Folleto de la solución

Sophos Emergency Incident Response

Servicio de asistencia integral, desde la investigación hasta la recuperación

Respuesta inmediata a amenazas activas

Cuando su empresa sufre un ataque, cada segundo cuenta. Cuando se produce un incidente, lo que necesita es agilidad, eficacia y conocimientos y experiencia multidisciplinares en materia de seguridad. También precisa visibilidad y conocimiento del panorama global de amenazas, en constante evolución, y de las últimas tácticas y técnicas de los ciberdelincuentes.

Sophos Emergency Incident Response puede asistirle cuando se produce un ciberincidente, y trabajar rápidamente para evaluarlo, contenerlo, comprenderlo y remediarlo. Nuestro equipo de expertos multidisciplinar aplica sus años de experiencia y conocimientos para clasificar, contener y neutralizar rápidamente las amenazas activas, y expulsar a los adversarios para evitar más daños. Sophos aplica lo que ha aprendido a través de miles de intervenciones para recomendar mejoras y acciones preventivas que no solo abordan la causa del incidente, sino que ayudan a aumentar su resiliencia frente a futuros ataques.

Refuerzo proactivo de las defensas y la postura de seguridad

Sophos Emergency Incident Response emplea un enfoque colaborativo e interactivo, y trabaja con su equipo para evaluar rápidamente la situación, contener y eliminar la amenaza según sea necesario, y facilitar orientaciones prácticas para la recuperación. Con el fin de identificar y eliminar amenazas, nuestro equipo proporciona análisis forense digital, análisis de malware, búsqueda de amenazas e información sobre amenazas de los equipos de investigación Sophos X-Ops y Counter Threat Unit. Contamos con expertos interdisciplinares en la materia (como testers de penetración e investigadores de amenazas) para garantizar una mitigación de riesgos y una recuperación integrales.

Detección e investigación

Contacto e investigación iniciales

Para garantizar una respuesta lo más rápida posible, Sophos se centra en la distribución inmediata de agentes en los dispositivos detectables. Esta asistencia remota de respuesta a incidentes permite la obtención de datos forenses para respaldar el análisis inicial, desarrollar acciones de contención acordes y determinar si se necesita tecnología adicional para aumentar rápidamente la visibilidad durante la intervención.

Ventajas para el cliente

- Amplíe su equipo con capacidades multidisciplinares y conocimientos forenses digitales y de respuesta a incidentes.
- Reduzca el impacto de un incidente y el riesgo de que se repita al comprender a fondo la amenaza.
- Amplíe la visibilidad, recabe hechos y determine respuestas rápidamente para adoptar las medidas adecuadas.

Investigación a fondo

Recogida de datos: activos, servicios afectados, impacto en el negocio, otros vectores de ataque.

Análisis forense iterativo y de amenazas: investigadores, expertos en búsqueda, testers de penetración y analistas ayudan a comprender mejor la amenaza.

Planificación de la remediación: empiece a planificar la remediación en paralelo y de acuerdo con la investigación.

Reducción de la superficie de ataque: Sophos puede facilitar una visión interactiva de los ciberdelincuentes para validar los controles e identificar puntos de reentrada adicionales para garantizar una mitigación integral de los riesgos.

Negociación del rescate: los expertos en negociaciones de ransomware aprovechan lo mucho que conocen a los ejecutores de ransomware para allanar la negociación y asesorar a la organización para que recupere los datos de forma segura y lo menos costosa posible.

Remediación

Protección y validación

Endurecimiento específico de la seguridad: el equipo de IR guía y respalda los esfuerzos tácticos de endurecimiento de los controles de seguridad que impedirán que el ciberdelincuente vuelva a entrar.

Contención: interrumpa la comunicación con los canales de comando y control del atacante.

Expulsión del adversario: expulsar al atacante de una red contenida requiere la eliminación orquestada de sus artefactos y el restablecimiento de los dominios vulnerados.

Recuperación

Recuperación de sistemas y datos: para ayudar a reconstruir y restaurar los sistemas y limpiar los datos, el equipo de Sophos IR trabaja con Partners de confianza para ofrecer servicios de recuperación transparentes y seguros.

Validación de hosts: gracias a nuestra tecnología de agentes líder en el sector, ayudamos a garantizar que los hosts restaurados estén listos para la producción.

Seguimiento

Mejora

Las lecciones aprendidas a través de las miles de intervenciones llevadas a cabo sirven a Sophos para orientar las mejoras recomendadas en los procesos de respuesta, así como las recomendaciones estratégicas para ayudar a trazar una hoja de ruta de transformación de la seguridad. Al final de la intervención, podemos facilitarle un informe formal de la investigación del incidente 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.

Funciones del servicio

- Rápida identificación y neutralización de las amenazas activas.
- Despliegue rápido de tecnologías.
- Recopilación y análisis de datos forenses digitales para identificar indicadores de peligro y seguir la actividad de los adversarios.
- Búsqueda de amenazas para identificar la actividad delictiva relacionada.
- Capacidad técnica, de gestión de incidentes y de asesoramiento a distancia e in situ.
- Equipo global de respuesta a incidentes acreditado y experimentado en escenarios de ciberamenazas comunes y poco comunes.
- Información sobre amenazas específica de los incidentes y un conocimiento a fondo de las técnicas actuales de los adversarios.
- Negociación experta del rescate.
- Informe posterior al incidente en el que se detallan las medidas adoptadas, lo que se ha averiguado y las recomendaciones.

¿Por qué elegir a Sophos para la respuesta a incidentes?

Sophos aporta su amplia experiencia a cada intervención de emergencia de ciberseguridad. Ofrecemos un servicio integral de respuesta a incidentes a una gran variedad de organizaciones, independientemente del sector y del tipo de incidente: desde pequeños percances con un único sistema afectado hasta situaciones de crisis en toda la empresa que interrumpen o dificultan de forma significativa las operaciones comerciales.

Nuestro versado equipo de respuesta a incidentes se beneficia de la experiencia acumulada y de sus amplias trayectorias, que abarcan equipos de respuesta a incidentes de seguridad informática (CSIRT) nacionales, militares y organizativos, fuerzas del orden y agencias de inteligencia. Combinan conocimientos de las principales prácticas de ciberseguridad con la respuesta a incidentes de primera línea, la información sobre amenazas de nuestros equipos de investigación X-Ops y Counter Threat Unit, los análisis de seguridad y los resultados de las intervenciones de evaluación y pruebas de seguridad para agilizar las investigaciones y garantizar la recuperación con confianza.

¿Está sufriendo un incidente activo?

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

Australia: +61 272084454

Austria: +43 73265575520

Canadá: +1 7785897255

Francia: +33 186539880

Alemania: +49 61171186766

Italia: +39 02 94752 897

Suiza: +41 445152286

Reino Unido: +44 1235635329

EE. UU.: +1 4087461064

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

Correo electrónico: EmergencyIR@sophos.com

Para obtener más información, visite

es.sophos.com/emergency-response

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

2025-06-04 BRES (MP)

SOPHOS