

EXACTAMENTE, ¿QUÉ ES XDR?

La detección y respuesta extendidas (XDR) es la próxima frontera para detener las amenazas sofisticadas actuales.

Se trata de un enfoque holístico que simplifica la ingestión de datos de seguridad, el análisis y los flujos de trabajo en todas las capas de seguridad de una organización.



Extendidas

Impulse su detección y respuesta para endpoints (EDR) con telemetría global obtenida e integrada en todas sus capas de seguridad completa.



Detección

Identifique y cace las amenazas más rápidamente con indicadores de ataque de distintas plataformas y con datos y alertas, dentro de una consola unificada.



Respuesta

Transforme la información de XDR en medidas orquestadas, y diseñe y automatice flujos de trabajo de respuesta multiplataforma para aplicar una corrección quirúrgica y optimizada.

¿POR QUÉ XDR AHORA?

Los datos de seguridad y sistemas aislados crean ángulos muertos importantes

45

el número de herramientas de ciberseguridad que se despliegan de media en las redes empresariales¹

Los equipos de seguridad deben responder con rapidez y agilidad a las amenazas actuales

92

minutos que tardan los atacantes en desplazarse lateralmente tras el acceso inicial²

Maximice el valor de su tecnología actual para reducir el riesgo

59 %

de los responsables de la toma de decisiones a nivel mundial manifiestan haber sufrido al menos una brecha de seguridad de los datos en sus empresas el último año³

COMPRE XDR VERDADERA

Muchos proveedores intentarán venderle XDR que no lo es realmente

ESTO NO ES XDR:

- ✗ NDR ≠ XDR
- ✗ SOAR ≠ XDR
- ✗ SIEM ≠ XDR
- ✗ NDR + SOAR + SIEM ≠ XDR

¡ESTO SÍ QUE ES XDR!



DETECCIÓN MÁS RÁPIDA, MUY FIABLE

Amplíe las tecnologías de protección a fuentes de datos externas para disfrutar de detección, investigación y caza en toda la superficie de ataque con total fiabilidad.



UN EXCELENTE ECOSISTEMA

Unifique telemetría relevante procedente de varias tecnologías y dominios para agilizar la respuesta a las amenazas, donde quiera que ocurran.



REDUCCIÓN DEL COSTE TOTAL DE PROPIEDAD

Incremente el valor de todas sus capas de seguridad consiguiendo que funcionen juntas en la pila.



RESPUESTA OPTIMIZADA

Permita que sus equipos de seguridad diseñen y automaticen flujos de trabajo de respuesta multiplataforma y multifase para la corrección quirúrgica y de pila completa.



OPERACIONES DE SEGURIDAD MÁS EFICIENTES

Correlacione los datos de distintas fuentes de manera inteligente, rápidamente y a escala, para proporcionar información de seguridad práctica desde una sola consola.

¿PREPARADO PARA LA VERDADERA XDR?

Empiece por la lista de verificación de XDR:



¿Tiene la solución funciones de **detección y respuesta para endpoints**?



¿Ofrece **información e inteligencia sobre amenazas** unificadas, para una detección precisa y una respuesta optimizada?



¿Ofrece **detección automática** en entornos de TI, cargas de trabajo de la nube, redes, correo electrónico y endpoints para **reducir el tiempo de filtrado y agilizar la respuesta**?



¿Incluye **integraciones basadas en la nube** para ingerir registros y eventos procedentes de múltiples fuentes de datos y de terceros?



¿Cuenta con una **alianza de partners estratégicos** con proveedores de soluciones líderes de la industria?

"EL FUNDAMENTO DE UNA BUENA XDR ES UNA BUENA EDR"³

— Informe de Forrester: Adapt Or Die: XDR Is On A Collision Course With SIEM And SOAR —

La solución definitiva para la detección, investigación, caza y respuesta unificada, en distintas plataformas.

FALCON XDR

Más allá del endpoint

Más información

FUENTES:
¹ <https://www.zdnet.com/article/the-more-cybersecurity-tools-an-enterprise-deploys-the-less-effective-their-defense-is/>
² <https://www.datreading.com/threat-intelligence/attackers-moving-faster-inside-target-networks-report>
³ <https://reprints2.forrester.com/#/assets/2/482/RES116772/report>