Preguntas frecuentes técnicas y de ventas – Sophos Emergency Incident Response

Preguntas frecuentes del público general

Descripción general

¿Qué es Sophos Emergency Incident Response?

Sophos Emergency Incident Response es un servicio que le asiste cuando se produce un ciberincidente, trabajando rápidamente para evaluar, contener, comprender y ofrecer recomendaciones de remediación. 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.

Emergency Incident Response también le ayuda a determinar si su organización se ha visto afectada por un incidente y a comprender el alcance del mismo. El servicio ofrece diversas tareas de investigación para ayudar a identificar la causa raíz de los incidentes, realizar evaluaciones para determinar si el comportamiento observado es malicioso, llevar a cabo actividades de búsqueda de amenazas, recabar información sobre amenazas y ayudar en las negociaciones de rescates.

¿A quién va dirigido Sophos Emergency Incident Response?

El servicio está pensado para cualquier organización que esté sufriendo un incidente de seguridad activo, que haya sufrido un ataque reciente que requiera una investigación más profunda o que haya detectado una actividad sospechosa que deba investigarse para saber si supone una amenaza.

¿Tengo que ser cliente de Sophos para poder serlo de Emergency Incident Response?

No. Emergency Incident Response está disponible tanto para los actuales clientes de Sophos como para los que no lo son.

Estoy sufriendo un incidente activo. ¿Qué debo hacer?

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

Contáctenos por correo electrónico en EmergencyIR@sophos.com.

¿El servicio Emergency Incident Response se presta de forma remota o in situ?

Están disponibles ambas opciones.

¿Cómo es de rápido el servicio Emergency Incident Response?

La mayoría de los clientes se incorporan en 2 horas y se les clasifica en 48 horas. Puesto que el servicio puede prestarse de forma totalmente remota, la respuesta puede iniciarse en cuestión de horas después de contactar con Sophos.

Preguntas frecuentes técnicas y de ventas – Sophos Emergency Incident Response

¿Cuánto se tarda en comenzar la incorporación?

El equipo de Emergency Incident Response puede empezar con el proceso de incorporación y comenzar la investigación tan pronto como reciba su aprobación.

¿Cuál es la metodología de Emergency Incident Response?

Una vez aceptado el contrato de servicio, nos ponemos manos a la obra con una reunión inicial, que puede hacerse por correo electrónico si así lo prefiere. La investigación comenzará una vez que hayamos acordado los objetivos de la intervención.

Emergency Incident Response incluye diferentes categorías de trabajo que podemos ofrecer. Durante la conversación inicial para definir el alcance, trabajamos con usted para identificar las categorías necesarias y acordar un número estimado de horas.

Las categorías de trabajo del servicio incluyen: gestión de la intervención, respuesta a incidentes, análisis forense digital, evaluación del peligro, búsqueda de amenazas, información sobre amenazas e investigación, negociación del rescate, informe de la intervención, asistencia in situ (si procede), correo electrónico corporativo comprometido y despliegue de software.

¿En qué idiomas se ofrece Emergency Incident Response?

Actualmente el servicio se ofrece en inglés y japonés. Debe hablar inglés o japonés con soltura a nivel técnico.

¿Sustituye Sophos a los servicios de análisis forense digital y respuesta a incidentes (DFIR) o colabora con ellos?

Emergency Incident Response es un servicio DFIR. No es necesario contratar a una empresa de seguridad independiente para DFIR, ya que el alcance de los servicios prestados a través de Emergency Incident Response puede incluir el análisis forense digital.

¿Tengo que instalar la tecnología de Sophos en los endpoints?

No. Emergency Incident Response se puede prestar con Sophos XDR, o podemos desplegar Sophos XDR Sensor junto con su solución actual. Cualquiera de las dos opciones nos permite investigar rápidamente el incidente.

El equipo de Emergency Incident Response no necesita esperar a que finalice el despliegue para tomar medidas correctivas a fin de contener y neutralizar la amenaza. El equipo se servirá de cualquier dato que esté disponible y utilizará las herramientas que considere adecuadas para ayudar en la respuesta.

¿Cómo se calculan los precios?

Sophos estimará el número de horas necesarias para responder al incidente en función de unas preguntas para determinar el alcance. Solo pagará por las horas reales utilizadas.

¿Hay algún coste adicional?

Si se solicita trabajo in situ, se le facturarán los gastos de desplazamiento.

¿Podemos desplegar Emergency Incident Response en un segmento del entorno, o se tiene que actuar sobre la totalidad del entorno?

En determinadas situaciones, Emergency Incident Response se puede aplicar a un segmento de su entorno. Un especialista de Emergency Incident Response podrá proporcionarle más detalles durante la planificación del servicio.

¿Puede trabajar Sophos con un intermediario que represente a mi organización, como un gabinete jurídico, en el contrato?

- Sí. Es posible trabajar con un intermediario.

¿Puede determinar Sophos qué archivos se han exfiltrado/robado en el ataque?

Como parte del servicio Emergency Incident Response, haremos lo posible por determinar qué archivos (si los hay) se han exfiltrado durante un ataque. Sin embargo, no podemos ofrecer garantías, ya que esto puede depender de los datos que estén disponibles para la investigación.

¿Descifrará Sophos el ransomware en mi nombre?

No. Esto no forma parte del servicio Emergency Incident Response.

¿Me ayudará Sophos a negociar o pagar un rescate?

Emergency Incident Response incluye la negociación experta del rescate con los atacantes. Sophos no facilita el pago del rescate, pero si es necesario puede recomendar y trabajar con terceros a este respecto, promocionando Sophos MDR o Taegis MDR.