Sophos Managed Detection and Response

Respuesta a amenazas a cargo de expertos

Sophos Managed Detection and Response (MDR) es un servicio totalmente gestionado prestado por un equipo de expertos que ofrece búsqueda, detección y respuesta a amenazas 24/7.

La notificación de amenazas no es la solución, sino el punto de partida

La mayoría de las organizaciones carecen de las herramientas, el personal y los procesos internos necesarios para defenderse de las ciberamenazas y gestionar su programa de seguridad. Sophos MDR ofrece detección y respuesta a amenazas de forma ininterrumpida. Neutralizamos amenazas sofisticadas 24/7.

Sophos MDR es un servicio prestado por cazadores de amenazas y expertos en respuesta dedicados a:

- Buscar y validar de forma proactiva posibles amenazas e incidentes
- Utilizar toda la información disponible para determinar el alcance y la gravedad de las amenazas
- Proporcionar información detallada sobre el contexto de una amenaza y los posibles efectos
- Tomar medidas para interrumpir, contener y neutralizar amenazas de forma remota
- Brindar asesoramiento para abordar la causa raíz de los incidentes recurrentes

Respuesta humana acelerada por máquinas

Sophos MDR, basado en Sophos XDR, fusiona la tecnología del Machine Learning con el análisis de expertos para ofrecer una búsqueda y detección de amenazas mejoradas, una investigación más a fondo de las alertas y acciones específicas para eliminar las amenazas con rapidez y precisión. Esta fusión de la prestigiosa protección para endpoints y XDR inteligente de Sophos con un equipo de expertos en seguridad de primera categoría da lugar a lo que llamamos "respuesta humana acelerada por máquinas".

Control y transparencia totales

Con Sophos MDR, puede controlar cómo y cuándo se derivan las posibles amenazas, qué medidas de repuesta se aplican y quién se incluye en las comunicaciones. Sophos MDR ofrece tres modos de respuesta para que tenga la flexibilidad de elegir la mejor forma de trabajar con nuestro equipo de MDR durante un incidente.

Notificar: le notificamos el posible incidente, le proporcionamos los detalles del mismo y le ayudamos a priorizarlo y responder según proceda.

Colaborar: trabajamos con su equipo interno o externo para responder a la detección.

Autorizar: contenemos y neutralizamos el incidente y le informamos sobre las medidas tomadas.

Aspectos destacados

- Búsqueda de amenazas, detección y respuesta avanzadas ofrecidas como un servicio totalmente gestionado
- Equipo de respuesta para la contención y neutralización de amenazas 24/7
- Controle qué acciones realiza el equipo de MTR en su nombre y cómo se gestionan los incidentes
- Acceda a la prestigiosa tecnología del Machine Learning y a un equipo de expertos altamente cualificados
- Dos niveles de servicio (Standard y Advanced) que ofrecen un conjunto completo de funciones para organizaciones de todos los niveles de madurez

SOPHOS

Niveles de servicio de Sophos MDR

Sophos MDR ofrece dos niveles de servicio (Standard y Advanced) a fin de proporcionar un conjunto completo de funciones para empresas de todos los tamaños y niveles de madurez. Independientemente del nivel de servicio, las organizaciones pueden usar cualquiera de los tres modos de respuesta (notificar, colaborar o autorizar).

Sophos MDR: Standard

Búsqueda de amenazas a partir de pistas 24/7

Las actividades o artefactos maliciosos confirmados (indicios sólidos) se bloquean o detienen automáticamente. Con esto se libera a los analistas de amenazas para que puedan dedicarse a la búsqueda a partir de pistas, que implica la investigación y el análisis de eventos causales y adyacentes (indicios débiles) para descubrir nuevos indicadores de ataque (IOA) e indicadores de peligro (IOC).

Comprobación del estado de seguridad

Nuestros exámenes proactivos le mantienen al día de sus condiciones operativas y configuraciones. También proporcionamos recomendaciones que puede usar para que Sophos XDR y otros productos de Sophos Central mantengan su máximo rendimiento.

Informes de actividades

Resumimos las actividades de los casos por periodos para que sepa qué amenazas hemos detectado y qué acciones de respuesta hemos adoptado en cada periodo.

Detección de adversarios

Utilizamos técnicas de investigación avanzadas para distinguir los comportamientos legítimos de las tácticas, las técnicas y los procedimientos (TTP) de los ciberdelincuentes.

Sophos MDR: Advanced, todas las funciones de Standard más:

Búsqueda de amenazas sin pistas las 24 horas

Usamos la ciencia de datos y la información sobre amenazas para anticipar ciberataques e identificar indicadores de ataque.

Telemetría optimizada

Complementamos nuestras investigaciones de amenazas con telemetría de productos de Sophos Central que van más allá del endpoint para ofrecer una imagen completa de su posición de seguridad.

Mejora proactiva de la posición de seguridad

Ofrecemos orientación prescriptiva para ayudarle a optimizar su posición de seguridad.

Responsable de respuesta a amenazas dedicado

Le proporcionamos un responsable de respuesta a amenazas dedicado que colabora con su equipo interno o externo en cuanto identificamos una incidencia y que trabaja con usted hasta que el incidente se haya resuelto.

Soporte telefónico directo

Su equipo tiene acceso telefónico directo a nuestro centro de operaciones de seguridad (SOC). Nuestro equipo de operaciones de MDR está disponible 24/7 y cuenta con el apoyo de equipos de soporte en 26 lugares de todo el mundo.

Detección de recursos

Proporcionamos información detallada sobre sus recursos gestionados y no gestionados y cómo protegerlos.

Paquete Onboarding Plus para clientes MDR

Onboarding Plus es un servicio de incorporación guiada de forma remota para los clientes que han comprado Sophos MDR. Este servicio incluye un contacto dedicado en los servicios profesionales de Sophos para la incorporación y la programación, ayuda con el despliegue y la formación, y una comprobación del estado de seguridad para garantizar que está aprovechando al máximo nuestras prácticas recomendadas de seguridad. Onboarding Plus incluye:

Día 1: planificación del despliegue y ejecución

- Inicio del proyecto
- Configuración de Sophos Central
- Revisión de las funciones de Sophos Central
- Creación y prueba del proceso de despliegue
- Despliegue de Sophos Central en su organización

Día 30: formación de XDR

- Aprendizaje de cómo piensa y actúa un centro de operaciones de seguridad (SOC)
- Búsqueda de indicadores de peligro
- Creación de consultas para investigaciones futuras

Día 90: formación de XDR

- Revisión de su políticas de seguridad actuales y actualización según sea necesario
- Determinación de las funciones que puede usar para mejorar aún más su ciberprotección (si procede)
- Recepción de documentación por escrito con recomendaciones basadas en nuestra comprobación del estado de seguridad

Si tiene alguna pregunta, póngase en contacto con nuestro equipo de servicios profesionales.

Américas: ProfessionalServices@sophos.com

APJ: ProfessionalServicesAU@Sophos.com.au

Europa: ProfessionalServicesEmea@Sophos.com

Para obtener más información, visite

es.sophos.com/mdr

Ventas en España:
Tel.: (+34) 91 375 67 56
Email: comercialES@sophos.com

Ventas en América Latina:
Email: Latamsales@sophos.com

22-08-01 DS-EN (DD)

SOPHOS