Sophos Rapid Response

Respuesta inmediata a amenazas activas

El servicio Sophos Rapid Response, prestado por un equipo de expertos en respuesta a incidentes, ofrece asistencia ultrarrápida a la hora de identificar y neutralizar amenazas activas contra su empresa.

Cada segundo cuenta durante un ataque

Al responder a una amenaza activa, es imperativo que el tiempo entre el indicador de peligro inicial y la mitigación completa de la amenaza sea lo más corto posible. A medida que un adversario avanza por la cadena de ataque, nos embarcamos en una carrera contrarreloj para evitar que alcance sus objetivos.

Con Sophos Rapid Response, le sacamos de la zona de peligro rápidamente gracias a nuestro equipo remoto 24/7 de gestores de respuesta a incidentes, analistas de amenazas y cazadores de amenazas, quienes:

- Toman medidas rápidamente para clasificar, contener y neutralizar las amenazas activas
- Expulsan a los adversarios de su entorno para evitar más daños a sus recursos
- Realizan una supervisión y respuesta 24/7 para mejorar su protección
- Recomiendan acciones preventivas en tiempo real para abordar la causa raíz
- Despliegan rápidamente la pila tecnológica en la nube de Sophos en toda su infraestructura
- Analizan datos complementarios de tecnologías de terceros
- Proporcionan un resumen detallado de la amenaza posterior al incidente que describe nuestra investigación

Funciones de Rapid Response

Rapid Response incluye todas las ventajas de Sophos Managed Threat Response Advanced, además de una serie de beneficios adicionales.

	Sophos Rapid Response
MTR Advanced en modo de respuesta a amenazas "Autorizar"	✔
Supervisión, búsqueda y respuesta a amenazas 24/7	✔
Responsable de respuesta dedicado durante la amenaza activa y acceso telefónico directo	✔
Análisis de datos complementarios de tecnologías de terceros	✔
Presupuesto urgente y activación de cuenta el mismo día	✔
Resumen formal de la amenaza posterior al incidente con los detalles de la investigación	✔

Aspectos destacados

- Rápida identificación y neutralización de amenazas activas
- Respuesta a incidentes y supervisión 24/7 durante 45 días
- Punto de contacto y responsable de respuesta dedicados
- Resumen de la amenaza posterior al incidente con todas las acciones realizadas
- Precios predecibles con costes fijos y sin cargos ocultos
- Diseñado para poder optar al reembolso de aseguradoras
- Transición fluida a una suscripción con Sophos Managed Threat Response (MTR) después de Rapid Response

SOPHOS

Neutralización de amenazas activas

El equipo de Sophos Rapid Response se especializa en la neutralización de amenazas activas. Ya sea una infección, un ataque o un acceso no autorizado a sus recursos que intenta burlar sus controles de seguridad, lo hemos visto y detenido todo.

Nuestro equipo de expertos en respuesta a incidentes forma parte de Sophos Managed Threat Response (MTR), nuestro servicio de búsqueda, detección y respuesta a amenazas 24/7 que busca, identifica, investiga y responde de forma proactiva a las amenazas en nombre de nuestros clientes como parte de un servicio totalmente administrado.

Incentivos alineados

Los servicios de respuesta a incidentes (IR) tradicionales se cobran por hora, lo que puede llevarle a subestimar el tiempo que se necesitará para mitigar por completo una amenaza. Esto abre la posibilidad de tener que pagar por horas extra. O, lo que es peor, incentiva al servicio de IR tradicional a maximizar el número de horas que tarda su respuesta.

Sophos Rapid Response se basa en un modelo de precios con cargos fijos sin costes ocultos determinado por el número de usuarios y servidores de su infraestructura. Y, al prestarse de forma remota, podemos iniciar las acciones de respuesta el primer día. Nos interesa tanto como a usted sacarle de la zona de peligro tan rápidamente como podamos, puesto que el tiempo es un factor que nunca afecta al coste.

Despliegue rápido

Para garantizar una respuesta lo más rápida posible, el proceso de despliegue rápido de Sophos se centra especialmente en la distribución inmediata de los agentes de Sophos MTR en endpoints y servidores detectables.

Una vez desarrollada una estrategia de sustitución usando utilidades de desinstalación para reemplazar los productos existentes, un equipo remoto de ingenieros de despliegue contacta con cada cliente de Rapid Response para iniciar un plan de acción a medida, sirviéndose de herramientas de automatización para un despliegue masivo en la red.

El equipo colabora para optimizar el estado de seguridad del agente de Sophos MTR en toda la red, asegurando el empleo de configuraciones recomendadas para acelerar la investigación.

Metodología de Rapid Response

Una vez que se ha aprobado Rapid Response y que el cliente ha aceptado nuestro acuerdo de servicio, nos ponemos manos a la obra de inmediato. Rapid Response consta de cuatro fases principales: incorporación, clasificación, neutralización y supervisión.

Incorporación

- Organizar una llamada inicial para establecer las preferencias de comunicación y confirmar (si procede) qué pasos de remediación se han tomado ya
- Identificar la magnitud y el impacto del ataque
- Definir entre las dos partes un plan de respuesta
- Empezar a desplegar el software del servicio

Clasificación

- Evaluar el entorno operativo
- Identificar indicadores de peligro conocidos o la actividad de adversarios
- Recopilar datos e iniciar actividades de investigación
- Colaborar en un plan para iniciar actividades de respuesta

Neutralización

- Retirar el acceso a los atacantes
- Impedir más daños en datos y recursos
- Evitar que continúe la exfiltración de datos
- Recomendar acciones preventivas en tiempo real para abordar la causa raíz

Monitorización

- Transición al servicio MTR Advanced
- Realizar una supervisión continuada para detectar reincidencias
- Proporcionar un resumen de amenazas tras el incidente

Resumen de amenazas detallado

Una vez que hayamos neutralizado la amenaza activa para su empresa, le presentaremos un resumen formal de nuestra investigación con los detalles de las acciones y las detecciones realizadas, además de recomendaciones a largo plazo sobre cómo mitigar una repetición de amenazas similares en el futuro.

Monitorización y respuesta 24/7 tras el incidente

En el momento en que el incidente queda resuelto y la amenaza inmediata para su empresa está neutralizada, le transferimos a nuestro servicio MTR de primer nivel, MTR Advanced, para proporcionarle un servicio proactivo de búsqueda, investigación, detección y respuesta a amenazas las 24 horas.

Si la amenaza se repite o se produce una nueva, estaremos listos para responder sin ningún coste adicional para usted. Si recibe algún ataque en un período de 45 días, le defenderemos durante esos 45 días de su plazo de suscripción.

¿Está sufriendo un incidente activo?

Llame a nuestros números regionales de abajo en cualquier momento para hablar con uno de nuestros asesores de incidentes:

EE. UU. +1 4087461064

Australia +61 272084454

Canadá +1 7785897255

Francia +33 186539880

Alemania +49 61171186766

Reino Unido +44 1235635329

Si todos los asesores de incidentes están ocupados, deje un mensaje y alguien se pondrá en contacto con usted a la mayor brevedad posible.

¿Está sufriendo un incidente activo?

Para obtener más información, visite es.sophos.com/rapidresponse

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

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

22-05-12 DS-ES (DD)

SOPHOS