Productos de CrowdStrike

CROWDSTRIKE

SERVICIOS GESTIONADOS DE DETECCIÓN Y RESPUESTA (MDR)

GUÍA PARA COMPRADORES

INTRODUCCIÓN

¿QUÉ ES MDR?

La escasez crónica de profesionales y expertos en ciberseguridad está afectando a organizaciones de todos los tamaños, en todos los sectores y en todo el mundo. El problema se acentúa en un momento en que los atacantes no dejan de mejorar sus técnicas, lo que les permite ejecutar ataques con mayor rapidez y eficacia. Para las empresas no es fácil ir más allá del enfoque de seguridad preventivo y afrontar la necesidad de detección temprana, Threat Hunting proactivo, y respuesta rápida y eficaz a las amenazas de forma permanente (24/7). Contratar a un equipo de seguridad y dotarlo de recursos para llevar a cabo todas estas tareas puede ser viable para las empresas de mayor tamaño con presupuestos holgados, pero la gran mayoría, con recursos más limitados, lo tendrá muy complicado.

Ante esta necesidad del mercado, surge la detección y respuesta gestionadas (MDR, Managed Detection and Response). MDR ayuda a las empresas mediante la implementación o mejora de las funciones de detección, respuesta, gestión y supervisión permanente de amenazas, todo ello ofrecido como un servicio.

Los proveedores de MDR emplean detección y respuesta para endpoints (EDR), así como otras tecnologías para conseguir visibilidad de los eventos relacionados con la seguridad en toda la organización, con el fin de facilitar la detección de amenazas y la investigación de incidentes. Analistas (humanos) supervisan las alertas y ayudan a dar una respuesta. Esa respuesta incluye la investigación de las alertas (clasificación), la adopción de medidas prácticas para reducir el impacto y el riesgo (mitigación) y, por último, la eliminación total de la amenaza y la reversión del endpoint a un buen estado conocido (remediación).

Busca una solución MDR que garantice resultados y que:

- Añada a tu equipo una amplia experiencia
- Erradique las amenazas en minutos y se encargue de la remediación
- Reduzca de manera significativa el riesgo de ciberseguridad y los costes asociados

¿POR QUÉ NECESITAN LAS EMPRESAS UNA SOLUCIÓN MDR?

La implementación de un programa de seguridad para endpoints puede ser extremadamente complicada. Es posible que las herramientas necesarias sean difíciles de utilizar y que requieran una gran cantidad de recursos humanos para su implementación, soporte y mantenimiento. Por esta razón, son muchas las empresas que no consiguen sacar el máximo provecho de las tecnologías de seguridad para endpoints que han adquirido. Esto se agrava en el caso de empresas que desean establecer una postura de seguridad sólida para endpoints. La exigencia de mayores niveles de seguridad inevitablemente implica tener que disponer de más recursos, con el consiguiente aumento del coste y la complejidad de la administración.

¿El resultado? Muchas empresas no consiguen implementar un programa de seguridad para endpoints básico, no digamos ya uno global. La situación se complica cuando se producen incidentes graves y la empresa no dispone de tiempo ni de experiencia para corregir adecuadamente la situación, lo que puede poner en peligro su seguridad.

Los retos que el MDR ayuda a afrontar:

- **Dificultades para implementar totalmente y configurar correctamente la tecnología que han adquirido.** Según el tamaño y la carga de trabajo de sus equipos de TI, es posible que algunas empresas carezcan de las herramientas o el ancho de banda necesarios para desplegar la solución en sus endpoints rápidamente y con éxito. Además, puede que no cuenten con el tiempo ni los expertos para configurar y ajustar convenientemente las directivas según sus requisitos de seguridad y garantizar la protección de los endpoints dada la constante evolución de las amenazas y el entorno. Esto podría provocar que la solución para endpoints solo se desplegara parcialmente y no se configurara correctamente, lo que generaría lagunas en la seguridad que pueden dejar a la empresa desprotegida ante las brechas.

- **Una sobrecarga diaria de alertas e incidentes.** Gestionar el ingente número de alertas que generan algunos productos de seguridad de endpoints puede ser agotador, incluso para las empresas que disponen de un equipo de seguridad dedicado o un centro de operaciones de seguridad (SOC). Para responder a las alertas no solo se necesita personal; el 67 % de los responsables de la toma de decisiones sobre tecnología consideran que las operaciones de seguridad son hoy como mínimo igual de difíciles que hace solo dos años.[1] Desafortunadamente, la mayoría de las empresas carecen tanto del personal como de la experiencia, lo que provoca que queden alertas sin comprobar, con el consiguiente riesgo de sufrir brechas importantes.

- **Las organizaciones carecen de recursos necesarios para aplicar la corrección adecuada tras los incidentes.** Si carecen de los recursos y el personal adecuado, las empresas no pueden conocer la naturaleza y el alcance de los incidentes a tiempo. El 80 % de los responsables de la toma de decisiones creen que la escasez de personal de seguridad afecta al nivel de vulnerabilidad de las empresas,[2] lo que a su vez puede dar lugar a que los incidentes no se corrijan de manera eficaz, no se resuelvan por completo o se tarde demasiado en gestionarlos, generando en las empresas vulnerabilidades y situaciones de peligro. Para corregir adecuadamente un incidente hace falta formación y experiencia. Muchas empresas que carecen de estos recursos se ven obligadas a llevar a cabo laboriosos procesos de recreación de imágenes de los endpoints. La alternativa que consiste en la combinación minuciosa de contramedidas —como la contención de red, la prevención de hash, la eliminación/modificación de valores de claves del registro y/o la detención/desactivación/reinicio de servicios— no es realista. Y la restauración no garantiza una total remediación del incidente.

- **Para poder implementar con éxito un programa.** Aunque la empresa cuente con los fondos suficientes para crear un programa de protección de endpoints interno, la implementación de una estrategia de seguridad madura requiere mucho tiempo; se pueden tardar meses, e incluso años, en encontrar y contratar a los expertos adecuados y adquirir la tecnología necesaria, definir las directivas y crear un proceso de respuesta a incidentes. Además, este tipo de programas suelen ser menos prioritarios que otros proyectos de TI más urgentes, por lo que se suele atrasar su implementación, lo deja a las empresas en situación de vulnerabilidad.

- **Dificultades para encontrar y retener a los expertos necesarios.** Para las empresas, incorporar al personal necesario para garantizar una protección eficaz de los endpoints puede ser todo un reto. Según el Consorcio Internacional de Certificación de Seguridad de Sistemas de Información, hay más de 3,4 millones de puestos vacantes en ciberseguridad en todo el mundo.[3] Ni siquiera las empresas que disponen de recursos económicos se libran de la enorme dificultad que plantea la contratación, formación y retención del personal cualificado necesario para hacer frente de manera adecuada a un panorama de amenazas avanzadas y sofisticadas. La escasez de personal cualificado es un problema que afecta de manera generalizada a toda la industria.

¿CUÁLES SON LOS ELEMENTOS FUNDAMENTALES DE LOS SERVICIOS DE MDR?

Los servicios gestionados de detección y respuesta se centran en reducir el plazo entre la detección y la respuesta para minimizar el riesgo de manera eficaz, gracias a la disminución del tiempo de permanencia del ciberdelincuente. Cuanto más rápidamente detecte y responda a la amenaza el proveedor de MDR, más rápida será la remediación.

Para ofrecer resultados satisfactorios a los clientes, un servicio de MDR debe contar con una serie de funciones básicas que permiten proporcionar una detección y respuesta rápidas: una plataforma sólida, Threat Hunting humano continuo, supervisión e investigación 24/7 y un proceso minucioso

1 *Fuente:* Informe de ESG 2023: SOC Modernization and the Role XDR. (https://research.esg-global.com/reportaction/515201525/Toc)
2 *Fuente:* Informe de ESG 2023: SOC Modernization and the Role XDR. (https://research.esg-global.com/reportaction/515201525/Toc)
3 *Fuente:* Informe de ESG 2023: SOC Modernization and the Role XDR. (https://research.esg-global.com/reportaction/515201525/Toc)

de remediación. Si falta cualquiera de estos componentes básicos, se hace considerablemente más difícil controlar el ciclo de vida completo del incidente de seguridad y poder devolver rápidamente el sistema a un buen estado conocido.

UNA PLATAFORMA SÓLIDA

Es fundamental contar con una plataforma de seguridad sólida para proporcionar MDR que cumpla las expectativas. La plataforma debe bloquear los ataques y, al mismo tiempo, capturar y grabar toda la actividad de los endpoints para facilitar análisis más profundos y Threat Hunting.

Una plataforma sólida necesita:

1. Una plataforma nativa de la nube y fácil de desplegar que reduzca los costes y complejidades, ya que proporciona una rentabilidad inmediata y no requiere hardware, software adicional ni configuraciones.
2. Un motor de análisis de comportamientos y aprendizaje automático para proporcionar visibilidad total en tiempo real e información de todo lo que ocurre a lo largo y ancho de su entorno.
3. Un solo agente ligero para proporcionar a la plataforma telemetría detallada de todo el entorno, incluidos endpoints, cargas de trabajo en la nube e identidades.

Lógicamente, la plataforma solo ofrece buena protección si se despliega completamente y se configura de manera adecuada. Un proveedor de MDR debe aportar su experiencia y mejores prácticas para facilitar el despliegue, la configuración y el ajuste de la plataforma. Esto tiene un impacto inmenso en la postura de seguridad y garantiza una rentabilización muy rápida, ya que la incorporación se realiza en cuestión de días, en lugar de llevar semanas o más tiempo.

THREAT HUNTING CONTINUO REALIZADO POR HUMANOS

La detección de amenazas puede descubrir muchos tipos de vulnerabilidades en el entorno de TI. La mayoría de las veces, la detección se basa en algoritmos y automatización, que son métodos rápidos y eficaces, capaces de bloquear las amenazas en tiempo de ejecución. Sin embargo, no hay que olvidar que los responsables de algunos ataques son personas que conocen bien las contramedidas utilizadas para detectar sus actividades y se esfuerzan en evadirlas y permanecer ocultos. La detección de este tipo de ataques ocultos y avanzados requiere un enfoque más proactivo.

Con el Threat Hunting, los expertos se encargan de analizar meticulosamente los datos para detectar señales casi imperceptibles de amenazas emergentes y ataques sofisticados. Estas señales pueden deberse a que los ciberdelincuentes utilizan tácticas, técnicas y procedimientos (TTP) nuevos (o no conocidos), usan credenciales robadas para suplantar la identidad de usuarios autorizados, o bien emplean herramientas y software locales para aprovechar los recursos existentes y camuflarse entre la actividad de administración cotidiana.

Un servicio de MDR que no proporcione detección realizada por humanos y prevención basada en la tecnología pierde la oportunidad de neutralizar las ciberamenazas conocidas en el perímetro y descubrir las más sofisticadas que pasan desapercibidas.

SUPERVISIÓN E INVESTIGACIÓN 24/7

Una vez que se ha creado una alerta de seguridad, es el analista de seguridad quien debe determinar qué medidas se deben aplicar, en caso necesario. Una parte del proceso de análisis de las amenazas se puede automatizar mediante técnicas de análisis en entornos aislados y de comportamientos, que proporcionan inteligencia práctica e indicadores de compromiso (IoC) personalizados, adaptados a las amenazas encontradas.

La detección de los ataques ocultos y avanzados requiere un enfoque más proactivo. Con el Threat Hunting, habrá personas especializadas examinando meticulosamente los datos de seguridad de la empresa en busca de señales imperceptibles de amenazas emergentes y ataques sofisticados.

Sin embargo, si bien muchas tareas de la fase de análisis se pueden automatizar, se necesitará una evaluación realizada por humanos para descifrar el resultado de las cargas de trabajo automatizadas y comprender realmente la veracidad, el alcance y las implicaciones de un ataque.

Además, un servicio de MDR que filtre las alertas de seguridad y centre su atención en las más graves, ignorando las de importancia media y baja, limita su eficacia, ya que los ataques suelen comenzar como una larga cadena de incidentes de seguridad no muy graves que, cuando se ignoran, permiten al atacante obtener acceso y afianzar su presencia en su red. Un servicio de MDR que analice todas las detecciones y alertas de seguridad de amenazas que se han evitado, lo que puede ser indicio de la existencia de un ataque de mayor envergadura, garantiza la neutralización de las intrusiones en la fase más temprana posible.

REMEDIACIÓN QUIRÚRGICA

Es necesario responder a las alertas de amenazas que verdaderamente constituyen un peligro para la empresa. Las fases de análisis e investigación deberían ofrecer el contexto necesario para determinar qué tipo de respuesta se precisa.

Las respuestas pueden ser muy diversas y pueden incluir eliminar el endpoint del entorno y aislarlo, con el objetivo de devolver el sistema a un buen estado conocido. Para muchas empresas, esto puede requerir la recreación de la imagen del endpoint. Sin embargo, con un buen contexto, analistas cualificados y herramientas eficaces, no es necesario llevar a cabo esa medida drástica. Esta es una ventaja importante de los proveedores de MDR, ya que el incidente se puede resolver totalmente sin implicar al cliente, con menos impacto en el negocio y un menor coste, además de más rápidamente que si se recrea totalmente el sistema a partir de la imagen.

La remediación constituye el último paso de la respuesta a un incidente — la recuperación—, que implica restaurar los sistemas a su estado previo al ataque, eliminar el malware, limpiar las entradas del registro y eliminar a los intrusos, así como cualquier mecanismo de persistencia que hayan utilizado. Esta fase final es la más importante y es fundamental realizarla correctamente, ya que, en caso contrario, toda la inversión en las demás fases de un programa MDR prácticamente se desperdicia. Los ciberdelincuentes se valen de innumerables artimañas para mantener su presencia una vez que han conseguido acceder a una red. Las tareas planificadas, los servicios de vigilancia y las puertas traseras redundantes son solo algunos de los métodos que utilizan para asegurarse de que su intrusión será resiliente frente a las contramedidas de cuarentena y contención básicas.

Con la gran variedad de servicios que incluye la categoría de MDR, es fundamental conocer bien las funciones que debe proporcionar un servicio de MDR y de qué manera satisfacen tus necesidades específicas como cliente.

¿QUÉ PARÁMETROS DEBE CUMPLIR TU SERVICIO DE MDR?

CrowdStrike ha definido un nuevo parámetro de ciberseguridad basado en información obtenida mientras ayudamos a miles de empresas a protegerse frente a las amenazas. Se conoce como "tiempo de propagación" y se refiere al tiempo que tarda un intruso en desplazarse lateralmente desde la zona de ataque inicial a otros sistemas de la red. El tiempo medio de propagación en 2022 era de 1 hora y 38 minutos.[5] Sin embargo, este dato omite algunos detalles: en el 36 % de los casos, el equipo de OverWatch descubrió que el atacante pudo desplazarse lateralmente a otros hosts en menos de 30 minutos.

LO VERDADERAMENTE DETERMINANTE PARA OFRECER RESULTADOS A LOS CLIENTES DE MDR: GARANTIZAR EL RESULTADO

"Tu solución MDR debe ofrecer la remediación como parte de la respuesta. Para las empresas, detener una intrusión antes de que se convierta en brecha es cuestión de tiempo. Puede requerir aislar de la red un sistema afectado, anular procesos, eliminar mecanismos de persistencia del sistema de archivos o entradas del registro de Windows, o llevar a cabo las más variadas acciones".[2]

4 Blog de Crowdstrike: ¿Tu solución de MDR te da soluciones o te da trabajo?

5 Global Threat Report 2023 de CrowdStrike

El tiempo de propagación pone de relieve el estrecho margen de tiempo del que dispone una empresa para impedir que un incidente se convierta en una brecha de seguridad. Si bien no es el único parámetro que permite juzgar el grado de sofisticación del ciberdelincuente, el tiempo de propagación aporta un medio interesante para evaluar su capacidad operativa. Resulta igualmente útil para los profesionales de la seguridad que desean evaluar el tiempo medio para la detección, la investigación y la remediación. CrowdStrike lo ha bautizado como "la regla 1-10-60" y recomienda que las empresas hagan todo lo posible para cumplir los siguientes parámetros de rendimiento:

- Detectar una intrusión en un plazo medio de 1 minuto.
- Investigar y conocer el incidente en menos de 10 minutos.
- Expulsar al adversario en menos de 60 minutos.

Las empresas que operan dentro de este marco tienen muchas más probabilidades de expulsar a los adversarios antes de que avancen más allá del punto de entrada inicial, minimizando así el impacto de su ataque. Por supuesto, las empresas pueden ajustar su objetivo de tiempo de respuesta según sus necesidades concretas. Esto dependerá en parte del tipo de atacantes a los que tienen más posibilidades de enfrentarse, teniendo en cuenta su sector empresarial y la región en la que operan principalmente. Sin embargo, al aplicar una estrategia de MDR, la regla 1-10-60 ofrece un marco que permite a cualquier empresa adecuar sus funciones al nivel de eficacia operativa que debería proporcionarle la confianza necesaria en su capacidad de detener una brecha de seguridad.

¿QUÉ DEBE TENER SIEMPRE UN SERVICIO DE MDR?

Antes de seleccionar un servicio de MDR, hay que plantearse las siguientes cuestiones.

¿Qué experiencia tienen los analistas que se encargan del servicio de MDR?
Una razón fundamental para invertir en un servicio de MDR es añadir a tu propia plantilla expertos que aportan mejores conocimientos y un mayor grado de madurez, sin necesidad de realizar costosas inversiones en captación y contratación de personal. CrowdStrike se encuentra en una posición inigualable para contratar y retener expertos en Threat Hunting y analistas de seguridad de élite con experiencia en distintos sectores, incluida la Administración pública, la comunidad de inteligencia, empresas comerciales y la defensa. El equipo de CrowdStrike ha demostrado su eficacia a la hora de detectar y detener las amenazas más sofisticadas.

¿Cuánto se tarda, de media, en incorporar y adaptar la solución MDR a tus necesidades?
Conseguir una postura de madurez en seguridad no es fácil. Tras dedicar tiempo y esfuerzo a elegir la solución MDR adecuada para tu organización, quieres ver los resultados inmediatamente y garantizar la protección. El desfase entre la decisión y la protección suele ser grande y genera lagunas de protección en la empresa. Incorporar y poner en marcha CrowdStrike Falcon Complete lleva solo unos 10 días de media, lo que acelera la protección de la empresa y consigue pasar de las palabras a los hechos.

¿ES MDR LO MISMO QUE MSSP?

Muchas empresas se preguntan, "¿Necesito un servicio de MDR si ya tengo un proveedor de servicios de seguridad gestionados (MSSP)?". Las ofertas de los MSSP pueden variar enormemente pero, en general, se centran en la supervisión y la administración de las herramientas de seguridad en una empresa. Esto incluye normalmente una clasificación básica de las alertas de seguridad, junto con otros servicios, como administración y actualizaciones de la tecnología, cumplimiento de normativas y gestión de vulnerabilidades.

Los servicios de MDR, por su parte, son mucho más especializados y ofrecen integración rápida e inmediata, normalmente con una plataforma tecnológica específica. Además, los servicios de MDR están más centrados en el objetivo de ayudar a las empresas a conseguir que sus SOC incorporen pasos específicos del flujo de trabajo de detección/respuesta. Gracias a este enfoque concreto, los servicios de MDR ofrecen valor inmediato por un reducido coste y en un período de tiempo muy corto.

¿Qué tipo de tecnologías de prevención automatizadas integra tu solución MDR?
Una solución MDR integral que se escale de forma adecuada para tu empresa ahora y en el futuro debe incluir las ventajas de una tecnología de prevención automatizada. Gracias a CrowdStrike Security Cloud y con una excelente inteligencia artificial, la plataforma CrowdStrike Falcon® emplea indicadores de ataque en tiempo real, inteligencia sobre amenazas, información de las herramientas evolutivas de los adversarios y telemetría enriquecida con datos de toda la empresa, para facilitar detecciones hiperprecisas, protección y remediación automatizadas, Threat Hunting de élite y visibilidad de las vulnerabilidades por prioridades. Esto facilita un despliegue escalable y rápido, una protección y un rendimiento de primer nivel, una reducción de la complejidad y una rentabilidad inmediata.

¿Incluye tu MDR servicios gestionados en la nube para la protección contra amenazas para la identidad?
Actualmente, el 80 % de las brechas de seguridad incluyen la vulneración de credenciales. Sin embargo, a pesar de su prevalencia, los ataques basados en la identidad siguen siendo extremadamente difíciles de detectar mediante un enfoque tradicional. Cuando se vulneran las credenciales válidas de un usuario y un atacante las utiliza para suplantar su identidad, suele ser muy difícil distinguir si se trata del comportamiento típico del usuario o si es el hacker el que actúa. Falcon Complete Identity Threat Protection (ITP) resuelve este problema. Es el primer y único servicio de protección de la identidad totalmente gestionado que proporciona prevención continua de amenazas para la identidad en tiempo real con implementación de directivas de TI avanzadas para cuentas gestionadas y no gestionadas, y administración, supervisión y corrección realizada por especialistas.

¿Emplea tu servicio MDR inteligencia de amenazas nativa e integrada?
Para detectar y responder a las amenazas emergentes con máxima eficacia, es fundamental dotar a los analistas de seguridad de inteligencia actualizada sobre las últimas técnicas, tácticas y procedimientos utilizados por los ciberdelincuentes activos. Los servicios de MDR de CrowdStrike disponen de la inteligencia sobre ciberamenazas que proporciona el equipo de élite de analistas de amenazas de CrowdStrike. CrowdStrike Intelligence reúne a investigadores de seguridad, expertos culturales y lingüistas para añadir al proceso de MDR información detallada y actualizada de las técnicas empleadas, obtenida de más de 200 atacantes. Este profundo conocimiento de las últimas técnicas, tácticas y procedimientos permite a CrowdStrike poner en práctica procedimientos de detección y respuesta eficaces y eficientes.

¿Cómo se va a comunicar el proveedor de MDR con tu equipo?
En todo servicio de MDR, durante el flujo de trabajo de detección/investigación/respuesta, hay un momento en el que el equipo del cliente debe asumir el control de nuevo. Comunicar este traspaso de control suele generar fricción y puede requerir la introducción de nuevas consolas, portales o flujos de trabajo que ralentizan la respuesta de tu equipo. Es esencial contar con una ubicación centralizada para facilitar el intercambio fluido de información entre el proveedor de MDR y el cliente. CrowdStrike Message Center reduce la fricción en la colaboración de MDR y permite una comunicación fluida, transparente y segura entre los analistas de servicios gestionados de CrowdStrike y los clientes. Gracias a CrowdStrike Message Center, integrado en la plataforma Falcon, los analistas de CrowdStrike pueden comunicar a los clientes en tiempo real información actualizada sobre los ataques en curso y la actividad relacionada, de manera que estén siempre convenientemente informados sobre las intrusiones y cualquier medida de mitigación que deban aplicar. Las comunicaciones son bidireccionales, por lo que CrowdStrike y los analistas del cliente se pueden comunicar libremente y colaborar en la plataforma Falcon.

Los servicios gestionados de remediación deben restaurar perfectamente los sistemas al estado previo al ataque, eliminar el malware, limpiar el registro, expulsar a los intrusos y eliminar los mecanismos de persistencia, evitando los procesos de restauración, siempre que sea posible.

¿Qué acciones de respuesta realizará tu servicio de MDR y cuáles deberás aplicar tú mismo?
La respuesta suele ser un término impreciso que provoca confusión en el mercado en cuanto a qué hace exactamente el proveedor de MDR y de qué parte del trabajo deben encargarse los clientes una vez que él haya terminado. Tu servicio de MDR debe ser capaz de aislar, contener y erradicar a los atacantes del entorno; esta fase de erradicación suele marcar el momento de traspaso de la responsabilidad al cliente y puede crear una cantidad importante de trabajo, una vez realizado el aislamiento y la contención. Falcon Complete se encarga de la gestión de esta última fase y lleva la respuesta un paso más allá del aislamiento y la contención, asumiendo también, cuando es posible, la remediación. Esto implica la eliminación del entorno de archivos, artefactos y procesos maliciosos, recuperando inmediatamente el buen estado de la empresa. De esta forma, el cliente obtiene resultados, en lugar de trabajo adicional.

¿Está disponible permanentemente tu servicio de MDR?
Los ciberdelincuentes no se van de vacaciones, así que tu servicio de MDR tampoco puede tomarse un descanso. Muchas empresas deciden contratar un servicio de MDR en parte para conseguir una cobertura frente amenazas las 24 horas del día, especialmente si sus propios equipos únicamente disponen de personal durante las horas de oficina.

¿Puede el proveedor de MDR reducir tu riesgo y al mismo tiempo el coste?
Para saber si tu solución MDR es capaz de reducir el riesgo y entender cómo afectan los incidentes a tus ingresos debes conocer exactamente el resultado que ofrece. CrowdStrike tiene un objetivo: detener las brechas. Falcon Complete gestiona el ciclo de vida completo de un incidente, asegurando la cadena de custodia de todos los incidentes de seguridad para que los expertos de CrowdStrike puedan estar totalmente dedicados a detener las brechas 24 horas al día, 7 días a la semana. Además, según una **una evaluación del impacto económico realizada por Forrester en 2021, por encargo de CrowdStrike**, Falcon Complete ofrece una rentabilidad de la inversión del 400 % y le ahorra a tu empresa más de 2500 horas de investigación al año.

¿Qué garantías tienes de que MDR podrá proteger tu empresa?
Abundan los servicios de MDR que dicen protegernos frente a ciberataques, pero la cuestión es "¿podemos fiarnos de que realmente es así?". Un servicio de MDR que no demuestra de manera fiable cómo cumple lo que promete y cuál es su capacidad para ejecutarlo genera dudas. Por eso CrowdStrike ha lanzado una iniciativa pionera: la **Garantía de prevención de brechas de seguridad**. CrowdStrike tiene total confianza en la protección contra brechas que ofrece, por lo que en caso de incidente, cubre los costes, para demostrar así la seguridad de que el servicio de MDR de Falcon Complete cumple su objetivo de detener los ataques.

¿Qué validación independiente tiene tu servicio de MDR?
Evaluar las soluciones MDR suele ser un proceso tedioso que requiere descifrar mensajes contradictorios sobre cuál es la solución más adecuada para cada caso concreto. Hay muchas empresas que prometen las mismas ventajas y resultados. Como parte de este proceso, debes preguntarte, "¿Qué validación independiente tiene esta solución MDR y cómo me sirve este análisis para tomar la decisión?". CrowdStrike ha sido nombrada líder en MDR por Forrester Wave y por IDC Marketscape, además de conseguir la máxima cobertura de detección en las evaluaciones de MITRE Engenuity ATT&CK® de 2022 sobre proveedores de servicios de seguridad. Consulta a estos expertos cuando vayas a evaluar una solución MDR.

¿Con qué frecuencia participa tu solución MDR en la gestión, ajuste y optimización de tu postura de MDR?
La mejora y optimización continuas son indispensables para defenderse contra las amenazas actuales. Los ciberdelincuentes son cada día más rápidos y sofisticados, por lo que es fundamental que tu servicio de MDR asuma en tu organización un papel determinante e integral en la gestión y la adaptación de la plataforma, las directivas y los procesos en lo relativo a MDR. Esto garantiza una optimización continua del servicio para ofrecer resultados y, en definitiva, para detener las brechas.

FALCON COMPLETE: UNA SOLUCIÓN MDR INTEGRAL Y EXTREMADAMENTE EFICAZ

CrowdStrike Falcon® Complete for Managed Detection and Response (MDR) combina las ventajas de Falcon, la plataforma de seguridad nativa en la nube líder del sector, con la eficiencia, la experiencia y la protección 24/7 que aporta el equipo mundial de expertos en seguridad de CrowdStrike, encargados de la supervisión, clasificación y respuesta continuas a las amenazas dirigidas contra las empresas de los clientes.

Funciones	MDR de Falcon Complete
Administración, ajuste y optimización permanentes	
Gestionada por expertos	✓
Administración proactiva de la plataforma	✓
Asesor de seguridad asignado	✓
Priorización de grupos de recursos	✓
Experiencia interdisciplinar	✓
Detección y prevención	
Supervisión continua con visibilidad en tiempo real	✓
Investigación de todas las detecciones (de gravedad baja, media, alta y crítica)	✓
Datos, herramientas y procesos especializados	✓
Protección de cargas de trabajo en nube	✓
Prevención gestionada de amenazas para identidad	✓
Threat Hunting e inteligencia	
Inteligencia sobre amenazas nativa e IoC integrados	✓
Informes de Threat Hunting trimestrales	
Total visibilidad del árbol de procesos en cualquier endpoint	✓
Threat Hunting 24/7 realizado por personas	✓
Incluye Threat Hunting proactivo realizado por personas	
Aislamiento y contención de todas las amenazas	✓
Remediación específica proactiva	✓

TU SERVICIO DE MDR DEBE GARANTIZAR RESULTADOS, NO DAR MÁS TRABAJO

Es el proveedor de MDR el que debe proporcionar estos resultados, no el cliente. Falcon Complete se compromete a cumplir estas expectativas.

Normalmente un cliente contrata un servicio de MDR por un motivo sencillo: evitar los daños de una brecha de seguridad. Muchos proveedores de MDR, que no son capaces de garantizar este resultado, desglosan los requisitos en compromisos más detallados, como el tiempo de respuesta de los analistas ante una alerta crítica. Este tipo de acuerdos de nivel de servicio (SLA) son útiles para controlar la eficacia del servicio a lo largo del tiempo, sin embargo, aunque este parámetro reduce el riesgo de brechas, dista mucho de satisfacer el objetivo principal: detener las brechas.

Falcon Complete incluye desde el primer día su Garantía de prevención de brechas de seguridad, diseñada para ofrecer a los clientes la seguridad de que CrowdStrike tiene total confianza en el equipo de seguridad y en los resultados que ofrece.

Existe una amplia gama de servicios de MDR disponibles actualmente. A la hora de elegir uno para sumarlo a tu equipo de seguridad, es importante que antes conozcas bien la capacidad del equipo para detectar, investigar y responder a las amenazas, además de sus carencias. Después, debes evaluar si el servicio de MDR proporciona cobertura total para personas, procesos y tecnología. Así podrás determinar si el servicio de MDR te obligará a realizar acciones de seguimiento (más trabajo) o simplemente te informará de que la amenaza ha sido erradicada y corregida (resultados), lo que implica de hecho detener las brechas que amenazan a tu empresa.

Reserva una demo de Falcon Complete MDR

Más información en **www.crowdstrike.com/es/**

ACERCA DE CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), líder mundial en ciberseguridad, ha redefinido la seguridad moderna con la plataforma nativa en la nube más avanzada del mundo, para proteger aspectos fundamentales del riesgo empresarial: las cargas de trabajo, la identidad y los datos, tanto en los endpoints como en la nube.

Gracias a CrowdStrike Security Cloud y una inteligencia artificial de talla mundial, la plataforma CrowdStrike Falcon® se nutre de indicadores en tiempo real, inteligencia sobre amenazas, información de las herramientas evolutivas de los adversarios y telemetría enriquecida con datos de toda la empresa, para facilitar detecciones hiperprecisas, protección y remediación automatizadas, Threat Hunting de élite y observación de vulnerabilidades por prioridades.

Desarrollada expresamente en la nube con una arquitectura de agente ligero único, la plataforma Falcon ofrece un despliegue rápido y escalable, protección y rendimiento superiores, menor complejidad y rentabilidad inmediata.

CrowdStrike: **We stop breaches.**

Blog | Twitter | LinkedIn | Facebook | Instagram