Perfeccionando la ciberseguridad con MDR:

La guía definitiva sobre detección y respuesta gestionadas

Digital Security
Progress. Protected.

Introducción: un enfoque preventivo en múltiples capas

El mundo está cambiando más rápido de lo que muchos defensores de redes pueden gestionar. Se enfrentan a un adversario ágil y decidido, armado hasta los dientes con la tecnología más avanzada. A medida que la superficie de ataque corporativa se expande con cada nueva inversión digital, aumentan tanto las probabilidades como los costes de sufrir una brecha de seguridad grave. El coste medio de una filtración de datos a nivel mundial asciende ya a casi 4,9 millones de dólares.

Para **gestionar estos riesgos crecientes**, las empresas deberían plantearse adoptar un enfoque **proactivo, centrado en la prevención**, diseñado para minimizar la superficie de ataque, reducir costes y complejidad, y mejorar la ciberhigiene.

Más de la mitad de las empresas que han sufrido una brecha de seguridad se enfrentan a una gran escasez de personal especializado en ciberseguridad. Este problema ha registrado un incremento del

26.2%

entre 2023 y 2024.

Fuente: *IBM: Cost of a Data Breach Report 2024*.

Los ciberdelincuentes solo necesitan tener éxito una vez para causar daños significativos. Por eso, el enfoque más avanzado en ciberseguridad corporativa combina la prevención en múltiples capas con capacidades de detección y respuesta. Sin embargo, el reto al que se enfrentan muchas empresas es que:

BRECHAS DE HABILIDADES Y ESCASEZ DE CONOCIMIENTOS afectan su capacidad para ejecutar operaciones de seguridad 24/7/365 (SecOps).

LA COMPLEJIDAD de las herramientas de detección y respuesta significa que algunas empresas podrían no contar con personal interno para operarlas.

LAS CIBERAMENAZAS ESTÁN VOLVIÉNDOSE MÁS SOFISTICADAS y tienen un impacto mayor, lo que permite a los actores maliciosos alcanzar sus objetivos con mayor rapidez.

LOS PRESUPUESTOS SON LIMITADOS, especialmente para grandes compras puntuales de infraestructura de detección y respuesta y operadores humanos.

PRESIONES DE CUMPLIMIENTO las presiones de cumplimiento están aumentando, amplificando el impacto negativo de los ataques en caso de incumplimiento.

Por eso, muchas empresas están recurriendo a la **detección y respuesta gestionadas (MDR)**. Al hacerlo, pueden acceder al poder combinado de un equipo de SecOps experto de terceros que utiliza herramientas avanzadas de inteligencia artificial para una respuesta rápida y contención de amenazas. Los mejores servicios MDR automatizarán el seguimiento y la elaboración de informes para mejorar el cumplimiento y promover mejoras continuas en la ciber-resiliencia. Esto permitirá que los equipos internos se centren en tareas estratégicas de mayor valor para el negocio.

$4.88 millones

fue el coste global medio de una brecha de seguridad en 2024, el cual representa el mayor aumento desde la pandemia.
Fuente: *Cost of a Data Breach Report 2024*.

Capítulo 1: Por qué tu empresa necesita MDR

Hoy en día, las empresas siguen ampliando su infraestructura y aplicaciones en la nube, apoyando el trabajo remoto y expandiendo sus cadenas de suministro digitales y tradicionales. Esto ofrece más oportunidades para los actores maliciosos altamente motivados, que cada vez más están aprovechando la inteligencia artificial, herramientas automatizadas, ofertas "como servicio" y más, para mejorar sus habilidades, profesionalizarse y amplificar los ataques. En este contexto, **MDR se está convirtiendo en una necesidad para empresas de todos los tamaños.**

DE LA PREVENCIÓN A MDR

Los equipos de seguridad internos están luchando para gestionar el volumen, la variedad, la velocidad y, en algunos casos, la sofisticación de las amenazas que enfrentan sus organizaciones. El ransomware se encuentra entre las más graves. El ransomware como servicio (RaaS) es una "industria" subterránea altamente competitiva, donde las bandas innovan continuamente para eludir los controles de seguridad y aumentar sus ganancias. Según los expertos en seguridad del gobierno británico, se espera que la amenaza aumente a medida que más adversarios consigan herramientas de inteligencia artificial.

Se espera que la frecuencia de los ataques de ransomware a gobiernos, empresas, consumidores y dispositivos aumente

cada 2

segundos para 2031

Fuente: *Cybercrime Magazine: Top 10 Cybersecurity Predictions and Statistics For 2024*.

"Los servicios de IA reducen las barreras de entrada, aumentando el número de ciberdelincuentes, y potenciarán sus capacidades al mejorar la escala, la velocidad y la eficacia de los métodos de ataque existentes."

James Babbage, director general de menazas de la Agencia Nacional contra el Crimen (National Crime Agency).

Los actores maliciosos están utilizando este tipo de herramientas para reducir el tiempo que transcurre desde el acceso inicial hasta el robo de datos o la implementación de ransomware. Este desafío no se limita solo al ransomware, sino que abarca toda la gama de amenazas a las que se enfrentan las empresas: desde malware de criptominería y redes de bots hasta troyanos bancarios y programas espía.

El impacto acumulado de estas tendencias debería llevar a los responsables de seguridad informática a centrarse en una verdad ineludible: la motivación de los actores maliciosos por lograr su objetivo suele ser mayor que la preparación de las empresas mediante medidas preventivas. Estos atacantes hacen todo lo posible por infiltrarse en el entorno corporativo sin ser detectados. Por eso, las empresas deben **equilibrar la prevención con la detección y la respuesta**. Este es precisamente el enfoque de ESET, centrado en la prevención, que **combina múltiples capas de tecnología de seguridad**. Su objetivo es proteger bloqueando el código malicioso o los actores dañinos antes de que puedan entrar o causar daño en el sistema del usuario.

El phishing fue el vector de ataque más costoso y frecuente en 2024, con un coste de

€4.88 millones

y un

15% muestra

la mayor parte de todos los ataques.

Fuente: *IBM: Cost of a Data Breach Report 2024*.

Sin embargo, si estas medidas son eludidas por actores sofisticados, debe existir una detección y respuesta rápidas y fiables para mitigar las amenazas avanzadas que logren comprometer un sistema. Puedes verlo como cerrar y asegurar todas las puertas y ventanas de tu casa, pero además instalar alarmas con detección de movimiento para detectar cualquier actividad sospechosa en caso de que alguien consiga entrar.

XDR es un recurso clave en este contexto. Permite a los equipos de operaciones de seguridad (SecOps) obtener una **visibilidad sin precedentes** de todo su entorno de IT desde una única consola, y detectar anomalías que puedan indicar amenazas mediante alertas de alta fidelidad. XDR es una evolución del EDR, que optimiza la detección de amenazas, la investigación, la respuesta y la búsqueda proactiva en tiempo real.

XDR unifica las detecciones relevantes de seguridad en los endpoints con la telemetría procedente de herramientas tanto de seguridad como empresariales, como el análisis y visibilidad de red (NAV), la seguridad del correo electrónico, la gestión de identidades y accesos, la seguridad en la nube, entre otras. Se trata de una plataforma nativa en la nube, basada en una infraestructura de big data, que ofrece a los equipos de seguridad flexibilidad, escalabilidad y oportunidades de automatización.

XDR TE PERMITE RESPONDER A VARIAS PREGUNTAS CLAVE SOBRE UN CIBERATAQUE:

¿Cómo comenzó?
¿Dónde y cuándo comenzó?
¿Qué endpoints están infectados?
¿Está contenido?
¿Cómo prevenimos que ocurra en el futuro?

Lo más importante es que puede ayudarte a tomar medidas correctivas rápidas para resolver los incidentes antes de que afecten gravemente a la empresa.

Sin embargo, incluso con la ayuda de XDR, los equipos de SecOps enfrentan **importantes desafíos** desde una perspectiva organizacional, especialmente las brechas de habilidades, la complejidad de las herramientas, las limitaciones de presupuesto y recursos, y la integración de herramientas; sin mencionar un panorama de amenazas que evoluciona rápidamente. **Por eso, muchos están recurriendo a MDR**, la forma más eficaz de detectar y contener las amenazas sofisticadas y en constante cambio.

CÓMO MDR ABORDA LAS AMENAZAS CONTEMPORÁNEAS

Aunque MDR varía según el proveedor, debería incluir al menos alguna de las siguientes variantes:

- **Monitorización y detección de amenazas 24/7:**
  Monitorización continua de la red, los endpoints y los entornos en la nube de la empresa.

- **Detección proactiva de amenazas:**
  A diferencia de las medidas de seguridad tradicionales que reaccionan a las alertas, MDR implica la detección proactiva de amenazas, lo que ayuda a identificar APTs y vulnerabilidades de día cero.

51%

es el número

de empresas que han establecido formalmente metodologías de detección de amenazas en 2024, en comparación con el 35% en 2023.
Fuente: *SANS: The Evolution of Enterprise Threat Hunting: Detailed Insights from the SANS 2024 Survey*.

- **Análisis y respuesta experta:**
  La experiencia de los profesionales de seguridad permite un análisis detallado y una toma de decisiones rápida, lo cual es crucial para abordar incidentes de seguridad complejos.

- **Inteligencia global sobre amenazas:**
  Una telemetría precisa, actual y relevante recopilada en todo el mundo proporciona inteligencia procesable para una respuesta rápida a incidentes y una detección de amenazas optimizada.

Las empresas que utilizan telemetría pueden lograr hasta un

60%

de mejora

en su capacidad para gestionar vulnerabilidades y amenazas, en comparación con aquellas que dependen únicamente de medidas de seguridad tradicionales.
Fuente: *Forrester: The Four Steps for More Proactive Security, 2024*.

- **Mejora continua**:
  Al analizar incidentes pasados, utilizar inteligencia avanzada sobre amenazas, centrarse en amenazas reales y proporcionar revisiones periódicas de seguridad y informes, los servicios MDR ayudan a prevenir la recurrencia de ataques similares al permitir que los equipos mejoren la ciberresiliencia.

FUNCIONES CLAVE DE MDR

MDR puede aportar enormes beneficios a las empresas que desean mitigar el riesgo cibernético, pero que no cuentan con los recursos internos necesarios para ayudarles a cerrar las brechas de habilidades, ahorrar costes y mejorar la detección y respuesta. Una solución de alto rendimiento debería permitir a las empresas:

Monitoriza

Los detectores de amenazas experimentados realizan un seguimiento de todo el entorno de IT del cliente y monitorizan activamente los grupos de malware y APT para proporcionar el más alto nivel de conciencia situacional.

Detecta

Los actores maliciosos tienen innumerables formas de burlar las defensas perimetrales, pero al aprovechar el análisis de comportamiento, pueden ser detectados para una rápida remediación.

Clasifica

Una evaluación inicial y la categorización de alertas filtran los falsos positivos y recopilan la información necesaria.

Prioriza

El análisis inteligente clasifica estas alertas por gravedad para asegurar que se aborden primero las amenazas más críticas. Esta es una fase crucial del flujo de trabajo de MDR, dada la dificultad que enfrentan muchos equipos de IT con la sobrecarga de alertas.

Investiga

Las herramientas automatizadas y la experiencia humana se combinan para profundizar en las alertas, realizando análisis de datos y registros con el fin de comprender su naturaleza y alcance. Será necesario determinar si una alerta es un verdadero positivo o no, y qué pasos deben tomarse para resolverla.

Responde

Un servicio MDR efectivo proporcionará acciones básicas de respuesta para bloquear y contener la amenaza, o bien, contención y remediación completa de los sistemas comprometi dos. Esto último podría implicar un restablecimiento de contraseñas, la aplicación de parches en endpoints específicos o incluso la reinstalación del sistema operativo en los ordenadores.

CARACTERÍSTICAS ESENCIALES A BUSCAR EN UNA SOLUCIÓN MDR

Los beneficios de externalizar la detección y respuesta son simples pero convincentes:

- El proveedor de MDR se encarga de toda la gestión de la tecnología de back-end, lo que permite a los empleados centrarse en tareas estratégicas de alto valor en lugar de ahogarse en alertas de seguridad.
- El proveedor de MDR también puede optimizar la tecnología de backend para alinearla con el perfil de riesgo y la infraestructura de cada cliente.
- Con la detección y respuesta gestionadas por un tercero, no será necesario pagar sueldos elevados para atraer y retener el mejor talento en ciberseguridad.
- Los clientes pueden beneficiarse de las economías de escala de su proveedor, su capacidad para atraer al mejor talento y su visión de otras empresas de clientes y entornos de amenazas.

Con tantas soluciones MDR inundando el mercado, puede ser un desafío saber por dónde empezar. Considera un proveedor capaz de ofrecer al menos lo siguiente:

Incorporación rápida y ajuste preciso

Las reglas de detección, exclusiones y parámetros deberán personalizarse para cada entorno de IT y las amenazas que enfrenta la organización. Una incorporación rápida es deseable, pero no a costa del rendimiento de la detección, que debe ser optimizado desde el primer día.

➜ Recuerda que la protección MDR generalmente mejorará con el tiempo.

Velocidad

Reduce el tiempo de detección y respuesta de incidentes de meses a minutos con tu proveedor de MDR. Es necesario detener el ataque en las fases iniciales (descubrimiento, movimiento lateral, persistencia) antes de que se ejecute el payload.

Servicio 24/7

Los actores maliciosos operan desde todas las zonas horarias y a menudo atacan en las primeras horas de la mañana o durante los fines de semana y festivos. Esto significa que el MDR debe funcionar las 24 horas del día, los 7 días de la semana. Los indicadores de compromiso y ataque deben investigarse de inmediato, en tiempo real.

Solución fácil de usar con una interfaz sencilla y una curva de aprendizaje baja

Esto hace que la solución sea accesible incluso para aquellos que son nuevos en la seguridad informática. El panel de control fácil de usar proporciona una visión clara del estado de seguridad y las alertas importantes.

Notificaciones personalizables y opciones avanzadas de informes

Para recibir automáticamente o bajo demanda informes sobre incidentes, el estado del entorno y otras actualizaciones.

Esto facilita la presentación del estado de la ciberseguridad a los ejecutivos, recibir alertas oportunas y generar informes accionables para auditorías y cumplimiento.

Compatibilidad perfecta con infraestructuras diversas

Integración efectiva con herramientas como SIEM, SOAR, herramientas de tickets y muchas otras. Ya sea que tengas entornos multi-SO, software de seguridad existente o configuraciones tanto locales como en la nube, deseas integrar todo sin problemas.

Un conjunto tecnológico integral

Una parte clave de una solución MDR es la tecnología subyacente. Debe incluir detección y respuesta en endpoints o detección y respuesta extendida (XDR), gestión de información y eventos de seguridad (SIEM), y orquestación y respuesta de seguridad (SOAR). Estos deben ser proporcionados por el proveedor de MDR o herramientas de terceros vinculadas a través de APIs.

Automatización e inteligencia artificial (IA)

La inteligencia artificial (IA) puede desempeñar un papel importante en la identificación de comportamientos anómalos y en el análisis de grandes volúmenes de datos para encontrar señales de compromiso o ataque.

La automatización también puede ejecutar rápidamente un conjunto de acciones para aislar sistemas y contener amenazas. Sin embargo, estas deben ser vistas siempre como herramientas de asistencia y no como un reemplazo de la experiencia de los analistas humanos.

Inteligencia humana

Tan importantes como son la IA y la automatización, tienen limitaciones que solo los expertos humanos pueden abordar de manera

➜ eficaz. Los profesionales experimentados en ciberseguridad pueden aportar una comprensión contextual de las anomalías de comportamiento señaladas por la IA para determinar si una alerta es realmente maliciosa. Esto ayuda a reducir los falsos positivos. Los humanos también son más capaces de adaptarse a nuevas amenazas emergentes en tiempo real.

Inteligencia sobre amenazas

Los feeds de inteligencia sobre amenazas actualizados regularmente, generados por el proveedor de MDR o terceros, son un componente clave de cualquier servicio MDR eficaz. Las actualizaciones deben ser recopiladas a partir de telemetría y curadas por equipos expertos en inteligencia sobre amenazas para revelar los métodos de ataque y las contramedidas efectivas.

Detección de amenazas

La detección de amenazas continua y sistemática debería ser un estándar en cualquier servicio MDR, con el fin de detectar los ataques más evasivos.

Remediación

No existe una regla establecida sobre si debe ser el proveedor de servicios o el cliente quien se encargue de la remediación/mitigación una vez que se ha descubierto una amenaza. Los compradores de IT deben buscar la oferta que mejor se ajuste a sus requisitos y capacidades internas.

Alineamiento

Asegura de que el servicio MDR se alinee operativamente con el resto del entorno de IT como, por ejemplo, si los resultados se integran con los sistemas de gestión de tickets y los flujos de trabajo internos.

Un proveedor debería ser capaz de generar informes de incidentes y actualizaciones de estado para garantizar total transparencia.

Cumplimiento

Un proveedor debería ser capaz de generar informes de incidentes y actualizaciones de estado para garantizar total transparencia.

Se espera que el mercado de MDR crezca a una tasa de crecimiento anual compuesta (CAGR) de aproximadamente

24%

desde 2024 hasta 2029.
Fuente: *MarketsAndMarkets: Managed Detection and Reponse (MDR) Market, 2024*.

Capítulo 2: Implementación de MDR con ESET

ESET ofrece uno de los servicios MDR más rápidos y efectivos del mercado. La clave de su potencia es una combinación ganadora de humanos y máquinas. Esto significa una investigación de seguridad y una inteligencia sobre amenazas de clase mundial, basadas en más de 30 años de experiencia y 11 centros de I+D, además de las capacidades de IA más avanzadas para identificar comportamientos anómalos que podrían pasar desapercibidos para los ojos humanos.

Además, los equipos de entrega del servicio ESET MDR están distribuidos por todo el mundo, lo que ayuda a los clientes a superar mejor las posibles barreras idiomáticas y hace que toda la experiencia sea más fluida.

Para clientes de empresa: ESET ofrece MDR en dos niveles. ESET MDR es un servicio potente pero asequible diseñado para satisfacer las necesidades de las pymes a partir de 25 puestos. ESET MDR Ultimate es un servicio altamente personalizado, adaptado a los requisitos específicos y el perfil de seguridad de los clientes de grandes empresas.

Funciona como una extensión fluida del departamento de IT del cliente, independientemente del sector, e incluye una respuesta completa ante incidentes con análisis forense digital (DFIR). El resultado es un servicio MDR de nivel empresarial diseñado para tener una mayor visibilidad y actuar con mayor rapidez, con el objetivo de detener y contener proactivamente las amenazas antes de que puedan causar algún daño.

Para MSPs: ESET entiende que tu empresa también puede enfrentarse a limitaciones de recursos, especialmente cuando trabaja para dar soporte a cientos de clientes a través de una superficie de ataque en constante crecimiento. Tu organización se convierte en un objetivo cada vez más atractivo, por ejemplo, como vía para que los actores maliciosos accedan de forma remota a los entornos de tus clientes.

Con ESET MDR, puedes diversificar tu cartera de servicios con detección y respuesta rápidas (en tan solo 20 minutos, potencialmente) y optimizar tus recursos internos para seguir ofreciendo el mejor servicio posible a tus clientes.

MDR COMO PARTE DE UNA SEGURIDAD HOLÍSTICA

Los servicios ESET MDR o ESET MDR Ultimate pueden adquirirse como parte de determinados niveles de suscripción a ESET PROTECT para respaldar una seguridad holística y multinivel. Estas son opciones más completas que combinan productos y servicios que abarcan la prevención, detección y respuesta. Gestionadas desde una única consola unificada, estas opciones incluyen:

ESET PROTECT MDR

Ideal para pequeñas y medianas empresas

- Consola de gestión
- Protección de endpoints
- Seguridad para el servidor
- Defensa contra amenazas avanzadas
- Cifrado de disco completo
- Gestión de vulnerabilidades y parches
- Detección y respuesta ampliada
- Autenticación multifactor
- **MDR Service**
- **Premium Support Service**

ESET PROTECT MDR Ultimate

Ideal para grandes empresas

- Consola de gestión
- Protección de endpoints
- Seguridad para el servidor
- Defensa contra amenazas avanzadas
- Cifrado de disco completo
- Gestión de vulnerabilidades y parches
- Detección y respuesta ampliada
- Autenticación multifactor
- **MDR Ultimate Service**
- **Premium Support Ultimate Service**

Conclusión

La ciberseguridad es una parte esencial de las operaciones de IT de las organizaciones. Sin embargo, en la mayoría de los casos, no es su prioridad principal, ni debería serlo. Las organizaciones necesitan poder concentrarse en su negocio principal y dejar la lucha contra una cohorte diversa, decidida y en constante crecimiento de actores maliciosos en manos de los expertos. Es aquí donde entran en juego los socios de seguridad de confianza, que aportan amplios recursos y décadas de experiencia en la industria.

MDR puede ofrecer una solución integral al integrar prevención, protección, detección y respuesta. Están disponibles servicios personalizados para satisfacer las diversas necesidades de diferentes organizaciones, ya sean pequeñas y medianas empresas (PYMES), proveedores de servicios gestionados.

MÁS INFORMACIÓN SOBRE MDR

¿EN QUÉ CONSISTE UNA IMPLEMENTACIÓN EXITOSA DE MDR?

Electrical Consultants, Inc.

ECI es una firma líder en consultoría de diseño e ingeniería, especializada en proyectos de infraestructuras y servicios eléctricos. Con más de 37 oficinas regionales en Estados Unidos y Canadá, ECI respalda la ingeniería y construcción de instalaciones de alta tensión a escala industrial, asegurando que cada proyecto se aborde con innovación, precisión y un firme compromiso con la excelencia.

ECI se enfrentaba a un importante reto de personal, ya que contaba con un equipo reducido dedicado a la gestión de la ciberseguridad, lo que dificultaba especialmente la supervisión fuera del horario laboral y la respuesta rápida ante amenazas. La organización necesitaba una solución fiable y rentable para monitorizar y responder a las amenazas las 24 horas del día, con el fin de proteger sus activos y operaciones.

Para ECI, la implementación de ESET MDR fue sencilla y requirió ajustes mínimos. El equipo de seguridad de ESET realizó una evaluación inicial exhaustiva y afinó la configuración de alertas para optimizar la detección de amenazas. Durante todo el proceso de configuración, un ingeniero de ESET proporcionó asistencia directa, garantizando una transición fluida y eficiente.

> "ESET MDR ha detectado numerosas amenazas e incidentes que, de otro modo, habríamos pasado por alto o no habríamos respondido a tiempo. En al menos una ocasión, la detección y respuesta de MDR evitó que un pequeño incidente se convirtiera en un problema mucho mayor para nuestra empresa."

Esto es ESET

Defensa proactiva. Nuestro objetivo es minimizar la superficie de ataque.

Mantente un paso por delante de las ciberamenazas conocidas y emergentes con nuestro enfoque basado en la **prevención, impulsado por la IA y la experiencia humana**.

Experimenta la mejor protección del mercado, gracias a nuestra propia **inteligencia global sobre ciberamenazas**, recopilada y examinada durante más de 30 años, que impulsa nuestra extensa red de I+D, dirigida por **investigadores aclamados por la industria**. ESET protege tu empresa para que pueda liberar todo el potencial de la tecnología.

La prevención multicapa es lo primero

La IA más avanzada se une a la experiencia humana

Inteligencia sobre amenazas de reconocimiento mundial

Soporte personalizado e hiperlocal

eset
Digital Security
Progress. Protected.