SOPHOS

Managed Threat Response (MTR)

Respuesta a amenazas a cargo de expertos

Sophos Managed Threat Response (MTR) es un servicio totalmente administrado prestado por un equipo de expertos que ofrece funciones de búsqueda, detección y respuesta a amenazas las 24 horas.

Aspectos destacados

- Funciones avanzadas de búsqueda, detección y respuesta ofrecidas como un servicio totalmente gestionado
- Colabore con un equipo de respuesta las 24 horas que toma medidas para contener y neutralizar las amenazas de forma remota
- Decida y controle qué acciones realiza el equipo de MTR y cómo se gestionan los incidentes
- Combina la prestigiosa tecnología del Machine Learning con un equipo de expertos altamente cualificados
- Dos niveles de servicio (Standard y Advanced) ofrecen un conjunto completo de funciones para empresas de todos los niveles de madurez

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

Pocas empresas cuentan con las herramientas, las personas y los procesos adecuados para gestionar eficazmente su programa de seguridad las 24 horas, a la vez que se protegen de forma proactiva contra las amenazas nuevas y emergentes. Más allá de la simple notificación de ataques o comportamientos sospechosos, el equipo de Sophos MTR emprende acciones específicas en su nombre para neutralizar incluso las amenazas más sofisticadas y complejas.

Con Sophos MTR, su empresa contará con el soporte de un equipo de cazadores de amenazas y expertos en respuesta, disponible las 24 horas, que se dedicarán 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.
- Aplicar el contexto empresarial adecuado para las amenazas válidas.
- Iniciar acciones para interrumpir, contener y neutralizar amenazas de forma remota.
- Brindar asesoramiento práctico para abordar la causa raíz de los incidentes recurrentes.

Respuesta humana acelerada por máquinas

Sophos MTR, basado en nuestra tecnología de Intercept X Advanced with EDR, 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 EDR 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

Sophos MTR le permite tomar las decisiones y controlar cómo y cuándo se derivan los incidentes potenciales, qué acciones de respuesta (si las hubiera) desea que tomemos y quién debe incluirse en las comunicaciones. Sophos MTR le ofrece tres modos de respuesta para que pueda elegir la forma de trabajo óptima para el equipo de MTR a la hora de colaborar con usted durante un incidente:

Notificar: Le notificamos la detección y le proporcionamos datos para ayudarle con la priorización y la respuesta.

Colaborar: Trabajamos con su equipo interno o puntos de contacto externos para responder a la detección.

Autorizar: Gestionamos las acciones de contención y neutralización y le informamos de las medidas tomadas.

Niveles de servicio de Sophos MTR

Sophos MTR 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 seleccionado, las empresas pueden beneficiarse de cualquiera de los tres modos de respuesta (Notificar, Colaborar o Autorizar) para adaptarse a sus necesidades específicas.

Sophos MTR: Standard

Búsqueda de amenazas a partir de pistas las 24 horas

Las actividades o artefactos maliciosos confirmados (indicios sólidos) se bloquean o detienen automáticamente, lo que libera la carga de trabajo de los analistas de amenazas para que puedan realizar búsquedas a partir de pistas. Este tipo de búsqueda de amenazas implica la agregación e investigación de eventos causales y adyacentes (indicios débiles) para descubrir nuevos indicadores de ataque y de peligro que antes no podían detectarse.

Comprobación del estado de seguridad

Mantenga el máximo rendimiento de sus productos de Sophos Central, empezando por Intercept X Advanced with EDR, con exámenes proactivos de sus condiciones operativas y mejoras de configuración recomendadas.

Informes de actividades

Los resúmenes de las actividades de los casos facilitan la priorización y comunicación para que su equipo sepa qué amenazas se han detectado y qué acciones de respuesta se han llevado a cabo dentro de cada periodo del informe.

Detección de adversarios

La mayoría de los ataques eficaces dependen de la ejecución de un proceso que puede parecer legítimo para las herramientas de supervisión. Mediante técnicas de investigación patentadas, nuestro equipo determina la diferencia entre un comportamiento legítimo y las tácticas, técnicas y procedimientos utilizados por los atacantes.

Sophos MTR: Advanced *Incluye todas las funciones de Standard, más lo siguiente:*

Búsqueda de amenazas sin pistas las 24 horas

Aplicando la ciencia de datos, la información sobre amenazas y la intuición de experimentados cazadores de amenazas, combinamos el perfil de su empresa, sus activos de alto valor y usuarios de alto riesgo para anticiparnos al comportamiento de los atacantes e identificar nuevos indicadores de ataque.

Telemetría optimizada

Las investigaciones sobre amenazas se complementan con la telemetría de otros productos de Sophos Central que van más allá del endpoint para ofrecer una imagen completa de las actividades del adversario.

Mejora proactiva de la posición de seguridad

Mejore de forma proactiva su posición de seguridad y refuerce sus defensas con una guía prescriptiva para solucionar las debilidades de configuración y arquitectura que merman sus funciones de seguridad general.

Responsable de respuesta a incidentes dedicado

Cuando se confirma un incidente, se le asigna un responsable de respuesta a amenazas dedicado para que colabore directamente con sus recursos locales (equipo interno o partner externo) hasta que se neutralice la amenaza activa.

Soporte telefónico directo

Su equipo tiene acceso telefónico directo a nuestro centro de operaciones de seguridad (SOC). Nuestro equipo de operaciones de MTR está disponible las 24 horas y cuenta con el apoyo de equipos de soporte en 26 emplazamientos en todo el mundo.

Detección de recursos

Desde datos sobre recursos que incluyen versiones de sistemas operativos, aplicaciones y vulnerabilidades hasta la identificación de activos gestionados y no gestionados, ofrecemos información valiosa durante las evaluaciones de impacto, la búsqueda de amenazas y como parte de las recomendaciones para mejorar la postura proactiva.

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

17-09-2019 DSES (GH)

SOPHOS