LOS MAYORES BENEFICIOS DE XDR

Las soluciones XDR reflejan la evolución continua de los productos de ciberseguridad. De hecho, XDR representa la culminación de la evolución de los productos de ciberseguridad, que va mucho más allá del ámbito de los productos de detección y respuesta de puntos finales (EDR) y de la detección y respuesta gestionadas (MDR).

XDR proporciona visibilidad de toda la superficie de ataque, que abarca entornos tanto en la nube como on-premise. Con XDR, las empresas obtienen una mejor detección y protección frente a amenazas, lo que les permite tomar decisiones precisas y en tiempo real basadas en datos recopilados y consolidados a través de una serie de puntos de entrada de amenazas.

Estos son cuatro de los mayores beneficios que ofrece XDR y lo que representan para su empresa.

1. Respuesta más rápida a incidentes

XDR ayuda a las empresas a identificar y responder a las amenazas más rápidamente gracias a sus capacidades de análisis avanzadas.

Qué significa para su empresa:

- Previene que las amenazas se propaguen y minimiza su impacto
- Reduce las probabilidades de pérdida de datos
- Reduce el riesgo de daños a la reputación

Pero ¿cuánto más rápido es XDR? Eche un vistazo a la tabla siguiente para descubrirlo.

Tiempo que suele tardar en resolverse

	Sin XDR	Con XDR
Resolución habitual de BEC (solo puerta de enlace)	De 1 a 2 meses	**De 1 a 2 horas**
Resolución de robos de identidad	De 3 a 4 semanas	**De 1 a 2 horas**
Resolución de infecciones de malware	De 3 a 4 semanas	**1 hora aprox**
Resolución de amenazas internas	De 3 a 6 meses	**4 horas aprox**
Resolución de extorsiones sin XDR	Variable	**Menos de 24 horas**

2. Visibilidad mejorada en todo su entorno de seguridad

XDR reúne la telemetría de todos sus sistemas —servidores, redes, nube, correo electrónico y endpoints— en un mismo panel de control y elimina los silos.

Qué significa para su empresa:

- Le ofrece una visión completa de la superficie de ataque
- Le ayuda a detectar vulnerabilidades o configuraciones incorrectas con mayor facilidad
- Simplifica el cumplimiento normativo y la presentación de informes con registros de auditoría más claros

3. Detección de amenazas más inteligente

XDR utiliza IA, análisis avanzados y algoritmos de aprendizaje automático para repeler ataques complejos de varias etapas, que las herramientas tradicionales a menudo pasan por alto. Puede detener tanto ataques conocidos como amenazas desconocidas de día cero. Además, proporciona información contextual en vez de alertas aisladas y ofrece detalles sobre los tipos y técnicas de los ataques.

Qué significa para su empresa:

- Le sitúa a la vanguardia de las complejas tácticas de los atacantes
- Reduce la fatiga por alertas, al automatizar la detección
- Proporciona una mejor comprensión de las tácticas, técnicas y procedimientos (TTP) de los atacantes

4. Costes de seguridad inferiores

Puesto que XDR optimiza sus conjuntos de herramientas y utiliza automatización, sus operaciones de seguridad resultan más eficientes y menos costosas.

Qué significa para su empresa:

- Se reduce la duplicidad de pagos por herramientas de seguridad
- Se libera presupuesto para invertir en otros campos
- Se maximiza el retorno de la inversión en seguridad

Estos no son en modo alguno los únicos beneficios de XDR. Para obtener más información sobre las ventajas de XDR y su funcionamiento, descargue nuestro libro electrónico Explicación de XDR: Un enfoque estratégico para la gestión de amenazas.

Barracuda