CISCO
SECURE

Guía del comprador de XDR

Navegue por el mercado emergente de Extended Detection and Response como un profesional

cisco SECURE

Comprensión de Extended Detection and Response (XDR)

¿Por qué el mundo necesita otro enfoque de seguridad?

Incluso los equipos de seguridad más confiables y mejor financiados saben que se enfrentan a presiones externas abrumadoras. El reciente cambio al trabajo remoto o híbrido ha sumado nuevas capas de complejidad. La superficie de ataque se expande constantemente. Hay un sinfín de alertas. Las herramientas de seguridad son incompatibles. Con tanta fricción entre las personas y la tecnología, no es de extrañar que la eficacia de la seguridad esté estancada y que los tiempos de permanencia promedio giren en torno a los 280 días[1].

Esta nueva normalidad precisa de resiliencia de seguridad, que es la capacidad de proteger la integridad de todos los aspectos de su empresa para que pueda resistir amenazas o cambios impredecibles y resurgir con más fuerza. Y la resiliencia de seguridad requiere más de lo que el pasado ha ofrecido.

Razones clave para explorar XDR:

1. Reduzca el agotamiento de las alertas
2. Acelere el tiempo de detección
3. Aumente la visibilidad de las herramientas
4. Obtenga un mejor contexto de amenazas

Entonces, ¿qué es exactamente XDR y por qué debe importarme?

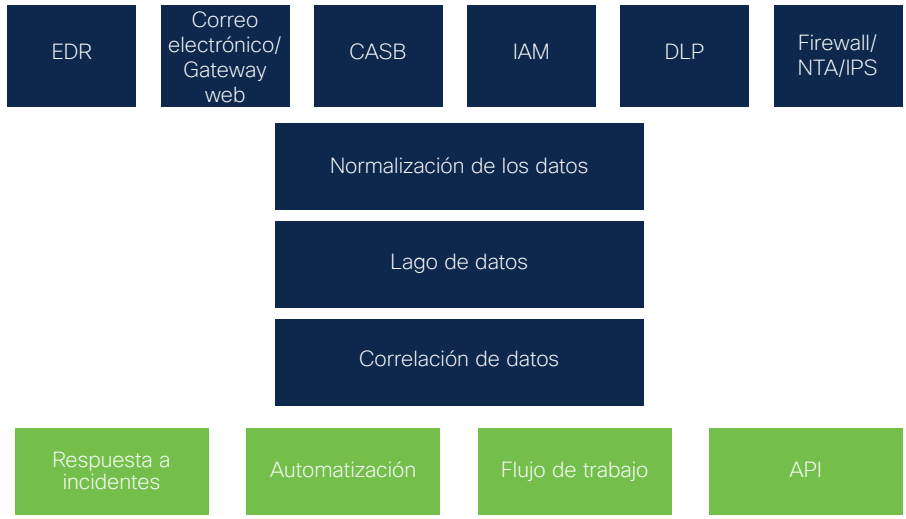
Si bien la integración en soluciones de puntos de seguridad nativos dentro de XDR es extremadamente beneficiosa, también es fundamental que una plataforma XDR aproveche y se conecte fácilmente a la tecnología de terceros existente, lo que ofrece un mejor ROI y un contexto más rico para todas las fuentes de datos. Este es un cambio de paradigma significativo con respecto a las estrategias existentes, donde la mayor parte de la detección y respuesta tiene lugar dentro de los silos y equipos de productos individuales. La unidad que ofrece XDR afecta varias áreas clave para cada equipo de seguridad:

En primer lugar, ofrece un valor rápido para los equipos con poca o ninguna calibración. Para los equipos que ya han realizado el trabajo de configuración de un SIEM o SOAR, las plataformas XDR se basan en dichos beneficios.

En segundo lugar, resuelve la fatiga de las alertas que afecta a muchos equipos, ya que la plataforma agrega y correlaciona todos los eventos dispares causados por la misma intrusión en incidentes.

En tercer lugar, ofrece elementos de automatización y orquestación listos para usar que ayudan a los equipos a eliminar tareas rutinarias para sus actividades diarias.

Arquitectura conceptual de XDR



1. Investigación del Instituto Ponemon presentada en el Informe del costo de una violación de datos de IBM 2020

cisco SECURE

Cinco elementos clave del funcionamiento correcto de XDR

1 Telemetría coordinada desde cualquier lugar de su entorno

Algo fundamental para XDR debe ser la amplitud de la visibilidad y la profundidad de la información. En este momento, los proveedores están posicionando sus productos existentes como componentes clave en XDR. Pero XDR real debe conectar no solo los datos, sino también la telemetría de la más amplia variedad de categorías de control de seguridad, repositorios de datos y proveedores de inteligencia de amenazas para determinar la probabilidad de intención maliciosa. Gracias a XDR, las organizaciones pueden cerrar las brechas y lograr una defensa generalizada en todo el ecosistema mediante una plataforma abierta e integrada en el campus, el centro de datos, la nube y el perímetro de la nube. Dado el contexto enriquecido extraído de cada una de estas soluciones integradas dentro de XDR, puede encontrar vulnerabilidades y corregirlas más rápidamente.

Funciones clave	Preguntas
Información completa del entorno	¿En qué medida su solución me brinda algo más que visibilidad en la red?
Telemetría procesable	¿Utiliza un lago de datos para ofrecer información o algo que proporcione una telemetría más impactante?
Fuentes confiables de datos	¿Cómo garantiza su solución que obtendré contexto en todos los terminales, los dispositivos y el tráfico que entra y sale de la red?

2 Aproveche la funcionalidad de detección de sus inversiones existentes, independientemente del proveedor

Si bien Gartner menciona componentes patentados en su definición de XDR, es fundamental que una solución XDR se desarrolle con un enfoque de plataforma abierta que se conecte fácilmente con tecnología de terceros. Cada componente de la pila de seguridad tiene elementos de detección únicos (detección de IoC, aprendizaje automático, análisis de comportamiento, etc.) que se tornan más potentes cuando se combinan. Las señales débiles de los silos se convierten en señales fuertes en conjunto. La detección en conjunto es fundamental para XDR, así que asegúrese de que la plataforma que elija funcione con toda su pila.

Funciones clave	Preguntas
Aprovecha sus soluciones	¿Cuántas de mis inversiones existentes puede aprovechar su enfoque de XDR?
Agnosticismo del proveedor	¿En qué se diferencian sus tecnologías de detección de otras que están en el mercado?
Incorpora análisis de terceros	¿Cuáles de sus soluciones tienen integraciones listas para usar?

3 Contexto unificado de fuentes realmente confiables que admiten una respuesta rápida y precisa

La unificación de la información de la red, el terminal y el correo electrónico (por mencionar algunos) proporciona una comprensión más precisa de lo que ha sucedido, cómo progresó y qué pasos deben tomarse para corregir la amenaza. Para que XDR sea eficaz se requieren capacidades de respuesta y corrección nativas, como aislar un host o eliminar un correo electrónico malicioso de todas las bandejas de entrada. Idealmente, estas acciones serían posibles con solo uno o dos clics. XDR también debe facilitar la creación de acciones de respuesta personalizadas, de modo que los equipos puedan desarrollar su seguridad a medida que pasa el tiempo.

Funciones clave	Preguntas
Inteligencia basada en el contexto	¿Puedo usar su XDR para comprender el impacto de una amenaza, el alcance de la intrusión y tomar medidas con un solo clic desde una interfaz?
Varias fuentes de verdad	¿Qué tipo de inteligencia de amenazas alimenta su detección y de dónde proviene esa inteligencia?
Mejore el MTTD	¿Cómo valida las fuentes de datos que utiliza en su solución?

4 Oportunidades continuas de automatización y organización para problemas a escala de la máquina

Seguir flujos de trabajo complicados, manuales y obsoletos expone a su empresa a amenazas y errores humanos. La plataforma XDR correcta tendrá sólidas capacidades de coordinación y automatización y hará que las tareas de seguridad repetitivas sean más fáciles y eficientes sin una curva de aprendizaje masiva para ponerse en marcha. La automatización de los flujos de trabajo críticos ayuda al equipo a responder a las alertas más rápidamente, lo que deja más tiempo y energía para tareas críticas, como la búsqueda de amenazas.

Funciones clave	Preguntas
Más automatización	Para sus integraciones de terceros, ¿los cambios de API de los proveedores violan sus scripts de automatización?
Vea a través del ruido de la seguridad	¿Cómo pueden ayudarme a organizar y automatizar los flujos de trabajo en mis soluciones existentes?
Supere las limitaciones de escala humana	¿Cómo admite su solución el monitoreo desde y hacia las cargas de trabajo basadas en la nube?

5 Un único punto de vista de investigación que simplifica el aislamiento y la corrección

XDR debe ampliar las herramientas esenciales en el kit de un equipo de respuesta a incidentes, brindando visibilidad de la telemetría adicional más allá del terminal. Una única consola permite la corrección directa, el acceso a la inteligencia de amenazas y las herramientas para proporcionar una vista unificada de una alerta. Además, XDR, que facilita la búsqueda de amenazas a través de modelos tales como MITRE ATT&CK, hará que la búsqueda de amenazas basada en hipótesis sea accesible para quienes son nuevos en el proceso y facilitará la anticipación de lo que viene.

Funciones clave	Preguntas
Mejore el MTTR	¿En qué medida ayuda su solución o acelera la corrección?
Permita más búsquedas de amenazas	¿Cómo ayuda su solución a mi equipo en sus esfuerzos de búsqueda de amenazas?

Avance con XDR

Recomendamos trabajar con las partes interesadas de XDR para determinar qué estrategia de XDR es adecuada para usted. Asegúrese de que los proveedores potenciales prioricen la automatización y la integración.

Comience con estas preguntas, pero asegúrese de comprender las diversas funciones y los requisitos de su pila actual para poder lograr resultados medibles y mejorar el ROI.

1. ¿Su oferta de XDR cubre la detección y respuesta de red y otras capas de seguridad, como correo electrónico, nube y firewall?
2. ¿Cómo me ayudarán a tomar medidas de seguridad mejores y más informadas?
3. ¿Cómo me ayuda XDR a automatizar el bloqueo o la corrección?
4. ¿Cuáles de sus soluciones tienen integraciones inmediatas entre sí?
5. ¿Cómo se relaciona su enfoque de XDR con otras iniciativas de seguridad, como SASE o Zero Trust?

cisco SECURE

XDR + Resiliencia de seguridad

Hoy en día, la incertidumbre es una garantía, desde las operaciones hasta las finanzas y la cadena de suministro. Las empresas están invirtiendo en resiliencia: la capacidad de resistir impactos imprevistos y salir fortalecidos. Pero estas inversiones no serán suficientes sin una pieza clave: la resiliencia de seguridad.

Las cinco dimensiones de la resiliencia de seguridad son las siguientes:

1. Activar miles de millones de señales en todo su ecosistema
2. Anticiparse a lo que vendrá a través de la inteligencia compartida
3. Priorizar alertas con análisis de contexto basado en riesgos
4. Cerrar las brechas en todo el ecosistema con integraciones
5. Fortalecerse a través de la orquestación y la automatización

La plataforma XDR correcta cumple con cada una de estas dimensiones. Y solo Cisco cumple con la promesa de XDR en la actualidad, a través de un contexto unificado, detecciones correlacionadas y respuestas más rápidas.

SecureX, nuestra plataforma de seguridad integrada, es un derecho con todos los productos de seguridad de Cisco y se integra fácilmente en las soluciones en su entorno mediante API abiertas. Esta capa unificada de detección y respuesta correlaciona la telemetría desde todos los puntos de control en un único punto de vista de investigación y simplifica mucho la priorización y la toma de medidas. Además, la orquestación integrada le permite automatizar las respuestas y descargar las tareas de rutina para liberar a los equipos para tareas más proactivas, como la búsqueda de amenazas.

No más carreras en el lugar, es hora de avanzar.

Si desea obtener más información sobre el enfoque de Cisco para XDR, comuníquese con su representante de ventas hoy mismo.

Sede central en América
Cisco Systems, Inc.
San José, CA

Sede central en Asia Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede en Europa
Cisco Systems International BV Amsterdam,
Países Bajos

cisco SECURE

Hoja de trabajo de validación de proveedores de XDR

Utilice este formato de tabla y las preguntas proporcionadas anteriormente en este documento para prepararse para las conversaciones con los proveedores de XDR.
Elija de 8 a 10 preguntas que sean más relevantes para su entorno y cópielas y péguelas a continuación.

Preguntas/Notas	Respuestas convincentes
Pregunta:	
Notas:	
Pregunta:	
Notas:	
Pregunta:	
Notas:	
Pregunta:	
Notas:	
Pregunta:	
Notas:	
Pregunta:	
Notas:	
Pregunta:	
Notas:	
Pregunta:	
Notas:	
Pregunta:	
Notas:	
Pregunta:	
Notas:	


CISCO
SECURE