# 5 Razones por las que el XDR es esencial para los CISOs

Por Harold Rivas*

Detección y Respuesta Extendidas, o XDR, es un término que escuché hace años mientras trabajaba como CISO en otras empresas antes de llegar a Trellix. En aquel entonces, consideraba que XDR era sólo un concepto. Recuerdo haberme preguntado: "¿Esto es real o simplemente otra palabra de moda que flota en la industria?"

En lugar de utilizar XDR hace años, lo manejé manualmente contratando equipos de desarrolladores y analistas para resolver mis desafíos en el Centro de Operaciones de Seguridad (SOC por sus siglas en inglés), que van desde la integración de inteligencia de amenazas, el enriquecimiento de datos, la detección automática de amenazas, la investigación de incidentes y la respuesta a ataques.

Avancemos rápido hasta el día de hoy... después de numerosas interacciones con clientes, discusiones con otros CISO y de haber implementado personalmente una plataforma XDR, aprendí y fui testigo de que XDR es absolutamente real. No es sólo una idea, un concepto o una palabra de moda. Es realmente un punto de inflexión para los SOC. Pero hay algunas cosas que desearía haber sabido antes y que creo que pueden ayudar a otros a considerar XDR hoy.

**La Tecnología Correcta**

La mayoría de los CISO se centran en reunir las soluciones adecuadas para solucionar un problema en particular. Según el informe Mind of the CISO 2023 de Trellix, el 94% de los CISO dice que la tecnología adecuada les ahorraría mucho tiempo y el 81% dice que la tecnología adecuada ayudaría a reducir sus horas extras.

Cuando compra más y más tecnologías puede generar capacidades y desafíos aislados, como visibilidad de extremo a extremo, problemas de administración de plataformas y más. Sale a buscar soluciones puntuales para resolver cada uno de los problemas. Pasa innumerables horas preparando su propuesta para convencer a la junta directiva del financiamiento necesario para proteger el negocio; y al final está administrando una pila tecnológica compleja con 50 a 60 soluciones diferentes y muchas de ellas no se comunican entre sí.

Así que empieza a preguntarse: ¿cómo podemos mi equipo y yo ser más rápidos y efectivos ahora que tenemos todas estas herramientas? Y ahí es donde comienza el viaje hacia XDR. ¿Cómo se puede crear más automatización y eficiencia? ¿Cómo informa mi computadora portátil a mi firewall sobre una amenaza e indica que es necesaria una respuesta o acción?

¿La respuesta? Necesitas una hoja de ruta. Y esa hoja de ruta conduce a XDR.

**¿Por qué el XDR?**

Muchas de las cualidades que deseamos que ofrezcan nuestras soluciones puntuales existentes, como mejor visibilidad, precisión y priorización, son una parte inherente de XDR. Con el XDR adecuado, puede, por primera vez, superar algunos de estos desafíos de largo tiempo.

Existen numerosas razones para querer evaluar su tecnología de ciberseguridad y explorar XDR. He reducido mis cinco razones principales a continuación. Estos fueron los principales motivos por los que Trellix implementó XDR y por qué me apasiona tanto este tema y quiero ayudar a otros CISO a mejorar sus capacidades SOC también.

1. Une tu gran cantidad de herramientas desconectadas.
2. Cumple con los requisitos regulatorios en constante cambio.
3. Reduce su costo total de propiedad.
4. Aumente la eficacia de SecOps en el tiempo medio para detectar (MTTD), investigar (MTTI) y responder (MTTR).
5. Desbloquee los datos que ya posee con una plataforma abierta que correlacione datos de otras fuentes de datos en su entorno, para obtener más valor de las inversiones existentes.

Y vemos que cada vez más empresas eligen XDR. Según nuestro informe Mind of the CISO 2023, el 47% ha compartido que ya usa XDR y espera mantenerlo o hacerlo crecer.

**Qué buscar en una solución XDR**

Hay algunas cosas que debe tener en cuenta al evaluar las soluciones XDR. Su XDR debe ser integral y abierto, integrando controles de seguridad nativos y fuentes de datos de terceros, para que se adapte perfectamente al entorno de su organización y le brinde visibilidad de un extremo a otro. Debe buscar la capacidad de contextualizar y priorizar las amenazas y permitir la detección, investigación y respuesta a amenazas en tiempo real. ¿La solución se adapta a su entorno, ya sea que prefiera un enfoque local, en la nube o híbrido? En Trellix, nuestra plataforma se basa en una base de inteligencia contra amenazas, controles de seguridad nativos y más de 1000 integraciones de datos, con XDR actuando como el cerebro de toda la plataforma.

La Guía de Mercado de Gartner® 2023 para detección y respuesta extendidas publicada recientemente, ofrece una descripción general del mercado de XDR, así como una guía práctica para ayudar a los clientes a comparar a un proveedor con los resultados esperados de XDR. Es un recurso valioso para desenredar el mercado XDR. En nuestra opinión, Trellix resuelve todos los casos de uso que menciona Gartner y está bien posicionado para resolver sus necesidades. Consulte el informe y obtenga más información sobre Trellix XDR.

---

* Harold Rivas lidera las iniciativas globales de cumplimiento y seguridad de Trellix, lo que permite a la empresa protegerse mejor contra amenazas, gestionar las necesidades de cumplimiento y los riesgos de terceros, e implementar las mejores prácticas en toda la industria. Habiendo sido CISO, aporta a Trellix más de dos décadas de experiencia en ciberseguridad. Anteriormente fue CISO en lendDepot y otras empresas como Santander Consumer y Fujitsu America. También dirigió programas globales de ciberseguridad en Citigroup. Cuenta con Licenciatura y Maestría en Administración de Empresas y múltiples certificaciones de la industria, incluyendo Seguridad de Sistemas de Información (CISSO), y es además orador y miembro activo de InfraGard del Buró Federal de Investigaciones (FBI).