SOPHOS
Cybersecurity delivered.

Cinco principales razones para usar los servicios de MDR

Monográficos de Sophos. Septiembre de 2022

Introducción

A medida que aumentan el volumen, la complejidad y el impacto de las ciberamenazas, las organizaciones recurren cada vez más a servicios de detección y respuesta gestionadas (MDR) para detectar y neutralizar ataques avanzados que las soluciones tecnológicas por sí solas no pueden detener. De hecho, Gartner prevé que, para el año 2025, el 50 % de las empresas utilizarán la MDR para supervisar, detectar y responder a las amenazas[1].

Sin embargo, con la proliferación de soluciones de defensa en el mercado, puede resultar difícil comprender qué es la MDR exactamente, cómo encaja en la totalidad de su ecosistema de ciberseguridad y las ventajas de utilizar un servicio de MDR. En esta guía se da respuesta a estas preguntas y se ofrece orientación práctica sobre qué debe tener en cuenta a la hora de elegir un servicio de MDR.

Sophos MDR

Sophos MDR es el servicio de MDR en el que más confía el mundo, puesto que protege más de 11 000[2] organizaciones de las amenazas más avanzadas, entre ellas, el ransomware. Con la puntuación más alta en Gartner Peer Insights™[3] y el reconocimiento como mejor proveedor en el informe G2 Grid® de 2022 de servicios de MDR para medianas empresas[4], con Sophos MDR sus ciberdefensas están en buenas manos.

Qué es la MDR

Para entender las ventajas de la MDR y qué hay detrás de la creciente demanda de servicios de MDR, es importante comprender qué es la MDR y qué no es.

La detección y respuesta gestionadas (MDR) es un servicio 24/7 totalmente gestionado prestado por expertos especializados en detectar y responder a los ciberataques que las soluciones tecnológicas por sí solas no pueden detener.

No hay que confundir la MDR con la EDR (detección y respuesta para endpoints) ni la XDR (detección y respuesta ampliadas). Aunque tanto la MDR como la EDR y la XDR permiten la búsqueda de amenazas, la EDR y la XDR son herramientas que permiten a los analistas buscar e investigar posibles ataques; con la MDR, los analistas de un proveedor de seguridad buscan, investigan y neutralizan amenazas por usted.

Como su nombre indica, las herramientas de EDR trabajan con puntos de datos procedentes de tecnologías de protección de endpoints, mientras que las herramientas de XDR utilizan fuentes de datos de toda la pila de TI (incluidas las soluciones de seguridad de firewalls, correo electrónico, la nube y dispositivos móviles) para ofrecer una mayor visibilidad e información más detallada. En Sophos nos basamos en nuestras soluciones de EDR y XDR líderes en el sector para diseñar nuestro servicio de MDR.

Lo que la MDR no hace es gestionar la ciberseguridad del día a día, es decir, desplegar tecnologías de seguridad, actualizar políticas, aplicar parches o instalar actualizaciones. Los proveedores de servicios gestionados (MSP) prestan servicios de administración de seguridad TI a organizaciones que necesitan apoyo en esta área.

Quién utiliza servicios de MDR

Organizaciones de todo tipo y de todos los sectores utilizan servicios de MDR, desde pequeñas empresas con recursos de TI limitados hasta grandes compañías con equipos de SOC internos. Una pregunta más importante sería cómo trabajan las organizaciones con los servicios de MDR. Hay tres modelos principales de respuesta MDR:

- El equipo de MDR gestiona totalmente la respuesta a amenazas en nombre del cliente.
- El equipo de MDR trabaja en colaboración con el equipo interno para gestionar la respuesta a amenazas.
- El equipo de MDR avisa al equipo interno y presta asesoramiento para la remediación.

Sophos cubre los tres métodos para adaptarse a los requisitos específicos de cada cliente según sea necesario.

1 Guía de mercado de Gartner para la MDR 2021
2 En agosto de 2022.
3 Reseñas de los últimos 12 meses a fecha de 1 de agosto de 2022. El contenido de Gartner Peer Insights consiste en las opiniones de usuarios finales individuales basadas en sus propias experiencias con los proveedores que aparecen en la plataforma; no deben considerarse declaraciones de hecho, ni representan las opiniones de Gartner ni de sus afiliados. Gartner no apoya a ningún proveedor, producto o servicio mencionado en este contenido ni ofrece ninguna garantía, expresa o implícita, con respecto a este contenido, sobre su exactitud o integridad, incluida cualquier garantía de comercialización o conveniencia para fines particulares.
4 Sophos ha sido nombrado como mejor proveedor en el informe G2 Grid® de 2022 de servicios de MDR para medianas empresas.

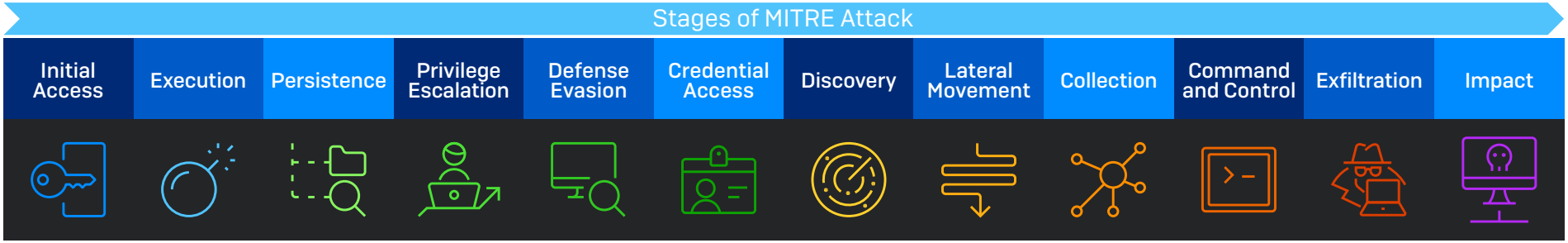
La necesidad de la detección y respuesta a amenazas a cargo de personas

La realidad es que las soluciones tecnológicas por sí solas no pueden evitar todos los ciberataques. Para no ser detectados por las soluciones de ciberseguridad, los ciberdelincuentes se sirven cada vez más de herramientas de TI legítimas, utilizan credenciales y permisos de acceso robados, y aprovechan vulnerabilidades sin parchear en sus ataques. Al hacerse pasar por usuarios autorizados y explotar los puntos débiles en las defensas de una organización, los ciberdelincuentes pueden evitar la activación de las tecnologías de detección automatizadas.

La imagen de abajo muestra los principales artefactos (herramientas) utilizados por los atacantes en cada fase de la cadena MITRE ATT&CK según lo observado en 2021 por los cazadores de amenazas en primera línea de Sophos. Como puede ver, herramientas utilizadas habitualmente por los equipos de TI, como PowerShell, PsExec y RDP, son explotadas con frecuencia por los adversarios. Las tecnologías automatizadas tienen dificultades para distinguir si son empleados de TI legítimos quienes utilizan estas herramientas o si se trata de atacantes que las explotan usando credenciales robadas.

Detener estos ataques avanzados que "viven de la tierra" requiere una combinación de tecnología y experiencia humana. Cada vez que un atacante realiza una acción, crea una señal. Si combinamos la experiencia humana con tecnologías de protección potentes y modelos de Machine Learning con IA avanzados, los analistas de seguridad pueden detectar, investigar y neutralizar incluso los ataques más avanzados perpetrados por humanos para impedir filtraciones de datos.

Si bien es posible buscar, investigar y responder a las amenazas de forma exclusivamente interna usando herramientas de EDR y XDR, utilizar un servicio de MDR, ya sea en colaboración con su equipo interno o como servicio totalmente externalizado, ofrece grandes ventajas.



Principales artefactos usados en cada fase de la cadena de MITRE ATT&CK. Manual de estrategias del adversario activo 2022, Sophos

Las tecnologías de protección continúan teniendo un papel clave en las defensas actuales

La detección y respuesta gestionadas a cargo de humanos constituye un elemento de ciberdefensa esencial, pero contar con tecnologías de protección de alta calidad sigue siendo crítico. Las tecnologías de seguridad para endpoints, redes y correo electrónico continúan desempeñando un papel fundamental en las defensas de hoy, y disponer de las soluciones más adecuadas puede incrementar la efectividad y el impacto de un servicio de MDR:

- Las tecnologías de protección automatizadas permiten a los responsables de la defensa mantenerse un paso por delante de un volumen cada vez mayor de ataques a medida que los atacantes se sirven de la automatización, la IA y el malware como servicio para multiplicar sus amenazas. Sophos Endpoint Protection bloquea el 99,98 % de las amenazas automáticamente antes de que afecten a la organización.
- Uno de los mayores desafíos prácticos a los que se enfrentan los cazadores de amenazas es el ruido: con un número tan elevado de señales, puede resultar difícil separar el grano de la paja. El uso de tecnologías de prevención superiores reduce el número de alertas que deben investigar los analistas. Al permitir a los cazadores de amenazas centrarse en menos detecciones más precisas, las tecnologías de prevención de alta calidad aceleran la respuesta a amenazas realizada por humanos.
- Los analistas utilizan detecciones y señales de las tecnologías de prevención para identificar e investigar actividades sospechosas. Cuanto mayor sea la calidad de las detecciones y más abundantes los datos contextuales, más rápidas y mejores serán la investigación y la respuesta.

Teniendo esto en cuenta, veamos ahora las cinco principales ventajas según las organizaciones que utilizan servicios de MDR.

1. Refuerce sus ciberdefensas

Una de las principales ventajas de utilizar un proveedor de MDR frente a los programas de operaciones de seguridad exclusivamente internos es una protección superior contra el ransomware y otras ciberamenazas avanzadas.

Con la MDR, se beneficiará de la amplia y profunda experiencia que aportan los analistas del proveedor. Un proveedor de MDR trata con un volumen y una variedad de ataques muy superiores a los de una organización individual, lo que les da un nivel de experiencia que es prácticamente imposible de replicar internamente.

Los equipos de MDR también investigan y responden a incidentes todos los días, por lo que utilizan las herramientas de búsqueda de amenazas con mucha más soltura. De esta forma, pueden responder con más rapidez y precisión en todas las fases del proceso, desde la identificación de señales relevantes hasta la investigación de posibles incidentes y la neutralización de actividades maliciosas.

Trabajar como parte de un gran equipo también permite a los analistas compartir sus conocimientos e información, lo que acelera aún más la respuesta. El equipo de Sophos MDR recopila runbooks para cada amenaza o atacante único con los que se encuentra. Una vez que se ha identificado a un adversario durante el transcurso del proceso, en lugar de tener que realizar una investigación extensa en el momento del ataque, nuestro equipo puede remitirse al runbook y pasar directamente a la acción.

Los runbooks se actualizan continuamente y los analistas registran información importante en cada intervención, por ejemplo:

- Las tácticas, técnicas y procedimientos (TTP) comunes o específicos de un ataque o atacante concretos.
- Indicadores de peligro (IOC) relevantes.
- Pruebas de concepto conocidas para exploits vinculados a vulnerabilidades abiertas.
- Consultas de búsqueda de amenazas útiles al gestionar un ataque o atacante concreto.

Otra ventaja de un servicio de MDR es que puede aplicar información de un cliente a otros que tengan el mismo perfil como objetivo para poder evitar de forma proactiva ataques similares en esa comunidad. Algunos escenarios de ejemplo en que el equipo de Sophos MDR investiga proactivamente los entornos de los clientes son:

- Un cliente de un sector vertical específico ha sido atacado de una manera en particular.
- Sophos X-Ops proporciona información sobre un ataque importante dirigido a un determinado sector o perfil de organización.
- Ha tenido lugar un incidente significativo en el ámbito de la seguridad y queremos cerciorarnos de si hay clientes afectados.

Si nuestros analistas detectan cualquier señal sospechosa, pueden investigar y remediar la situación rápidamente y así crear inmunidad colectiva para el grupo objetivo.

La mayor amplitud y profundidad de la experiencia y la capacidad para aplicar conocimientos en todos los entornos de nuestros clientes permiten al equipo de Sophos MDR reforzar las defensas de las organizaciones más allá de lo que conseguirían por su cuenta.

"Entre los resultados tangibles obtenidos con Sophos MDR se incluyen una reducción del 90 % en el tiempo para detectar amenazas de alto riesgo que requieren investigación, una reducción del 95 % en el tiempo para identificar el origen de un ataque y el tipo de amenazas, y una mayor precisión de las detecciones".
Chitale Dairy, India

"Los técnicos de pruebas de penetración se sorprendieron enormemente de que no lograron entrar de ninguna manera. En ese punto supimos que podíamos confiar plenamente en el servicio de Sophos".
University of South Queensland, Australia

"Con Sophos MDR, hemos reducido nuestro tiempo de respuesta a amenazas drásticamente".
Tata BlueScope Steel, India

"Recibimos notificaciones de cualquier amenaza en tiempo real".
Bardiani Valvole, Italia

2. Libere la carga de trabajo de TI

La búsqueda de amenazas lleva tiempo y es imprevisible. Para los profesionales de TI que compaginan múltiples tareas y prioridades, puede resultar difícil hacer frente al reto: el 79 % de los equipos de TI admiten que no están totalmente al día de la revisión de registros para identificar señales o actividades sospechosas[5].

Dado el posible impacto de un ataque en la organización, cuando se detecta algo sospechoso, es necesario dejarlo todo para que la amenaza pueda investigarse y gestionarse de inmediato. La urgencia inherente a este trabajo puede impedir a los equipos centrarse en tareas más estratégicas y a menudo más interesantes.

Trabajar con un servicio de MDR le permite liberar la carga de trabajo de TI para respaldar las iniciativas centradas en el negocio. Las organizaciones que utilizan Sophos MDR sistemáticamente obtienen notables mejoras de eficiencia de TI, lo que a su vez les permite perseguir más eficazmente los objetivos de su organización.

"Desde que implementamos Sophos, hemos logrado liberar un número importante de horas operativas, lo que ha permitido a nuestros equipos centrarse en iniciativas que han incrementado la satisfacción de nuestros estudiantes".
London South Bank University, Reino Unido

"La capacidad de Sophos MDR para remediar o eliminar amenazas de forma rápida y alertarnos sobre ellas nos libera para que podamos centrarnos en tareas de alto valor".
Tomago Aluminium, Australia

"Al contar con Sophos MDR, podemos respaldar y desarrollar otras áreas de la organización como la gestión de vulnerabilidades, la aplicación de parches y la concienciación sobre seguridad".
The Fresh Market, EE. UU.

"Sophos está siempre al día de la actividad y las amenazas más recientes para que nosotros podamos centrarnos en prestar un servicio seguro y de excelencia a clientes y artistas".
CD Baby, EE. UU.

5 Encuesta independiente a 5600 profesionales de TI, enero-febrero de 2022. Encargada por Sophos y realizada por Vanson Bourne.

3. Gane en tranquilidad 24/7

Hay ciberdelincuentes por todo el planeta, por lo que puede llegar un ataque en cualquier momento. Los adversarios están más activos durante las horas en que es menos probable que su equipo de TI esté online, como por la noche, los fines de semana y periodos festivos. Por lo tanto, la detección y respuesta a amenazas es una tarea que debe realizarse de manera ininterrumpida. Si solo la lleva a cabo en horario de oficina, su organización estará expuesta.

Gracias a su cobertura 24/7, los servicios de MDR ofrecen una gran tranquilidad y confianza. Para los equipos de TI esto significa, literalmente, poder dormir mejor por las noches: podrán relajarse sabiendo que el proveedor de MDR les relevará en su responsabilidad y recuperarán su tiempo personal.

Una cobertura 24/7 por parte de expertos y un alto nivel de ciberpreparación en todo momento da a altos directivos y clientes una gran tranquilidad de que sus datos y la propia organización están bien protegidos.

"Contar con el equipo de Sophos MDR me ayuda a dormir por las noches porque sé que estamos protegidos 24/7".
Vancouver Canucks, Canadá

"El equipo de Sophos actúa como nuestro portero, esperando detrás de nosotros con sus habilidades y dándonos la tranquilidad de que nos cubre las espaldas".
Inspire Education Group, Reino Unido

"Ahora tenemos más confianza en la fiabilidad, robustez y exhaustividad de nuestra infraestructura de seguridad".
Aligned Automation, India

"El negocio es ahora mucho más resiliente gracias a Sophos MDR".
McKenzie Aged Care Group, Australia

4. Añada experiencia, no personal

La búsqueda de amenazas es una operación altamente compleja. Las personas que trabajan en este ámbito deben poseer unos conocimientos específicos a la vez que muy especializados. El perfil típico de un cazador de amenazas debe caracterizarse por lo siguiente:

- **Creatividad y curiosidad**: buscar amenazas puede ser como buscar una aguja en un pajar. Los cazadores de amenazas a menudo pueden pasar días buscando amenazas, utilizando numerosos métodos para sacarlas a la luz.
- **Experiencia en ciberseguridad**: la búsqueda de amenazas es una de las operaciones más avanzadas dentro de la ciberseguridad. Es indispensable disponer de experiencia previa en el campo y conocimientos básicos.
- **Conocimiento del panorama de amenazas**: comprender las tendencias más recientes de las amenazas es imprescindible a la hora de buscar y neutralizar entidades desconocidas.
- **Mentalidad de adversario**: la capacidad de pensar como un hacker es fundamental para combatir los métodos dirigidos por humanos de hoy en día.
- **Capacidad de redacción técnica**: los cazadores de amenazas deben mantener un registro de todos sus descubrimientos como parte del proceso de investigación. Por lo tanto, la capacidad de comunicar una información tan compleja es crucial para proseguir la búsqueda hasta su conclusión.
- **Conocimiento de sistemas operativos (SO) y redes**: un conocimiento avanzado de ambos es esencial.
- **Experiencia en codificación/scripting**: necesaria para ayudar a los cazadores de amenazas a crear programas, automatizar tareas, analizar registros y realizar tareas de análisis de datos para apoyar y hacer avanzar sus investigaciones.

Reunir todas las competencias de esta lista se da muy rara vez, a lo que se suma la notable escasez de habilidades en el sector de TI. Por esta razón, contratar a expertos en búsqueda de amenazas es una tarea ardua, si no imposible, para muchas organizaciones.

Los servicios de MDR le ofrecen la experiencia que necesita. En Sophos, tenemos a cientos de analistas expertos que prestan servicios de MDR de forma continuada a clientes de todo el mundo. Sophos MDR permite a los clientes ampliar sus capacidades en operaciones de seguridad sin incrementar su plantilla.

"Ahora disponemos de un centro de seguridad ampliado sin necesidad de crear nuestro propio departamento interno".
Hammondcare, Australia

"Sophos MDR nos ha ayudado a seguir el ritmo a las ciberamenazas, cada vez más numerosas y sofisticadas, sin tener que ampliar nuestro equipo de operaciones de seguridad".
Tourism Finance Corporation of India Limited, India

"Sophos nos ahorra el gasto de contratar a cinco nuevos empleados para hacer este trabajo".
AG Barr, Reino Unido

5. Mejore su ROI de ciberseguridad

Mantener un equipo de búsqueda de amenazas 24/7 es caro. Para contar con una cobertura ininterrumpida, necesita un mínimo de cinco o seis responsables de ciberseguridad que trabajen en distintos turnos. Sirviéndose de las economías de escala, los servicios de MDR ofrecen una forma rentable de proteger su organización y estirar aún más su presupuesto de ciberseguridad.

Además, al reforzar su protección, los servicios de MDR también reducen enormemente el riesgo de sufrir una costosa filtración de datos y evitan los perjuicios financieros de gestionar un incidente grave. El coste medio de remediar un ataque de ransomware en organizaciones de tamaño mediano fue de 1,4 millones USD en 2021[6], por lo que invertir en la prevención es una sabia decisión financiera.

Si recurre a un proveedor de MDR que ofrece soluciones de ciberseguridad para endpoints y otras, puede disfrutar de importantes ventajas en materia del TCO al consolidar todas sus herramientas con un único proveedor y al agilizar la gestión de los proveedores.

Por último, si elige un proveedor que se integra con sus actuales tecnologías de seguridad, puede incrementar el retorno de sus inversiones existentes. En Sophos tenemos un enfoque a la MDR desvinculado de cualquier proveedor que le permite aprovechar sus actuales productos de detección, investigación y respuesta a amenazas, lo que aumentará su ROI. Con Sophos MDR, puede utilizar nuestras excelentes herramientas, las de otros proveedores o una combinación de ambas.

"Sophos nos cubre una carga de trabajo equivalente a la de seis empleados a tiempo completo por el coste de menos de uno".
Detmold Group, Australia

"Reunir todos nuestros productos de seguridad bajo un mismo techo nos ha permitido ahorrar dinero e impulsar la eficiencia".
Independent Parliamentary Standards Authority, Reino Unido

"Sophos MDR se amortiza con creces. Si detiene un incidente grave en un año, su coste se recupera diez veces, si no más".
Hammondcare, Australia

"Nos hemos ahorrado 15 horas por semana y la productividad se ha multiplicado por 2,6".
Tourism Finance Corporation of India Limited, India

6 El estado del ransomware 2022, Sophos. Encuesta independiente a 5600 profesionales de TI de 31 países

Qué debe tener en cuenta al seleccionar un servicio de MDR

Los servicios de MDR varían de un proveedor a otro. Hay muchas cosas que deben considerarse al evaluar los servicios. Asegúrese de plantearse las siguientes cuestiones.

1. **Niveles de soporte e interacción ofrecidos**

   ¿Quiere un proveedor de MDR que gestione por completo su respuesta a amenazas, que la gestione en colaboración con su equipo o que avise a su equipo para que tome medidas? Determine qué nivel de soporte e interacción prefiere y compare a los proveedores.

   En Sophos actuamos como una extensión de los equipos de TI de nuestros clientes de la forma en que estos lo necesiten. Tanto si desea un servicio de soporte 24/7 totalmente gestionado como si requiere apoyo para un equipo interno, nosotros nos adaptamos.

2. **Amplitud y profundidad de la experiencia en materia de amenazas**

   Una experiencia más amplia y profunda en respuesta a ciberamenazas se traduce en unas mejores defensas. Comprenda la dimensión de la experiencia a la que pueden recurrir los analistas de MDR del proveedor y cómo aplican los aprendizajes colectivos en las infraestructuras de sus clientes.

   Explore también la profundidad de los conocimientos de seguridad tras el equipo de MDR del proveedor y la calidad de los datos contextuales proporcionados para ayudar a los analistas a priorizar e investigar alertas.

   Sophos MDR protege más de 11 000 organizaciones de todo el mundo y trabaja con los sectores de sanidad, educación, fabricación, comercio minorista, tecnología, finanzas, gobierno y servicios, entre muchos otros. Esta amplia y profunda experiencia nos permite ofrecer una protección sin igual a nuestros clientes.

   Sophos MDR está respaldado por el equipo de Sophos X-Ops, con más de 30 años de experiencia en malware y capacidades de IA líderes en el mundo, que proporciona datos y análisis detallados para ayudar a los agentes de MDR a identificar y neutralizar las amenazas rápidamente.

3. **Experiencia de los clientes en el día a día**

   Un proveedor de MDR eficaz se convierte en una extensión de su propio equipo; asegúrese de que querrá trabajar con él una vez firmado el contrato. Hable con clientes del proveedor para entender sus experiencias y consulte sitios de reseñas independientes para conocer las opiniones de los clientes.

   Sophos MDR es el proveedor de MDR con más evaluaciones y mejores puntuaciones en Gartner Peer Insights a fecha de 1 de agosto de 2022, con una valoración media de 4,8/5*. Encontrará testimonios de clientes independientes aquí.

4. **Amplitud y profundidad de la telemetría**

   Los adversarios no siguen una única ruta tecnológica, y la búsqueda de amenazas de su proveedor de MDR tampoco debería. Cuanto mayor sea la visibilidad de los analistas sobre todo su entorno, mejor podrán detectar y responder a actividades maliciosas. Pregunte a los proveedores acerca de sus integraciones de seguridad y con qué amplitud pueden integrar señales de todo su entorno de TI.

   Sophos MDR proporciona extensas integraciones en toda la pila de TI, incluidas integraciones nativas y de terceros con tecnologías para endpoints, redes, la nube, el correo electrónico y Microsoft 365. Nuestro enfoque desvinculado de cualquier proveedor permite a los analistas tener una visibilidad amplia de todo el entorno del cliente, lo que a su vez refuerza la detección, investigación y respuesta a amenazas.

Resumen

A medida que evolucionan las ciberamenazas, la MDR se está convirtiendo rápidamente en una protección fundamental para las organizaciones de todos los tamaños. Trabajar con un proveedor de MDR de confianza y eficacia probada ofrece numerosos beneficios, tanto si desea externalizar por completo la búsqueda de amenazas como si prefiere complementar y mejorar sus propios servicios:

1. Refuerce sus ciberdefensas.
2. Libere la carga de trabajo de TI.
3. Gane en tranquilidad 24/7.
4. Añada experiencia, no personal.
5. Mejore su ROI de ciberseguridad.

Para obtener más información acerca de Sophos MDR, hable con su partner de Sophos o visite es.sophos.com/mdr

es.sophos.com/mdr

Sophos ofrece soluciones de ciberseguridad líderes en el sector a empresas de todos los tamaños, protegiéndolas en tiempo real de amenazas avanzadas como el malware, el ransomware y el phishing. Gracias a nuestras funcionalidades next-gen probadas, los datos de su organización estarán protegidos de forma eficiente por productos con tecnologías de inteligencia artificial y Machine Learning.

2022-09-16 ES-WP (DD)

SOPHOS