Kaspersky Next XDR Expert

Más grande, más rápido y mejor

kaspersky

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

¿Para quién es XDR?

XDR está diseñado para organizaciones con un alto nivel de madurez en seguridad que requieran una plataforma única capaz de proporcionar una visión integral y coherente de todas las actividades en su infraestructura.

XDR: detección y respuesta extendida

Es una sigla que está de moda, pero, como sucede con todas las tecnologías relativamente nuevas, no todo el mundo está seguro de lo que significa o lo que puede hacer por su organización. Solo una cosa sí es segura: el XDR proporciona una transformación estratégica que permite avanzar de la reactividad a la proactividad, dejando atrás la doctrina del 'esperar y ver' que carece de eficacia en el campo de 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 en específico? Sin duda alguna, la falta de trabajadores capacitados a nivel global, la sobrecarga en los equipos de seguridad IT y un constante panorama de amenazas sin tregua, junto con la avalancha de alertas, la disparidad en herramientas, la falta de inteligencia de amenazas efectiva y el aumento en los ciberataques, son problemas palpables que no se pueden ocultar. No obstante, en medio de estos desafíos, 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], mientras que 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 está diseñado para organizaciones con un alto nivel de madurez en seguridad que requieran una plataforma única capaz de proporcionar una visión integral y coherente de todas las actividades en su infraestructura.

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

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

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.

El continuo crecimiento y evolución de la superficie de ataque y del panorama de amenazas en su conjunto

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. De manera simultánea, la barrera de entrada para los hackers nunca ha sido tan baja. En un extremo del espectro, encontramos a compradores poco calificados que adquieren económicos paquetes de amenazas en la web oscura, mientras que en el otro extremo, nos enfrentamos a hackers pacientes y altamente capacitados que desarrollan ataques más complejos. Sin olvidar las amenazas internas y las vulnerabilidades en la cadena de suministro que se puedan presentar.

La gestión de la seguridad requiere una cantidad considerable de procesos manuales.

Con el aumento en la cantidad de datos de seguridad para recopilar y procesar, el enfoque manual se vuelve ineficiente e ineficaz. 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

Una incompetencia para desarrollar reglas de detección, ajustar los controles de seguridad e identificar y abordar amenazas de manera rápida y eficiente, debido a la 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 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.

Herramientas que no se ajustan a su propósito

Cuando las mismas herramientas se convierten en parte del problema, algo tiene que cambiar. Las herramientas existentes suelen tener problemas para detectar e investigar amenazas avanzadas, y 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 IT tiene dificultades para trabajar con herramientas diferentes y desconectadas que manejan datos dispares. Esto resulta insuficiente, incómodo, confuso y costoso. Otro desafío es que las herramientas actuales no se adaptan a la creciente superficie de ataque y hay grandes brechas en las capacidades de detección y respuesta en la nube.[6]

¿Es de extrañar que su CISO se vea estresado?

La buena noticia es que la mejora de las operaciones de seguridad es una prioridad y recibirá financiamiento: un 88 % de las organizaciones planea invertir más este año. Además, un 66 % afirma que la consolidación de herramientas es una de sus principales prioridades, y el desarrollo y despliegue de aplicaciones modernas ha acelerado el ritmo, lo que demanda la adquisición de nuevas habilidades.[7]

88%

de las organizaciones gastará más dinero este año en mejorar sus operaciones de ciberseguridad

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 en la nube. Utiliza algoritmos de aprendizaje automático y análisis de comportamiento para identificar amenazas sofisticadas, como malware, ransomware y amenazas avanzadas persistentes (APT).

Acciones automatizadas de respuesta y remediación

XDR automatiza las acciones de respuesta y remediación, 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.

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

[6] Fuente: Informe de ESG sobre el papel de XDR en la Modernización de los SOC, 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 XDR que se utiliza como referencia a la palabra extendido. XDR extiende las capacidades ofrecidas por EDR para detectar amenazas complejas de manera proactiva en múltiples niveles de infraestructura, para así 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, 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".

Si bien SIEM tiene casos de uso que van más allá de la detección de amenazas y la personalización de SOAR puede ser útil, en lo que respecta a la detección y respuesta de amenazas, el análisis avanzado y la protección mejorada de XDR son incomparables.

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.

Ofrece visibilidad en tiempo real

XDR brinda visibilidad en tiempo real del estado 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. Esto la convierte en una solución verdaderamente proactiva, con la capacidad de detectar amenazas de forma anticipada y responder a incidentes de manera más rápida. 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

Mediante el uso de una inteligencia de amenazas de alta calidad y una base de datos extensa, XDR proporciona una información contextual muy valiosa sobre las amenazas y los atacantes. Esta inteligencia de amenazas mejorada simplifica la investigación de alertas y la gestión de incidentes, al mismo tiempo que ayuda a los equipos de seguridad a comprender las tácticas, técnicas y motivaciones de los actores de amenazas. Esto permite una defensa proactiva y una respuesta a incidentes más eficaz.

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 automatización y brindar una visibilidad y un conocimiento pleno sin tener que reemplazar las soluciones de seguridad de terceros que ya se encuentran en uso. Además, es importante recordar que la integración respalda el cumplimiento al proporcionar una visión completa de los incidentes de seguridad y el comportamiento de los usuarios.

Está claro que XDR puede proporcionar lo que promete: control, estabilidad y esa ventaja crítica. Sin embargo, no todas las ofertas de XDR son iguales. ¿Cómo puede elegir la más 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 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

La integración efectiva de una solución XDR con terceros es otro aspecto de suma importancia, ya que la interoperabilidad convierte la inversión en una opción más sostenible desde el inicio. 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

Kaspersky Extended Detection and Response

Más información

latam.kaspersky.com

#kaspersky
#bringonthefuture