Kaspersky Next XDR Expert

Más grande, más rápido, mejor

kaspersky

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

¿Para quién es XDR?

XDR es para organizaciones que tengan una postura 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.

XDR: Detección y respuesta extendidas

Es un acrónimo 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. Algo es seguro: XDR involucra un giro estratégico desde la reactividad a la proactividad, porque la doctrina del "espera y verás" no sirve en la ciberseguridad. Lo correcto es considerar a XDR como una estrategia, en lugar de solo como un producto.

Entonces, ¿XDR supone un potencial cambio de paradigma o es solo una solución más para un problema tecnológico específico? Sin dudas, estos problemas existen, desde la falta global de trabajadores capacitados, los equipos de seguridad saturados y un panorama de amenazas que nunca se detiene, hasta el exceso de alertas, la disparidad en herramientas, la mala inteligencia de amenazas y la expansión 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 externa de amenazas"[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 postura 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, más del 80 % en empresas, a través de varias verticales. Estos 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 punto 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: Informe de ESG sobre el papel de XDR en la Modernización de los SOC, 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. Al mismo tiempo, la barrera de entrada para hackers nunca fue tan baja, con compradores de amenazas empaquetadas económicas de bajos conocimientos a un extremo del espectro y hackers pacientes y altamente cualificados que desarrollan ataques complejos en el otro extremo. Sin olvidar las amenazas internas y las vulnerabilidades en 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 sobre la escalabilidad, genera una sobredependencia en la participación humana directa y disminuye la eficacia a la hora de enfrentar amenazas en general.

Una incapacidad de desarrollar reglas de detección

Una incapacidad de desarrollar reglas de detección, ajustar los controles de seguridad e identificar y abordar amenazas de manera rápida y eficiente, debido a una falta de tiempo, recursos y capacidad. 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 de 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.

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 manipulan datos dispares. Esto resulta insuficiente, incómodo, confuso y costoso. Otro desafío es que las herramientas actuales no escalan para abordar la expansión de la superficie de ataque, y hay grandes brechas en las capacidades de detección y respuesta en la nube.[6]

No es sorprendente que su CISO se vea estresado.

La buena noticia es que la mejora de las operaciones de seguridad es una prioridad, y recibe financiamiento: el 88 % de las organizaciones gastará más este año, el 66 % afirma que la consolidación de las herramientas es una prioridad y el desarrollo y despliegue de aplicaciones modernas incrementó la velocidad, lo que requiere mayores conocimientos.[7]

88 %

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

66 %

afirma que la consolidación de herramientas es una prioridad

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 de 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 automáticamente a endpoints vulnerados, bloquea actividades maliciosas y soluciona vulnerabilidades para reducir el esfuerzo manual y el tiempo de respuesta.

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 en 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: Informe de ESG sobre el papel de XDR en la Modernización de los SOC, mayo de 2022

[6] Fuente: Informe de ESG sobre el papel de XDR en la Modernización de los SOC, 2022

[7] Fuente: Informe de ESG sobre el papel de XDR en la Modernización de los SOC, mayo de 2022

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

La clave está en la X: extendido. XDR extiende las capacidades ofrecidas por EDR para detectar amenazas complejas de manera proactiva en múltiples niveles de la infraestructura, y responder y contrarrestar automáticamente 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, mientras que al mismo tiempo simplifica la administración de la seguridad de la información al automatizar la integración entre productos.

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

SIEM tiene casos de uso 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 postura de seguridad de la organización. Recopila y analiza datos de diferentes fuentes, como endpoints, servidores, firewalls y plataformas en la nube, para proporcionar información exhaustiva de amenazas y actividades sospechosas en una consola única. Esto lo hace realmente proactivo: búsqueda de amenazas proactiva y respuestas a incidentes más rápidas. Una visión holística ayuda a los equipos de seguridad a identificar actividades sospechosas e incidentes de seguridad potenciales de manera más eficiente.

Contextualiza datos e inteligencia de amenazas

Cuando utiliza inteligencia de amenazas de alta calidad y una base de datos de inteligencia de amenazas exhaustiva, XDR brinda información contextual muy útil acerca de amenazas y atacantes. Esta inteligencia de amenazas enriquecida simplifica la investigación de alertas y el manejo de incidentes, y ayuda a los equipos de seguridad a entender las tácticas, técnicas y motivaciones de los actores de amenazas, posibilitando medidas de defensa proactiva y respuesta a incidentes más efectivas.

Permite operaciones de seguridad simplificadas

Cuando se integran de forma adecuada, las mejores soluciones se encajan en la infraestructura actual sin problemas para ofrecer los mejores resultados de la automatización, y brindan una visibilidad y concientización completas sin tener que reemplazar las soluciones de seguridad de terceros que ya se encuentran en uso. Y no olvide que, al brindar una visión exhaustiva de los incidentes de seguridad y el comportamiento de los usuarios, la integración respalda el cumplimiento.

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

Hay cinco 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 las EPP y la 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) robusta, 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 endpoint: PC, equipos portátiles, máquinas virtuales, dispositivos móviles y diferentes sistemas operativos.

2

Contar con inteligencia de amenazas 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 importan

Al invertir en algo tan importante con la ciberseguridad de tu empresa, no se deben pasar por alto las evaluaciones independientes. Solicita los resultados en pruebas independientes. Busca el reconocimiento internacional de medios como Forrester, IDC y otros. ¿Las soluciones se implementan en todo el mundo? Solicita casos de estudio.

5

¿La solución tendrá vigencia en el futuro?

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

¿Por qué Kaspersky?

La más probada. La más premiada. Protección de Kaspersky.

Kaspersky es una empresa de ciberseguridad global establecida, con un fuerte historial de experiencia en seguridad. Hemos estado protegiendo a organizaciones de todo el mundo durante más de 25 años y hemos recibido 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 una estabilidad competitiva.

Más información

Kaspersky Extended Detection and Response

Más información

www.kaspersky.es

#kaspersky
#bringonthefuture