Guía breve

# 9 COSAS A TENER EN CUENTA AL ELEGIR UN SERVICIO MDR

Digital Security
Progress. Protected.

# MDR puede ayudar a superar las brechas en la capacidad de seguridad y experiencia. Elegir el proveedor adecuado es clave.

Entre las empresas de todos los tamaños, hay un reconocimiento creciente de la necesidad de una seguridad más proactiva. La continua adopción de la computación en la nube, las nuevas prácticas de trabajo híbridas y la cadena de suministro digital han incrementado la superficie de ataque, y los agentes maliciosos se han vuelto más ingeniosos para encontrar formas de infiltrarse en las redes.

Sin embargo, solo las grandes empresas operan a una escala que les permite equipar un centro de operaciones de seguridad completo y dotarlo de analistas de seguridad a tiempo completo. Incluso si cuentas con los fondos, los especialistas en ciberseguridad escasean. Si la tuya es una empresa mediana o pequeña, es probable que tengas que depender de especialistas de IT para asumir la responsabilidad de defender el entorno de IT.

Los servicios de detección y respuesta gestionadas (MDR) llenan el vacío para las empresas que necesitan superar brechas en la capacidad de seguridad y experiencia. Proporcionan acceso a servicios gestionados por profesionales de ciberseguridad y a los conjuntos de herramientas especializadas que necesitan para ejercer su labor.

Sin embargo, quienes utilizan el término MDR para describir sus ofertas cuentan con una amplia variedad de modelos de entrega. Si has decidido mejorar tu seguridad y contratar un servicio MDR externo, necesitas investigar para encontrar el proveedor que mejor se adapte a tu empresa. Aquí tienes las preguntas que deberías hacer.

## 1. ¿CUÁL ES EL PROCESO DE INTEGRACIÓN Y AJUSTE DEL PROVEEDOR?

Los tiempos de integración varían, al igual que las herramientas preferidas y los modelos de entrega de los distintos proveedores de MDR. Asegúrate de comprender el proceso de integración y el grado de implicación que necesitará tu equipo de IT para evitar sorpresas.

Debe haber cierta personalización de las reglas de detección, exclusiones y parámetros para adaptarse a las necesidades de tu entorno de IT y a las amenazas que enfrenta tu empresa. Una integración más rápida siempre es deseable, pero puede haber un compromiso aquí, buscando un equilibrio entre poner en marcha el servicio MDR lo antes posible y lograr un rendimiento óptimo de detección desde el primer día.

Además, ten en cuenta que la protección proporcionada por un servicio MDR mejora con el tiempo. Se requiere cierto perfeccionamiento a medida que las herramientas y los analistas humanos adquieren experiencia práctica y aprenden qué es normal y qué es anómalo en tu entorno.

## 2. ¿EL SERVICIO ES 24/7?

Las bandas adversarias operan desde países y zonas horarias de todo el mundo, lo que significa que un servicio MDR debe ser una labor 24/7. Los indicadores de compromiso y los indicadores de ataque deben investigarse de inmediato, en tiempo real, para que se pueda iniciar una respuesta adecuada.

Un servicio local tiene algunas ventajas, pero estas desaparecen rápidamente si la dotación de personal durante la noche no es adecuada. Tu mejor opción podría ser un servicio que te proporcione un representante local y que además mantenga centros de operaciones de seguridad completamente dotados en ubicaciones de todo el mundo para una operación 24/7 real.

## 3. ¿CUÁL ES EL CONJUNTO TECNOLÓGICO? ¿QUÉ FUENTES DE DATOS SE UTILIZAN?

Un elemento fundamental de un servicio MDR es un conjunto tecnológico proporcionado por el proveedor que gestione la detección, investigación, mitigación y respuesta. Puede ser un conjunto tecnológico desarrollado por el proveedor o un conjunto de herramientas de terceros enlazadas mediante APIs. Las herramientas probablemente incluirán detección y respuesta en endpoint o ampliada (EDR o XDR), gestión de información y eventos de seguridad (SIEM), y orquestación y respuesta de seguridad (SOAR), y deberían integrarse con tu plataforma de protección de endpoint.

La característica distintiva de un XDR frente a un sistema EDR es la incorporación de fuentes de datos externas a los endpoints, incluyendo el tráfico de red y varios archivos de registro. Pregunta qué fuentes de datos se utilizarán como parte del esfuerzo de monitorización. Una ventaja de un servicio proporcionado por un proveedor de protección de endpoints es que la plataforma de

endpoints no solo puede alimentar directamente el XDR, sino que también puede proporcionar telemetría que recopila datos únicos sobre ataques.

Los adversarios cibernéticos son cada vez más hábiles en el uso de servicios en la nube como vector de ataque o parte de la cadena de ataque, así que asegúrate de que tu proveedor MDR sea capaz de detectar y monitorizar actividades en la nube.

## 4. ¿QUÉ PAPEL JUEGA LA AUTOMATIZACIÓN EN LA OFERTA? ¿QUÉ PAPEL DESEMPEÑAN LOS ANALISTAS HUMANOS?

Un conjunto tecnológico robusto es importante, pero lo que hace que un servicio MDR sea MDR es la atención de los analistas de ciberseguridad humanos en el proceso.

La inteligencia artificial puede desempeñar un papel valioso en la identificación de comportamientos anómalos y en el análisis de acciones aparentemente no relacionadas para reconocer correlaciones y señales de compromiso o ataque. La automatización puede ejecutar rápidamente un conjunto de acciones que aíslan sistemas o detienen un ataque en seco. Estas son funciones de asistencia y no reemplazan la experiencia humana de los analistas.

En su prisa por salir al mercado o hacer sus servicios más asequibles, algunos proveedores de MDR dependen en exceso de la automatización para algunas partes de sus ofertas (para más información, consulta "¿Quién se encarga de la mitigación y remediación?" más abajo). Algunos ofrecen servicios escalonados, donde los niveles superiores ponen a disposición servicios dirigidos por expertos, como responsables dedicados a la respuesta ante incidentes, respuesta forense digital a incidentes (DFIR) y análisis experto de malware.

## 5. ¿QUÉ FUENTES DE INTELIGENCIA SOBRE AMENAZAS SE UTILIZAN?

La inteligencia sobre amenazas actualizada acerca de las actividades de los adversarios cibernéticos globales es un componente clave de un servicio MDR verdaderamente eficaz. Recopiladas a partir de la telemetría y seleccionadas por equipos de inteligencia sobre amenazas, estas actualizaciones revelan métodos de ataque y comparten contramedidas.

Los feeds de inteligencia sobre amenazas pueden ser generados por el proveedor del servicio MDR u obtenidos de uno o más terceros. Es importante comprender las fuentes de la inteligencia del proveedor, cómo se recopila y cómo se hace accionable dentro del servicio.

Poner inteligencia sobre amenazas actualizada y vigente frente a los analistas de seguridad es clave para detectar amenazas latentes dentro de tu entorno (tema n.º 6).

# Acerca de ESET Detección y respuesta gestionadas

Los servicios MDR de ESET se basan en una base sólida: la galardonada protección de endpoints de ESET; ESET Detección y respuesta ampliada, que proporciona herramientas prácticas para analistas de seguridad; y expertos en seguridad humanos que gestionan las consolas. Trabajan en una red global de centros de operaciones para monitorizar y responder a amenazas; recopilar y seleccionar inteligencia sobre amenazas; y rastrear de manera vigilante a los adversarios cibernéticos internacionales y sus tácticas, técnicas y procedimientos.

El servicio está disponible en dos niveles, uno diseñado para ofrecer protección sofisticada a pequeñas y medianas empresas y el otro que constituye efectivamente un centro de operaciones de seguridad (SOC) para empresas. Ambos niveles incluyen los componentes clave de un servicio MDR, incluyendo la detección de amenazas continua y la monitorización práctica, contención y erradicación de amenazas. El nivel superior ofrece mayor acceso a servicios personalizados o especializados de expertos en ciberseguridad de ESET.

# ESET MDR ofrece:

- **Detección de amenazas, monitorización y respuesta para clientes de cualquier tamaño y nivel de experiencia en seguridad**
- **Servicio siempre activo, 24/7, que aplica una combinación de automatización impulsada por IA y experiencia humana**
- **Una biblioteca predefinida de patrones de detección de comportamiento, personalizada y adaptada al entorno del cliente**
- **Un equipo global de inteligencia sobre amenazas que rastrea incidentes críticos actuales y toma acciones coordinadas para contrarrestar amenazas**

## 6. ¿QUÉ TIPOS DE DETECCIÓN DE AMENAZAS SE OFRECEN?

El objetivo del adversario es establecer una presencia desconocida en la red empleando tácticas, técnicas y procedimientos que evadan los mecanismos de detección existentes. Encontrar estas amenazas ocultas y evasivas es el ámbito de la detección proactiva de amenazas.

La inclusión de la detección de amenazas y el alcance de los servicios es uno de los diferenciadores clave entre los servicios MDR. Busca una detección de amenazas continua y sistemática; debe considerarse parte de los requisitos básicos para un servicio MDR.

Algunos proveedores ofrecen específicamente detección de amenazas personalizada de forma planificada o recurrente, enfocada en ciberamenazas actuales, u ofrecen detección de amenazas histórica basada en hipótesis que se apoya en datos de detecciones pasadas y métodos de ataque.

## 7. ¿QUIÉN SE ENCARGA DE LA MITIGACIÓN Y REMEDIACIÓN?

Entre los proveedores de MDR, no existe una visión compartida sobre qué parte —el proveedor del servicio o el comprador— es responsable de la parte de "respuesta" de MDR. Si bien la detección de sistemas comprometidos y ataques activos es una parte universal de los servicios MDR, varían en sus enfoques para mitigar la amenaza (contención para evitar daños adicionales) y remediarla (restaurando datos y la funcionalidad del sistema).

Algunos proveedores solo tomarán medidas de respuesta si pueden ser automatizadas; de lo contrario, solo ofrecen asistir al personal de IT del cliente. Otros ofrecen la respuesta como parte de un servicio de nivel superior, bajo un contrato de retención o por un precio adicional.

Los clientes también difieren en su nivel de comodidad con los cambios realizados por terceros. Puede que seas reacio a permitir que el servicio MDR remedie tus sistemas porque carecen de un conocimiento profundo del posible impacto en los procesos de empresas. Puede que prefieras un enfoque que dependa del servicio MDR para contener la amenaza y eliminarla, dejando la restauración completa a tu personal de IT.

## 8. ¿CÓMO SE ALINEA EL ENFOQUE DEL PROVEEDOR CON TU EMPRESA?

Cuando ocurren incidentes, el impacto del servicio MDR va más allá de la seguridad y afecta otras partes de tu empresa. Revisa el enfoque del proveedor respecto a la contención y considera cómo las acciones tomadas se alinearán con los requisitos de tu empresa.

Desde el punto de vista operativo, considera cómo y si sus actividades y resultados pueden o deben integrarse con tus sistemas de gestión de tickets y flujos de trabajo internos.

El proveedor también debe poder proporcionar o permitirte generar informes sobre incidentes pendientes y resueltos, el estado de tu entorno y cualquier otro detalle que gestione en tu nombre.

## 9. SI TIENES REQUISITOS NORMATIVOS O DE CUMPLIMIENTO ESPECÍFICOS, ¿PUEDE EL SERVICIO CUMPLIRLOS?

Si tienes requisitos de privacidad, residencia o retención de datos, verifica que el proveedor MDR pueda cumplirlos. Es posible que debas ajustar o hacer excepciones especiales a los procesos estándar para cumplir con tus normativas locales.

Si estás buscando o ya cuentas con cobertura de seguro de ciberseguridad, compara los elementos del servicio del proveedor con los requisitos del seguro. Los controles cibernéticos adicionales que forman parte del servicio MDR pueden calificarte para la cobertura o reducir tu prima.

## CONCLUSIÓN

MDR es una categoría de mercado en rápido crecimiento. Según Gartner, hay más de 600 proveedores que ofrecen servicios MDR (o servicios que denominan MDR); el 30% de las empresas están utilizando activamente MDR, y ese número se duplicará para 2025.

En términos generales, los proveedores de MDR que han respondido a la creciente demanda se dividen en dos categorías: (1) empresas que ofrecen servicios de IT gestionados de forma externalizada y han añadido MDR a su oferta y (2) empresas de software de seguridad que han añadido un componente de servicios. Más allá de esta categorización general, existen modelos muy diversos sobre cómo debe diseñarse y entregarse un servicio MDR. Comprender esas diferencias es importante.

Aplaudimos tu reconocimiento de la necesidad de contar con un servicio MDR y esperamos que esta guía te sea útil para encontrar la opción adecuada para tu empresa.

# Esto es ESET

## **Defensa proactiva.** Nuestro negocio es minimizar la superficie de ataque.

Mantente un paso por delante de las amenazas cibernéticas conocidas y emergentes con nuestro **enfoque centrado en la prevención, impulsado por la inteligencia artificial y la experiencia humana**.

Experimenta una protección de primer nivel, gracias a nuestra **inteligencia sobre ciberamenazas** global interna, compilada y analizada durante más de 30 años, que impulsa nuestra extensa red de I+D, liderada por **investigadores reconocidos por la industria**. ESET protege tu empresa para que puedas aprovechar todo el potencial de la tecnología.

**EXPLORAR**

ESET®

Digital Security
**Progress. Protected.**