XDR

Más grande, más rápido, mejor

El potencial de innovación de XDR

kaspersky bring on the future

¿Para quién es XDR?

XDR es para organizaciones que tengan una posición de seguridad madura y que necesiten una plataforma única que les brinde una visión completa y coherente de lo que ocurre en toda su infraestructura.

¿Un cambio de paradigma o una solución más para un problema específico?

XDR: detección y respuesta extendidas

Es una sigla que está de moda, pero, como todas las tecnologías relativamente nuevas, no todo el mundo está seguro de qué significa o qué puede hacer para su organización. Sin embargo, de lo que no hay duda es que XDR marca un cambio estratégico desde la reactividad hacia la proactividad, ya que la doctrina del 'espera y verás' es insuficiente en la ciberseguridad. Lo correcto es considerar a XDR como una estrategia, en lugar de solo como un producto.

Entonces, ¿supone XDR un potencial cambio de paradigma o es solo una solución más para un problema tecnológico específico? Los problemas a los que se enfrenta el sector son reales y multifacéticos, incluyendo desde la falta global de trabajadores capacitados, los equipos de seguridad de TI sobrecargados y un panorama de amenazas en constante evolución, hasta el exceso de alertas, la disparidad en las herramientas disponibles, la deficiente inteligencia de amenazas y la ampliación de la superficie de ataque. IDC sostiene que XDR será una "fuerza disruptiva, que impactará en las ventas de SIEM, EDR, SOAR, inteligencia de red y plataformas de análisis de amenazas, así como de proveedores de inteligencia de amenazas externas"[1], y Forrester cree que la tecnología de XDR diferenciada "reemplazará la detección y respuesta en endpoints (EDR) en el corto plazo y usurpará el lugar de SIEM en el largo plazo"[2].

XDR será una fuerza disruptiva — IDC

Más dispositivos, más aplicaciones, más tráfico de red, más datos, más amenazas...

¿Para quién es XDR y qué desafíos puede resolver?

XDR es para organizaciones que tengan una posición de seguridad madura y que necesiten una plataforma única que les brinde una visión completa y coherente de lo que ocurre en toda su infraestructura.

Los desafíos de ciberseguridad que estas organizaciones enfrentan son coherentes y están establecidos. ESG Research realizó una encuesta a profesionales de ciberseguridad y TI[3] en organizaciones con 100 o más empleados, encontrando que más del 80% de las respuestas provenían de empresas de diversas verticales industriales. Estas son algunas de las conclusiones clave:

Dificultades a la hora de mantenerse al día con los requisitos operativos de las tecnologías de SOC

Administrar las operaciones de seguridad es más difícil ahora que en cualquier otro momento de los últimos dos años, debido a las dificultades para mantenerse al día con las necesidades operativas de las tecnologías de SOC: escalabilidad en la segmentación de datos, equilibrio de carga en motores de procesamiento, adición de capacidad de almacenamiento, etc.

[1] Fuente: IDC, Global Security Products Analysis: From Power Point to Power Product, Where Is XDR Right Now? 2022

[2] Fuente: Forrester, Extended Detection and Response (XDR) — A Battle Between Precedent and Innovation, Allie Mellen, Senior Analyst, 2021

[3] Fuente: ESG Research Report, SOC Modernization and the Role of XDR, 2022

El crecimiento y los cambios constantes de la superficie de ataque y el panorama de amenazas en general

Más dispositivos, más aplicaciones, más tráfico de red, más datos, más amenazas. El panorama de amenazas no se queda quieto y las ciberamenazas evolucionan todo el tiempo en volumen y complejidad a medida que las nuevas herramientas se multiplican. Paralelamente, el acceso a recursos para llevar a cabo ataques nunca ha sido tan fácil como ahora; en un extremo del espectro, tenemos a actores poco calificados que adquieren herramientas de hacking a bajo costo en la web oscura, y en el otro, a hackers metódicos y altamente capacitados que construyen ataques avanzados y meticulosos. Además, no podemos perder de vista las amenazas internas y las vulnerabilidades que emergen dentro de la cadena de suministro.

La gran cantidad de procesos manuales necesarios para administrar la seguridad

Hay más datos de seguridad para recopilar y procesar, y el procesamiento manual es ineficiente y poco efectivo. Esto crea una tormenta perfecta que impacta en la escalabilidad, genera una sobredependencia en la participación humana directa y disminuye la eficacia a la hora de enfrentar amenazas en general.

Una incompetencia para desarrollar reglas de detección

La incapacidad para formular reglas de detección efectivas, afinar los controles de seguridad y responder a las amenazas de forma rápida y eficaz se debe a la escasez de tiempo, recursos y capacidad técnica adecuada. Las organizaciones no siempre tienen la capacidad o el personal adecuado para estar a la altura del análisis y las operaciones de seguridad. Lo que nos lleva al siguiente problema.

La auténtica falta global de talento

A pesar de que el número de profesionales de ciberseguridad a nivel global nunca fue tan alto, con 4.7 millones de especialistas, aún hay una brecha de 3.4 millones que debe cubrirse (y no se está haciendo). Esta brecha está creciendo dos veces más rápido que la fuerza laboral, con un aumento interanual del 26.2 %.[4]

[4] Fuente: (ISC)², Cybersecurity Workforce Study, 2022

Las herramientas existentes suelen tener problemas

para detectar e investigar amenazas avanzadas, y aun así, se necesitan conocimientos especializados para utilizarlas y administrarlas.

88%

de las organizaciones gastará más dinero este año en mejoras de las operaciones de seguridad

66%

afirma que la consolidación de herramientas es una prioridad

Herramientas que no se ajustan a su propósito

Cuando las mismas herramientas se convierten en parte del problema, algo debe cambiar. Las herramientas existentes suelen tener problemas para detectar e investigar amenazas avanzadas, pero aun así, se necesitan conocimientos especializados para utilizarlas y administrarlas. Las investigaciones[5] muestran que las herramientas actuales suelen ser poco efectivas al correlacionar alertas, y el personal de seguridad de TI tiene dificultades para trabajar con herramientas diferentes y desconectadas que manejan datos dispares. Esto resulta insuficiente, incómodo, confuso y costoso. Además, las herramientas de seguridad disponibles actualmente no escalan adecuadamente frente a la creciente superficie de ataque, lo que resulta en notorias deficiencias en la capacidad de detectar y responder a las amenazas en la nube.[6]

¿Es de extrañar que su CISO se vea estresado?

La buena noticia es que la optimización de las operaciones de seguridad se ha convertido en una prioridad financiada, con el 88% de las organizaciones aumentando su presupuesto este año. Además, un 66% considera esencial la consolidación de herramientas. Al mismo tiempo, el ritmo acelerado del desarrollo y lanzamiento de aplicaciones modernas está impulsando la demanda de nuevas habilidades.[7]

¿Qué hace XDR?

A continuación, explicamos cómo XDR puede superar estos desafíos.

XDR detecta mejor las amenazas avanzadas

Las capacidades de detección de amenazas de XDR funcionan en endpoints, redes y entornos en la nube. Utiliza algoritmos de aprendizaje automático y análisis de comportamiento para identificar amenazas sofisticadas, incluido el malware, el ransomware y las amenazas avanzadas persistentes (APT).

Acciones de respuesta y corrección automatizadas

XDR automatiza las acciones de respuesta y corrección, lo que permite que las organizaciones contengan amenazas de manera rápida y minimicen cualquier daño potencial. Puede aislar o colocar en cuarentena endpoints en riesgo, bloquear actividades maliciosas y solucionar vulnerabilidades para reducir el esfuerzo manual y el tiempo de respuesta, todo de manera automática.

Se integra con herramientas de protección de endpoints

La integración con EPP es un problema clave, y XDR aprovecha la telemetría avanzada de endpoints y el análisis de comportamiento para proporcionar conocimientos profundos sobre actividades de endpoints. Utiliza algoritmos avanzados de aprendizaje automático para identificar comportamientos sospechosos e indicadores de ataque (IOA), lo que posibilita la detección temprana de amenazas sofisticadas.

[5] Fuente: ESG Research Report, SOC Modernization and the Role of XDR, mayo de 2022

[6] Fuente: ESG Research Report, SOC Modernization and the Role of XDR, 2022

[7] Fuente: ESG Research Report, SOC Modernization and the Role of XDR, mayo de 2022

¿Qué lugar ocupa XDR en el ecosistema de EDR, MDR, SOAR y SIEM?

La clave está en la X de Extendido. XDR extiende las capacidades ofrecidas por EDR para detectar amenazas complejas de manera proactiva en múltiples niveles de infraestructura y responder automáticamente a estas amenazas.

Un enfoque integrado resulta fundamental

Al integrar múltiples herramientas y aplicaciones de seguridad, y supervisar datos en endpoints, redes, nubes, servidores web, servidores de correo electrónico y más, XDR va más allá en la detección y eliminación de amenazas, al tiempo que simplifica la administración de la seguridad de la información mediante la automatización de la interacción entre productos.

Forrester cree que, en la mayoría de los casos, XDR no reemplazará las plataformas de análisis de seguridad completamente, al afirmar que "XDR está en evolución y esperamos que las plataformas de análisis de seguridad y XDR colisionen en los próximos cinco años".

SIEM tiene casos de uso que van más allá de la detección de amenazas, y la personalización de SOAR es útil, pero, cuando se trata de detectar y responder a amenazas, el análisis avanzado de la protección mejorada de XDR no tiene comparación.

Ofrece visibilidad en tiempo real

XDR brinda visibilidad en tiempo real de la posición de seguridad de la organización. Recopila y analiza datos de diferentes fuentes, como endpoints, servidores, firewalls y plataformas en la nube, para proporcionar información integral de amenazas y actividades sospechosas en una consola única. Esta capacidad integral permite una actitud verdaderamente proactiva, caracterizada por la búsqueda anticipada de amenazas y respuestas más ágiles a los incidentes. Al ofrecer una perspectiva holística, XDR facilita a los equipos de seguridad la detección eficiente de actividades anómalas y la previsión de incidentes de seguridad.

Contextualiza datos e inteligencia de amenazas

Cuando utiliza inteligencia de amenazas de alta calidad y una base de datos de inteligencia de amenazas integral, XDR brinda información contextual muy útil acerca de amenazas y atacantes. Esta inteligencia de amenazas enriquecida no solo simplifica la investigación de alertas y el manejo de incidentes, sino que también capacita a los equipos de seguridad con un entendimiento más profundo de las tácticas, técnicas y motivaciones de los actores de amenazas. Este conocimiento facilita la implementación de medidas de defensa proactivas y una respuesta a incidentes significativamente más efectiva.

Permite operaciones de seguridad simplificadas

Si se integran correctamente, las mejores soluciones se adaptarán sin esfuerzo a su infraestructura actual para ofrecer los mejores resultados de la automatización y brindar una visibilidad y un conocimiento plenos sin tener que reemplazar las soluciones de seguridad de terceros que ya se encuentran en uso. No olvide que, al brindar una visión integral de los incidentes de seguridad y del comportamiento de los usuarios, la integración respalda el cumplimiento.

Es claro que XDR puede cumplir con las expectativas: brindar control, estabilidad y esa ventaja tan importante. Sin embargo, no todas las ofertas de XDR son iguales. ¿Cómo puede elegir la que sea adecuada para su organización?

Hay 5 aspectos a considerar cuando se comparan proveedores y soluciones de XDR

A continuación, explicamos cómo XDR puede superar estos desafíos.

1

Existe un vínculo directo entre la calidad de una solución de XDR y la sinergia entre EPP y EDR de un proveedor

Una solución de EDR para la detección y respuesta avanzadas de ciberamenazas sofisticadas al nivel de los endpoints es un elemento clave para XDR. Al mismo tiempo, EDR necesita una plataforma de protección de endpoints (EPP) sólida para filtrar grandes cantidades de amenazas masivas de manera automática. Es importante considerar con atención las características de protección de endpoints y verificar que se admitan todos los tipos de endpoints: PC, equipos portátiles, máquinas virtuales, dispositivos móviles y diferentes sistemas operativos.

2

Contar con inteligencia actualizada y una visión completa de las tácticas y técnicas de los ciberdelincuentes es esencial para contrarrestar las ciberamenazas

Es bastante simple: cualquier solución de XDR que valga la pena ofrecerá estas dos capacidades, junto con contexto adicional para mejorar y acelerar la investigación y respuesta a incidentes.

3

La integración con soluciones de terceros es más sostenible y rentable

Otro problema crucial es qué tan bien se integra una solución de XDR con productos de terceros ya que la interoperabilidad hace que la inversión sea más sostenible desde el primer momento. Una solución de XDR que ofrezca numerosas opciones de integración genuinas recopilará más fuentes de datos y brindará una imagen más completa de la situación de la infraestructura.

4

Las reseñas independientes, el reconocimiento global y los resultados en pruebas independientes son importantes

Cuando invierte en algo tan importante para su empresa como la ciberseguridad, no se deben pasar por alto las evaluaciones independientes. Solicite los resultados en pruebas independientes. Busque el reconocimiento internacional de medios como Forrester, IDC y otros. ¿Se implementan las soluciones en todo el mundo? Solicite casos de estudio.

5

¿Está su inversión preparada para el futuro?

La tecnología no suele quedarse quieta, en especial para algo como XDR, que es relativamente nuevo; debería ver cuál es el plan futuro del proveedor y cómo se corresponde al desarrollo constante de su organización.

¿Por qué Kaspersky?

La más probada. La más premiada. La protección Kaspersky.

Kaspersky es una empresa de ciberseguridad global establecida con una sólida trayectoria en seguridad. Hace más de 25 años que protegemos a organizaciones de todo el mundo; recibimos incontables premios y galardones por nuestros productos y servicios. Entre 2013 y 2022, los productos de Kaspersky:

587

alcanzaron 587 primeros puestos

685

quedaron entre los tres primeros puestos

827

participaron en 827 pruebas y revisiones independientes

En 2023, Kaspersky recibió la mención de Empresa líder en el mercado de soluciones de XDR por parte de la empresa global de asesoría e investigación de tecnología ISG. ISG define empresas "líderes" como aquellas que tienen una oferta integral de productos y servicios y que representan una fortaleza innovadora y estabilidad competitiva.

Más información

https://latam.kaspersky.com

#kaspersky
#bringonthefuture