Sophos Compromise Assessment

Descubra la evidencia de una infracción antes de que afecte a su empresa

El año pasado, las empresas invirtieron una mediana de 37 días y una media de 2,4 millones USD en la detección y la recuperación de infracciones de seguridad. Prestado por un equipo de expertos en respuesta a incidentes, el servicio Sophos Compromise Assessment ofrece la forma más rápida y efectiva de identificar actividad de atacantes en curso o pasada en su entorno, lo que permite a su organización tomar medidas inmediatas y decididas.

Identifique actividad de atacantes activa o reciente

Prestado por un equipo de expertos en búsqueda de amenazas y respuesta a incidentes, el servicio Sophos Compromise Assessment identifica rápidamente si un atacante ha superado sus defensas, cuantifica el nivel de riesgo para su organización y ofrece orientación detallada sobre las medidas que se deben tomar para eliminar la amenaza.

La amplia experiencia en respuesta a las amenazas más avanzadas de hoy día permite al equipo de Sophos Incident Response (IR) Services identificar los indicadores de peligro (IoC) mediante investigaciones selectivas de recursos potencialmente en peligro. El resultado es una evaluación rápida y exhaustiva que ayuda a su organización a gestionar el riesgo y el cumplimiento al tiempo que mantiene la eficiencia operativa.

Metodología de Sophos Compromise Assessment

El equipo de Sophos IR Services mantiene una comunicación directa con su organización en cada fase de la evaluación del peligro, proporcionando información clara sobre la amenaza, la exposición al riesgo y las medidas que se deben tomar para resolver el incidente y abordar la causa raíz.

1. **Llamada de coordinación inicial**: la evaluación comienza con un intercambio eficiente de información sobre la posible amenaza, la identificación de las principales personas de contacto y la confirmación del alcance del despliegue y el proceso de investigación que se deberá seguir.
2. **Despliegue de las herramientas de investigación**: la instalación guiada de la galardonada plataforma de Sophos basada en la nube asegura que los datos en los dispositivos designados se capturan inmediatamente, lo que permite al equipo de Sophos IR Services realizar una evaluación exhaustiva del estado de seguridad del dispositivo.
3. **Investigación de amenazas y evaluación del riesgo**: en caso de confirmarse una amenaza activa, el equipo de Sophos IR Services hará inmediatamente una llamada de amenaza activa a sus principales personas de contacto para discutir el riesgo de que tenga lugar un incidente de seguridad generalizado y las medidas urgentes que deben tomarse.
4. **Llamada de resumen e informe por escrito**: entrega de documentación técnica y un resumen ejecutivo no técnico detallando la evidencia de la actividad del atacante, la exposición al riesgo y orientación para eliminar la amenaza y abordar la causa raíz.

Normalmente, las cuatro fases de Sophos Compromise Assessment se completan en un plazo de siete días desde llamada de coordinación inicial.

Aspectos destacados

- Identifique rápidamente si un atacante está operando en su entorno sin ser detectado
- Cuantifique el posible riesgo de un incidente de seguridad generalizado
- Comuníquese directamente con un equipo de expertos formado por cazadores de amenazas y especialistas en respuesta a incidentes en cada fase de la investigación
- Reciba un exhaustivo análisis de la actividad del atacante, el riesgo de exposición y orientación sobre cómo eliminar la amenaza y abordar la causa raíz
- Soporte para iniciativas de gestión de riesgos e iniciativas de cumplimiento, así como las medidas de debida diligencia para fusiones y adquisiciones

SOPHOS

Investigación rápida y exhaustiva

Sophos Compromise Assessment investiga e identifica una amplia variedad de actividades de atacantes incluyendo:

- Actividad de red sospechosa
- Propagación lateral
- Archivos anómalos o maliciosos
- Ejecución de malware automatizada
- Acceso no autorizado
- Aumento de privilegios
- Evasión de defensa
- Robo de credenciales
- Exfiltración de datos
- Scripts sin verificar

Tras la evaluación

Si el equipo de Sophos IR Services confirma que un atacante ha logrado superar sus defensas, poniendo en peligro sus datos y su empresa, existe la opción de incorporación prioritaria a Sophos Rapid Response. Este servicio de respuesta a incidentes a gran escala clasificará, contendrá y neutralizará la amenaza activa en todo su entorno de TI. Un equipo remoto de expertos en respuesta a incidentes disponible 24/7 actuará rápidamente para expulsar al adversario de su entorno y recomendar acciones preventivas en tiempo real para abordar la causa raíz.

Si no se detecta ninguna señal de una infracción, Sophos Managed Detection and Response (MDR) puede dotar a su organización con servicios de detección y respuesta 24/7 ininterrumpidos. Nuestro equipo de cazadores de amenazas y expertos en respuesta buscan y validan de forma proactiva posibles amenazas e incidentes las 24 horas. El equipo adopta continuamente medidas para interrumpir, contener y neutralizar amenazas en evolución y proporciona asesoramiento práctico para abordar la causa raíz de los incidentes y mejorar su higiene de seguridad.

¿Está sufriendo un incidente activo?

Sophos Rapid Response le saca 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. La incorporación empieza en cuestión de horas y la mayoría de clientes son clasificados en 48 horas. Si está en medio de una amenaza activa, llame a nuestros números regionales de abajo en cualquier momento para hablar con uno de nuestros asesores de incidentes.

Si está en medio de una amenaza activa, envíe un correo al equipo de Rapid Response a rapidresponse@sophos.com o llame a su número regional de abajo:

EE. UU.: +1 4087461064

Australia: +61 272084454

Canadá: +1 7785897255

Francia: +33 186539880

Alemania: +49 61171186766

Reino Unido: +44 1235635329

España: +34913758065

Suecia: +46 858400610

Italia: +39 02 947 52897

Austria: +43 73265575520

Suiza: +41 445152286

Países Bajos: +31 162708600

¿Está sufriendo un incidente activo?

Reciba soporte ultrarrápido
de Sophos Rapid Response

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

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

2023-06-27 DS-ES (PC)

SOPHOS