunto para cumplir las grandes promesas de este nuevo enfoque de la seguridad de TI. Esta sección cubrirá los tres pilares de la filosofía de XDR de Cisco Secure para comprender mejor las ideas en las que se basa SecureX.

X: Un alcance amplio

El alcance extendido de las herramientas de XDR no solo permite que los equipos de seguridad vean más y más rápido, sino que también ayuda a simplificar las pilas de seguridad modernas complejas y difíciles de manejar. La plataforma de XDR no puede trabajar sola, por lo que la compatibilidad con las soluciones de seguridad existentes es fundamental para lograr una visión completa de los recursos de seguridad.

Cisco Secure ofrece una variedad de herramientas de seguridad que se integran fácilmente a tu plataforma y cree que este debería ser el estándar. Cualquier plataforma de XDR cuyo uso se justifique debe tener amplias capacidades de integración para que las organizaciones puedan aprovechar al máximo las herramientas que ya tienen, al tiempo que se benefician de una plataforma de XDR.

Adicionalmente, una plataforma de XDR debería extraer datos de tantas fuentes como sea posible. Cualquier recurso o endpoint que tenga información que recopilar es un punto de ataque potencial y debe ser monitoreado. Una buena plataforma de XDR debe tener compatibilidad total con una sólida detección y respuesta de red (*Network Detection and Response*, NDR), y detección y respuesta de endpoints (*Endpoint Detection and Response*, EDR), lo que garantiza una visibilidad completa de todos los recursos vulnerables.

D: Análisis rápido y potente

Una parte igualmente importante de las herramientas de XDR es cómo permiten que el personal de seguridad identifique correctamente los ataques y aprenda de ellos. Hay dos componentes principales en el análisis de XDR: 1) la forma en que las herramientas existentes y las herramientas de aprendizaje automático de XDR procesan la información, y 2) la forma en que se presenta la información a los equipos de seguridad.

La complejidad de los entornos de TI actuales significa que hay una gran cantidad de datos de seguridad que requieren un contexto para comprenderlos completamente y actuar en consecuencia. Las herramientas de análisis impulsadas por el aprendizaje automático son la forma más eficiente de procesar esta cantidad de datos, y una buena solución de

XDR debe incluir potentes capacidades de aprendizaje automático para respaldar los equipos de seguridad.


RECUERDA

La legibilidad de la información de seguridad también es esencial para una solución de XDR exitosa. Incluye paneles fáciles de usar que contienen la información que necesitas, cuando la necesitas, y herramientas de visualización para analizar mejor los datos de seguridad.

La visualización debe incluir los historiales de ataques, métricas de uso, actividad de la red y la capacidad de mapear los puntos de contacto de una amenaza con tus sistemas. El análisis de XDR se trata de una identificación rápida y precisa de amenazas, para que los profesionales de seguridad puedan resolver rápidamente el problema en cuestión.

R: Reducción del tiempo de permanencia en la automatización

La automatización ha sido parte del espacio de seguridad de TI durante algún tiempo, pero las plataformas de XDR pueden llevarla a un nuevo nivel. La automatización como parte de una plataforma de XDR se beneficia con las otras fortalezas de la solución. Los planes de automatización están bien informados, tienen acceso a una pila completa de información de seguridad y se pueden administrar fácilmente por medio de un panel centralizado.


RECUERDA

Estos beneficios no solo reducen la carga de trabajo del personal de seguridad, sino que también pueden reducir el tiempo de permanencia. Las respuestas automatizadas pueden poner en marcha la respuesta al aislar los recursos comprometidos, apagar los servidores y realizar otras tareas simples. Como la plataforma de XDR tiene acceso centralizado a muchos servicios, cuando se identifica una amenaza, las tareas de automatización pueden evitar que sistemas similares sufran el mismo ataque.

Plataforma SecureX

SecureX es una experiencia de plataforma integrada y nativa de la nube dentro del portafolio de Cisco y conectada a tu infraestructura. Está integrada y abierta para su simplicidad, unificada en una ubicación para su visibilidad y maximiza la eficiencia operativa para proteger tus redes, endpoints, aplicativos y la nube. Reduce el tiempo de permanencia y las tareas impulsadas por humanos para contrarrestar los ataques y cumplir con las normas.

Integración con soluciones nuevas y existentes

Un buen producto de XDR no se puede bloquear de ciertos sistemas debido a la falta de integración de la solución. Como tal, SecureX mantiene una postura abierta hacia otros productos de seguridad que tienen API RESTful abiertas y sólidas, muchas de ellas integrales para aprovechar todo el potencial de las soluciones de XDR.

Una respuesta de seguridad integral necesita información de los servicios de identidad y autorización, herramientas de seguridad de correo electrónico, soluciones de detección de endpoints, redes y más. Muchas soluciones de seguridad existentes que ya están en tu caja de herramientas serán compatibles con SecureX.

Cisco Secure tiene muchas soluciones de seguridad disponibles que se integran fácilmente con SecureX. Dos herramientas destacadas son su detección y respuesta de red (NDR) Cisco Secure Network Analytics y las soluciones Cisco Secure Endpoint de detección y respuesta de endpoints (EDR). Las soluciones fuertes de EDR y NDR son parte esencial de una plataforma de XDR exitosa.

Más allá de eso, SecureX se integra con el grupo de inteligencia de amenazas de Cisco, Talos. Talos proporciona una visión integral de las amenazas actuales y emergentes. Esta inteligencia de seguridad se puede aprovechar de manera efectiva en tu propio ecosistema de seguridad, ampliando aún más el alcance ya amplio de SecureX.

Panel centralizado

SecureX ofrece un panel fácil de leer que se puede personalizar para adaptarse a las necesidades específicas de cualquier equipo. Cisco lo divide en un diseño de tres partes:

- Una lista desplegable de productos de seguridad a la izquierda para acceder rápidamente a una herramienta específica
- Una vista grande y centralizada de métricas de amenazas y datos de análisis en el centro
- Una fuente de noticias que mantiene a los equipos actualizados sobre los nuevos desarrollos en el panorama de la seguridad

RECUERDA

Es uno de los componentes principales de las herramientas de XDR que permite al personal de seguridad identificar y responder rápidamente a las amenazas. Las vistas centralizadas de un ecosistema de seguridad pueden ayudar a reducir la fatiga de las alertas y la sobrecarga de información, y también reducir los falsos positivos al proporcionar información clara y precisa a los equipos de seguridad.

Detección y respuesta ante amenazas

Cuando se combinan con las capacidades de detección de los productos Cisco Secure, las características de respuesta y detección de amenazas de SecureX incluyen un enfoque de varias capas para el análisis mediante aprendizaje automático. Varios motores de aprendizaje automático, incluidos los supervisados, no supervisados, estadísticos y de comportamiento, hacen que las alertas y la identificación sean rápidas. Estos motores comparan el comportamiento de las amenazas con el conocimiento de seguridad existente para ayudar en la clasificación y poner en marcha un plan de respuesta.

La información de seguridad recibe contexto dentro del ecosistema más grande, y los equipos pueden ver las correlaciones entre los recursos y los sistemas afectados. SecureX se beneficia enormemente de la telemetría recopilada de la gran base de clientes de Cisco en este sentido. Cisco Secure aprovecha una red global de inteligencia de amenazas que puede identificar amenazas e identificar rápidamente instancias futuras de esa amenaza en su base de clientes. Los potentes análisis, la vista centralizada, la amplia inteligencia de amenazas y el fácil acceso a los recursos de seguridad significan que los tiempos de respuesta pueden reducirse y los equipos de seguridad tienen espacio para tomar decisiones más informadas sobre cómo responder.

Orquestación

SecureX contiene flujos de trabajo de orquestación seleccionados para la búsqueda de amenazas, la gestión de vulnerabilidades y la optimización del tráfico. Estos flujos no son fijos, pero pueden usarse como modelos para planes que se adapten a las necesidades de tu organización.

SecureX cuenta con una interfaz para arrastrar y soltar que permite crear flujos de trabajo personalizados. Las respuestas, aprobaciones y acciones automatizadas se pueden combinar en un libro de estrategias de respuesta para aumentar los tiempos de respuesta para futuras amenazas de seguridad.

Capítulo 6
Diez cosas que recordar sobre las herramientas de XDR

En este capítulo, se analizan algunas de las principales conclusiones de este libro y se destacan las características clave que se deben buscar en las soluciones de detección y respuesta extendida (*Extended Detection and Response*, XDR) y en las plataformas de seguridad integrales como SecureX.

Reducir el tiempo de detección y respuesta

En definitiva, las plataformas de XDR tienen como objetivo reducir los tiempos de detección y respuesta. Más datos y más herramientas no significan equipos de seguridad más rápidos. Con frecuencia, significan equipos de seguridad sobrecargados. Las herramientas de XDR se enfocan en proporcionar información procesable mediante análisis respaldados por aprendizaje automático y un panel centralizado. En el lado de la respuesta, las funciones de orquestación y automatización agilizan el proceso de respuesta al proporcionar herramientas personalizables y fáciles de usar para el personal de seguridad.

Visualizar datos de seguridad integrados

La plataforma de XDR recibe una gran cantidad de información y debe organizarla para reducir la fatiga de las alertas, los falsos positivos y las molestias generales de las operaciones de seguridad. Los paneles centrales son centros de información personalizables para que los equipos de seguridad organicen sus datos para adaptarse a las necesidades de la organización. Las herramientas de visualización, como los mapas de incidentes, deberían ayudar a identificar las fuentes de amenazas y rastrear puntos de ataque potencialmente nuevos.

Monitoreo preciso

Como las plataformas de XDR por lo general ofrecen análisis basados en aprendizaje automático y dependen de herramientas de seguridad secundarias para la recopilación de datos, los equipos de seguridad deben tener una visión clara del ecosistema de una organización. Brindar buena información, sobre mucha información, limpia lo que el personal realmente ve, lo que hace más fácil enfocarse en preocupaciones legítimas de seguridad.

Contextualizar las alertas y reducir los falsos positivos

Las características del panel centralizado de XDR brindan contexto a las situaciones de seguridad. Las alertas que llegan son más confiables, porque el sistema de XDR tiene la inteligencia de amenazas relevante necesaria para tomar decisiones sobre qué es un comportamiento anormal y qué no.

Los falsos positivos son una pérdida de recursos y la visión integral que tienen las herramientas de XDR sobre la infraestructura de TI ayuda a reducir su frecuencia.

Respuestas automatizadas

Las características de la automatización han existido en el espacio de la seguridad por un tiempo, pero el amplio alcance de las herramientas de XDR permite que sus herramientas de automatización se beneficien con algunos ajustes. Muchos productos de XDR ofrecen automatización basada en el aprendizaje automático que puede encargarse de las tareas de seguridad rutinarias, de modo que el personal de seguridad pueda ocuparse de los trabajos más difíciles que necesitan la intervención humana.

Apertura

Las herramientas de XDR no trabajan de manera independiente y requieren el apoyo de herramientas de seguridad especializadas. Las plataformas de XDR ofrecen muchas opciones de integración, con las herramientas de seguridad existentes y con las que se agreguen en el futuro.

CONSEJO

La EDR y la NDR en particular son dos herramientas a tener en cuenta al desarrollar tu infraestructura de seguridad.

Almacenar y analizar registros a escala

Debido a las poderosas herramientas de análisis que ofrecen las soluciones de XDR, estas plataformas pueden procesar grandes cantidades de datos de seguridad. Las soluciones de XDR son fáciles de escalar para que tu organización pueda crecer con el tiempo, sin preocuparte sobre cómo tendrán que cambiar tus análisis de seguridad.

Abordar los requisitos de cumplimiento

La gran cantidad de datos que pueden procesar las soluciones de XDR también significa que se pueden cumplir con confianza los requisitos normativos y de cumplimiento de la industria.

RECUERDA

Las organizaciones que participan en la atención médica o las finanzas necesitan especialmente herramientas amplias de registro y análisis.

Las soluciones en silo son soluciones parciales

La infraestructura de seguridad se ha vuelto tan generalizada que los sistemas de silos se han vuelto comunes. La infraestructura de TI de nivel corporativo no puede depender de esta separación de sistemas, pues los atacantes se expanden y desarrollan sus estrategias de ataque. La información de seguridad incompleta puede generar falsos positivos y la fatiga de las alertas, pues las herramientas de monitoreo no tendrán el contexto completo de la actividad sospechosa.

Recordar los factores humanos

El personal de seguridad que administra estas herramientas es la parte más importante de cualquier entorno de seguridad de TI exitoso. Las soluciones de seguridad ineficientes sobrecargan al personal de seguridad con amenazas falsas positivas, alertas innecesarias que provocan la fatiga de las alertas, y herramientas de identificación y respuesta mediocres que afectan su rendimiento.

Experience Simplified

The Cisco SecureX platform is a built-in experience within our security portfolio that connects with your entire security infrastructure.

Learn how **Cisco's XDR platform approach can elevate your security goals.**

¡Obtén un punto de vista centralizado de tu infraestructura de seguridad!

El objetivo principal de las plataformas de XDR es reducir los tiempos de detección y respuesta, minimizar la fatiga de las alertas y agregar contexto a las alertas legítimas. Las herramientas de XDR se enfocan en proporcionar inteligencia sobre amenazas mediante análisis respaldados por aprendizaje automático y un panel centralizado que permite actuar sobre las amenazas con confianza. Las funciones de orquestación y automatización agilizan el proceso de respuesta al proporcionar herramientas personalizables y fáciles de usar para el personal de seguridad.

Dentro...

- Cómo han evolucionado las amenazas de seguridad
- Herramientas y técnicas modernas de seguridad
- Desglose de XDR
- Cómo las soluciones en silos crean obstáculos
- Superar los problemas que enfrentan las operaciones de seguridad corporativa
- Consolidación del análisis de detección
- Remediación de investigaciones

James Sullivan es un escritor de tecnología que reside en Portland, Oregón. Su trabajo se concentra en la seguridad en la nube, la IoT y las soluciones de bases de datos en la nube. James disfruta de los podcasts de ficción de terror, los juegos de mesa y el estudio de los patrones lingüísticos del maullido frenético de su gato.

ISBN: 978-1-394-15626-9
Not For Resale

para dummies®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.