Domina la Ciberseguridad con MDR:

La Guía Definitiva para la Detección y Respuesta Gestionada

Digital Security
Progress. Protected.

Introducción: Un Enfoque Multicapa Preventivo

El mundo está cambiando más rápido de lo que muchos defensores de la red pueden manejar. Se enfrentan a un adversario ágil y decidido, armado hasta los dientes con la última tecnología. A medida que la superficie de ataque de las empresas se amplía con cada nueva inversión digital, aumentan las posibilidades y los costes de una filtración grave de la seguridad. El coste promedio de una filtración de datos en todo el mundo asciende actualmente a casi 4,9 millones de dólares.

Para **gestionar estos riesgos crecientes**, las organizaciones deben considerar la posibilidad de adoptar un **enfoque proactivo que dé prioridad a la prevención**, diseñado para minimizar la superficie de ataque, reducir los costes y la complejidad, y mejorar la ciberseguridad.

Más de la mitad de las organizaciones que han sufrido infracciones se enfrentan a altos niveles de escasez de personal de seguridad. Este problema representa un

26.2%

entre 2023 y 2024.

Fuente: IBM: Reporte del Coste de una Filtración de Datos 2024.

Las ciberamenazas solo necesitan tener éxito una vez para causar daños significativos. Por eso, el enfoque más avanzado de la ciberseguridad corporativa combina la prevención multicapa con la detección y la respuesta. Sin embargo, el reto al que se enfrentan muchas organizaciones es que:

LAS FALTAS DE COMPETENCIAS Y LA ESCASEZ DE CONOCIMIENTOS afectan a su capacidad para llevar a cabo operaciones de seguridad 24/7/365 (SecOps).

LA COMPLEJIDAD de las herramientas de detección y respuesta significa que algunas empresas pueden no tener a nadie en plantilla para manejarlas.

LAS AMENAZAS CIBERNÉTICAS SON CADA VEZ MÁS SOFISTICADAS e impactantes, lo que permite a las ciberamenazas alcanzar sus objetivos con mayor rapidez.

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

LAS PRESIONES DE CUMPLIMIENTO ESTÁN AUMENTANDO, lo que amplifica el impacto negativo de los ataques en caso de incumplimiento.

Por eso, muchas **organizaciones están recurriendo a la detección y respuesta gestionadas (MDR).** Al hacerlo, pueden acceder a la potencia combinada de un equipo experto de SecOps de terceros que utiliza sofisticadas herramientas de IA para una respuesta rápida y la contención de amenazas. Los mejores servicios de MDR automatizarán el seguimiento y la elaboración de informes para mejorar el cumplimiento y la mejora continua de la ciberseguridad. Esto liberará a los equipos internos para que se centren en tareas estratégicas de mayor valor para la empresa.

$4.88 millones

fue el costo promedio mundial de una filtración de datos en 2024, lo que supone el mayor salto desde la pandemia.

Fuente: IBM: Reporte del Coste de una Filtración de Datos 2024.

Capítulo 1: Por qué tu empresa necesita MDR

Las organizaciones actuales siguen desarrollando infraestructuras y aplicaciones en la nube, apoyando el trabajo remoto y ampliando sus cadenas de suministro digitales y tradicionales. Esto brinda más oportunidades a los ciberdelincuentes altamente motivados, que aprovechan cada vez más la IA y las herramientas automatizadas, las ofertas «como servicio» y más para mejorar sus habilidades, profesionalizarse y amplificar los ataques. En este contexto, el **MDR se está convirtiendo en una necesidad para las empresas de todos los tamaños.**

DE LA PREVENCIÓN AL MDR

Los equipos de seguridad internos se esfuerzan por gestionar el volumen, la variedad, la velocidad y, en algunos casos, la sofisticación de las amenazas a las que se enfrenta su organización. El ransomware es una de las más graves. El ransomware como servicio (RaaS) es una «industria» clandestina altamente competitiva en la que las bandas innovan continuamente para eludir los controles de seguridad y aumentar sus beneficios. Según expertos en seguridad del gobierno británico, **se espera que la amenaza aumente** a medida que más adversarios se hagan con herramientas de inteligencia artificial.

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

cada 2 segundos en 2031

Fuente: Cybercrime Magazine: Las 10 principales predicciones y estadísticas sobre ciberseguridad para 2024.

«Los servicios de IA reducen las barreras de entrada, aumentando el número de ciberdelincuentes, y potenciarán su capacidad al mejorar la escala, velocidad y eficacia de los métodos de ataque existentes».

Fuente: James Babbage, Director General de Amenazas de la National Crime Agency.

Los cibercriminales están utilizando estas herramientas para acortar el tiempo que transcurre desde el acceso inicial hasta el robo de datos o el despliegue de ransomware. Se trata de un reto, no solo en el contexto del ransomware, sino en toda la gama de amenazas a las que se enfrentan las organizaciones, desde el malware de minería de criptomonedas y las redes de bots hasta los troyanos bancarios y el spyware.

El impacto acumulativo de estas tendencias debería centrar la atención de los responsables de la seguridad informática en una verdad ineludible. La motivación de los ciberdelincuentes para tener éxito es a menudo mayor que la preparación de las empresas mediante medidas preventivas. Hacen todo lo posible por entrar en el entorno corporativo sin ser vistos. Por eso, las organizaciones deben **equilibrar la prevención con la detección y la respuesta.** Esto es en lo que se centra el enfoque de prevención de ESET, **mediante la combinación de múltiples capas de tecnología de seguridad.** Su objetivo es proteger mediante el bloqueo de código o actores maliciosos para que no entren o dañen el sistema de un usuario.

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

€4.88 millones

y un

15% de participación

entre todos los ataques

Fuente: IBM: Reporte del Coste de una Filtración de Datos 2024.

Sin embargo, si estas medidas son burladas por ciberdelincuentes sofisticados, existe una detección y respuesta rápidas, y fiables para mitigar las amenazas avanzadas que consiguen comprometer un sistema. Piense en ello como si cerrara todas las puertas y ventanas con llave y cerrojo, pero luego instalara alarmas de detección de movimiento para detectar actividades sospechosas si alguien consigue entrar en casa.

El XDR es un activo clave. Permite a los equipos de operaciones de seguridad (SecOps) obtener una **visibilidad sin precedentes** de su entorno informático desde un único panel y detectar anomalías que indiquen amenazas mediante alertas de alta fidelidad. XDR es una evolución de EDR, que optimiza la detección, investigación, respuesta y caza de amenazas en tiempo real.

XDR unifica las detecciones de endpoints relevantes para la seguridad con la telemetría de herramientas empresariales y de seguridad como el análisis y la visibilidad de redes (NAV), la seguridad del correo electrónico, gestión de usuario y accesos, la seguridad en la nube, etc. Se trata de una plataforma nativa en la nube construida sobre una infraestructura de big data para proporcionar a los equipos de seguridad flexibilidad, escalabilidad y oportunidades de automatización.

XDR PERMITE RESPONDER A VARIAS PREGUNTAS CLAVE SOBRE UN CIBERATAQUE:

¿Cómo empezó?
¿Dónde comenzó?
¿Cuándo comenzó?
¿Qué endpoints están infectados?
¿Se ha contenido?
¿Cómo podemos prevenirlo en el futuro?

Y lo que es más importante, puede ayudarle a tomar medidas correctivas rápidas para resolver los incidentes antes de que afecten gravemente a la organización.

Sin embargo, incluso con la ayuda del XDR, los equipos de SecOps se enfrentan a **grandes retos** desde el punto de vista organizativo, sobre todo en lo que respecta a las carencias de conocimientos, la complejidad de las herramientas, las limitaciones presupuestarias y de recursos, y la integración de las herramientas, por no mencionar la rápida evolución del panorama de las amenazas. **Por eso, muchos están recurriendo al MDR,** la forma más eficaz de detectar y contener amenazas sofisticadas y en constante cambio.

CÓMO ABORDA EL MDR LAS AMENAZAS ACTUALES

Aunque el MDR varía de un proveedor a otro, debe incluir al menos alguna variación de lo siguiente:

- **Supervisión y detección de amenazas 24/7:** Supervisión continua de la red, los endpoints y los entornos en la nube de una organización

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

51%
es el número

de organizaciones que han establecido formalmente metodologías de caza de amenazas en 2024, en comparación con el 35% en 2023.

Fuente: SANS: La evolución de la caza de amenazas empresarial: Insights Detallados de la Encuesta SANS 2024.

- **Análisis y respuesta de expertos:**
  La experiencia de los profesionales de la 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:**
  La telemetría precisa, actual y relevante recopilada en todo el mundo proporciona inteligencia procesable para una respuesta rápida ante incidentes y una detección optimizada de amenazas.

Las organizaciones que utilizan la telemetría pueden lograr hasta un

60% de mejora

en su capacidad para gestionar vulnerabilidades y amenazas en comparación con las que se basan únicamente en medidas de seguridad tradicionales.
Fuente: : Forrester: Los cuatro pasos para una seguridad más proactiva, 2024.

- **Mejora continua:**

Al analizar incidentes pasados, utilizar inteligencia avanzada sobre amenazas, centrarse en las amenazas reales y proporcionar comprobaciones e informes periódicos sobre el estado de la seguridad, los servicios MDR ayudan a prevenir la repetición de ataques similares al permitir a los equipos mejorar la resistencia cibernética.

FUNCIONES CLAVE DEL MDR

El MDR puede aportar enormes beneficios a las organizaciones que desean mitigar los riesgos cibernéticos, pero que no disponen de los recursos internos necesarios, ayudándoles eficazmente a colmar las brechas de competencias, ahorrar costes y mejorar la detección y la respuesta. Una solución de alto rendimiento debe permitir a las organizaciones:

Supervisar

Los cibercriminales experimentados realizan un seguimiento de todo el entorno de TI del cliente y supervisan activamente el malware y los grupos APT para proporcionar el máximo nivel de conocimiento de la situación.

Detectar

Los cibercriminales tienen innumerables maneras de colarse a través de las defensas perimetrales, pero al aprovechar el análisis de comportamiento, pueden ser detectados para una rápida corrección.

Triaje

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

Priorizar

Los análisis inteligentes clasifican estas alertas por gravedad para garantizar que se abordan primero las amenazas más críticas. Esta es una fase crítica del flujo de trabajo de MDR, dado que muchos equipos de TI luchan contra la sobrecarga de alertas.

Investigar

Las herramientas automatizadas y la experiencia humana se combinan para profundizar en las alertas, realizando análisis de datos y registros para comprender su naturaleza y alcance. Tendrán que calcular si una alerta es un verdadero positivo o no, y qué pasos hay que dar para resolverla.

Responder

Un servicio MDR eficaz proporcionará acciones de respuesta básicas para bloquear y contener la amenaza, o bien contención y reparación completa de los sistemas comprometidos. Esto último podría implicar el restablecimiento de contraseñas, la aplicación de parches en endpoints específicos o incluso la restauración de los ordenadores.

Las ventajas de externalizar la detección y respuesta son sencillas, pero contundentes:

- El proveedor de MDR se encarga de toda la gestión de la tecnología back-end, liberando al personal para que se centre en tareas estratégicas de alto valor en lugar de agobiarse con alertas de seguridad.
- El proveedor de MDR también puede optimizar la tecnología back-end para alinearla con el perfil de riesgo y la infraestructura de cada cliente.
- Con la detección y respuesta gestionadas por un tercero, no habrá necesidad de pagar salarios elevados para atraer y retener a los mejores talentos en ciberseguridad.
- Los clientes pueden beneficiarse de las economías de escala de su proveedor, de su capacidad para atraer a los mejores talentos y de su conocimiento de otras organizaciones de clientes y entornos de amenazas.

CARACTERÍSTICAS ESENCIALES QUE HAY QUE BUSCAR EN UNA SOLUCIÓN MDR

Con tantas soluciones MDR inundando el mercado, puede resultar difícil saber por **dónde empezar.** Considere un proveedor capaz de ofrecer al menos lo siguiente:

Rápida incorporación y puesta con precisión

Las reglas de detección, las exclusiones y los parámetros deberán personalizarse para cada entorno de TI y las amenazas a las que se enfrenta la organización. Una incorporación más rápida es deseable, pero no si esta perjudica el rendimiento de la detección, que debe optimizarse desde el primer día.

➜ Recuerde que la protección MDR suele mejorar con el tiempo.

Velocidad

Reduzca el tiempo de detección y respuesta a incidentes de meses a minutos con su proveedor de MDR. Necesita detener el ataque en las fases iniciales (descubrimiento, movimiento lateral, persistencia) antes de que se ejecute la carga útil.

Servicio 24/7

Los ciberdelincuentes operan desde todos los husos horarios y a menudo atacan de madrugada, los fines de semana o días festivos. Esto significa que MDR debe trabajar las 24h. Los indicadores de compromiso y ataque deben investigarse inmediatamente, en tiempo real.

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

Es accesible incluso para los que inician en la seguridad informática. El panel de control fácil de usar ofrece una visión clara del estado de la seguridad y de las alertas importantes

Notificaciones personalizables y opciones avanzadas de generación de reportes

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, la recepción de alertas oportunas y la generación de informes procesables para auditorías y cumplimiento de normativas.

Compatibilidad perfecta con diversas infraestructuras

Integración eficaz con herramientas como SIEM, SOAR, herramientas de tickets y muchas otras. Tanto si dispone de entornos con varios sistemas operativos, software de seguridad existente o configuraciones tanto locales como en la nube, lo que desea es una integración sin problemas.

Una plataforma tecnológica completa

Una parte clave de una solución MDR es la tecnología subyacente. Debe incluir la detección y respuesta ampliada (XDR), la gestión de eventos e información de seguridad (SIEM) y la orquestación y respuesta de seguridad (SOAR). Todo ello debe ser proporcionado por el proveedor de MDR o por herramientas de terceros vinculadas a través de APIs.

Automatización e IA

La IA puede desempeñar un gran papel en la identificación de comportamientos anómalos y el análisis de grandes volúmenes de datos para encontrar indicios de compromiso o ataque.

La automatización también puede ejecutar rápidamente un conjunto de acciones para aislar los sistemas y contener las amenazas. Pero siempre debe considerarse como una ayuda y no como un sustituto de la experiencia de los analistas humanos.

Inteligencia humana

Por muy importantes que sean la IA y la automatización, tienen limitaciones que solo los expertos humanos pueden abordar con eficacia. Los profesionales experimentados en ciberseguridad pueden añadir una comprensión contextual de las anomalías de comportamiento marcadas 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 las amenazas nuevas y emergentes en tiempo real.

Inteligencia sobre amenazas

La constante actualización de la información sobre amenazas, por parte del proveedor de MDR o terceros, es esencial en un servicio MDR eficaz. XDR integra las detecciones de endpoints con la telemetría de herramientas de seguridad y empresariales, como el análisis y visibilidad de la red (NAV), la seguridad del correo electrónico, gestión de usuario y accesos, la seguridad en la nube, etc. Es una plataforma nativa en la nube construida sobre una infraestructura de big data que brinda flexibilidad y escalabilidad a equipos de seguridad.

Búsqueda

Cualquier servicio MDR debe incluir de forma estándar una búsqueda continua y sistemática de amenazas, con el fin de erradicar los ataques más evasivos.

Reparación

No hay ninguna norma establecida sobre si el proveedor de servicios o el cliente debe encargarse de la corrección o mitigación una vez descubierta una amenaza. Los compradores de TI deben buscar la oferta que mejor se adapte a sus necesidades y capacidades internas.

Alineación

Asegúrese de que el servicio MDR se alinea operativamente con el resto del entorno de TI, por ejemplo, si las salidas se integran con los sistemas de gestión de tickets y los flujos de trabajo internos.

Un proveedor debe ser capaz de generar informes de incidencias y actualizaciones de estado para una total transparencia.

Cumplimiento

El servicio MDR debe ser capaz de cumplir los requisitos de privacidad, residencia o retención de datos que pueda tener el cliente, así como las estipulaciones exigidas por las pólizas de seguros.

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

24%

de 2024 a 2029

Fuente: MarketsAndMarkets: Mercado de detección y respuesta gestionadas (MDR), 2024.

Capítulo 2: Implementación de MDR con ESET

ESET ofrece uno de los servicios de MDR más rápidos y eficaces del mercado. La clave de su poder es una combinación exitosa de humanos y máquinas. Esto significa investigación de seguridad e inteligencia de amenazas de clase mundial -construida sobre la base de más de 30 años de experiencia y 11 centros de Investigación y Desarrollo- más capacidades líderes de IA para identificar comportamientos anómalos que los ojos humanos podrían pasar por alto.

Además, los equipos de prestación de servicios de ESET MDR están repartidos por todo el mundo, lo que ayuda a los clientes a superar mejor las posibles barreras lingüísticas y hace que toda la experiencia sea más fluida.

Para clientes empresariales: 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 asientos. ESET MDR Ultimate es un servicio altamente personalizado adaptado a los requisitos específicos y al perfil de seguridad de los clientes empresariales.

Funciona como una extensión sin fisuras de la función de TI del cliente -sea cual sea su vertical- y ofrece una completa Respuesta Digital Forense a Incidentes (DFIR). El resultado es un MDR de nivel empresarial diseñado para ver más y actuar más rápido, con el fin de detener y contener proactivamente las amenazas antes de que puedan causar daños.

Para proveedores de servicios gestionados (MSP): ESET entiende que su negocio también puede sufrir limitaciones de recursos, especialmente al trabajar para apoyar a potencialmente cientos de clientes a través de una superficie de ataque en crecimiento. Su organización es un objetivo cada vez más atractivo, por ejemplo, como un medio para que los ciberdelincuentes accedan de forma remota a los entornos de los clientes.

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

MDR COMO PARTE DE LA SEGURIDAD INTEGRAL

Los servicios de ESET MDR o ESET MDR Ultimate se pueden adquirir como parte de niveles de suscripción específicos de ESET PROTECT para apoyar la seguridad integral en múltiples capas. Estas son opciones más completas que combinan productos y servicios que cubren prevención, detección y respuesta. Gestionados a través de un solo panel de control, estos incluyen:

ESET PROTECT MDR

Ideal para pequeñas y medianas empresas

- Consola de gestión
- Protección moderna de endpoints
- Seguridad de servidores
- Defensa avanzada frente a amenazas
- Cifrado de disco completo
- Gestión de vulnerabilidades y parches
- Detección y respuesta ampliadas
- Autenticación multifactor
- **Servicio MDR**
- **Servicio de soporte Premium**

ESET PROTECT MDR Ultimate

Ideal para organizaciones de nivel empresarial

- Consola de gestión
- Protección moderna de endpoints
- Seguridad de servidores
- Defensa avanzada frente a amenazas
- Cifrado de disco completo
- Gestión de vulnerabilidades y parches
- Detección y respuesta ampliadas
- Autenticación multifactor
- **Servicio MDR Ultimate**
- **Asistencia Premium Ultimate Service**

Conclusión

La ciberseguridad es una parte esencial de las operaciones de TI de las organizaciones. Sin embargo, en la mayoría de los casos, no es su enfoque principal, ni debería serlo. Necesitan poder concentrarse en su negocio principal y dejar la batalla contra un grupo diverso, decidido y en crecimiento de ciberdelincuentes a los expertos. Aquí es donde entran los socios de seguridad de confianza, que aportan amplios recursos y décadas de experiencia en la industria.

MDR puede ofrecer una solución integral al abarcar prevención, protección, detección y respuesta. Los servicios personalizados están disponibles para satisfacer las diversas necesidades de varias organizaciones, ya sean PYMEs, MSPs o grandes empresas. Es hora de eliminar el riesgo cibernético con asistencia experta.

APRENDE MÁS SOBRE MDR

¿CÓMO ES UNA IMPLEMENTACIÓN EXITOSA DE MDR?

Electrical Consultants, Inc.

ECI es una firma de consultoría de diseño e ingeniería de primer nivel especializada en proyectos de servicios públicos de energía e infraestructura. Con más de 37 oficinas regionales en los Estados Unidos y Canadá, ECI apoya la ingeniería y construcción de instalaciones de alta tensión a gran escala, asegurando que cada proyecto se aborde con innovación, precisión y una dedicación a la excelencia.

ECI enfrentó un desafío significativo de personal, con solo un pequeño equipo dedicado a gestionar la ciberseguridad, lo que hacía que la monitorización fuera de horas y la respuesta rápida a las amenazas fueran particularmente difíciles.

La organización necesitaba una forma confiable y rentable de monitorear y responder a las amenazas las 24 horas del día para proteger sus activos y operaciones.

Para ECI, la implementación de ESET MDR fue sencilla, requiriendo ajustes mínimos. El equipo de seguridad de ESET realizó una evaluación inicial exhaustiva y ajustó la configuración de alertas para optimizar la detección de amenazas.

A lo largo del proceso de configuración, un ingeniero de ESET proporcionó apoyo práctico, asegurando una transición fluida y eficiente.

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

Somos ESET

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

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

Experimenta una protección de primera clase, gracias a nuestra **inteligencia global de amenazas cibernéticas,** compilada y examinada durante más de 30 años, que impulsa nuestra extensa red de Investigación y Desarrollo, liderada por **investigadores aclamados por la industria**. ESET protege tu empresa para que puedas aprovechar todo el potencial de la tecnología

Multicapa, prevención ante todo

Combinación de IA avanzada y experiencia humana

Inteligencia de prestigio mundial sobre amenazas

Asistencia personalizada e hiperlocal

eset
Digital Security
Progress. Protected.