SOPHOS

Casos de uso de Sophos EDR y XDR

Disponibles con Intercept X Advanced with XDR, Intercept X Advanced with EDR, Intercept X Advanced for Server with XDR e Intercept X Advanced for Server with EDR

Responda a preguntas críticas sobre la búsqueda de amenazas y las operaciones de TI y tome medidas cuando sea necesario. Tanto los administradores de TI como los analistas de ciberseguridad pueden servirse de su potente funcionalidad.

Realice operaciones de seguridad TI y tareas de búsqueda de amenazas.

- Use consultas SQL ya escritas totalmente personalizables.
- Tome las medidas oportunas rápidamente cuando tenga la información que necesita.
- Cubre endpoints, servidores, firewalls, correo electrónico, hosts en la nube y más

Sophos XDR

Casos de uso de operaciones de TI

Los casos de uso de operaciones de TI mantienen la higiene de sus operaciones de TI en excelente estado. Estos son algunos casos de uso de ejemplo:

Comprobación del estado de seguridad de los dispositivos

Identifique los dispositivos con problemas de rendimiento, acceda a ellos de forma remota y tome las medidas necesarias.

- Detecte dispositivos con falta de espacio en disco, un uso de memoria/CPU excesivo o un reinicio pendiente.
- Acceda remotamente a los dispositivos para liberar espacio en disco, investigar las causas del uso excesivo y reiniciar cuando sea necesario.

Vulnerabilidades

Detecte los dispositivos con problemas o vulnerabilidades que el malware o los atacantes pueden explotar.

- Localice dispositivos con vulnerabilidades de software, encuentre servicios en ejecución desconocidos o extensiones de navegadores no autorizadas y detecte credenciales de cuentas compartidas o robadas.
- Acceda a dispositivos de forma remota para instalar parches, investigar y detener servicios desconocidos, desinstale extensiones de navegadores y actualice credenciales de cuentas en la nube.

Software no deseado

Localice software que pueda causar problemas de cumplimiento o productividad.

- Encuentre programas no deseados como Spotify, Steam y BitTorrent.
- Acceda remotamente a los dispositivos y desinstale software.

Errores de configuración

Detecte dispositivos y cargas de trabajo en la nube con problemas de configuración que puedan suponer riesgos de seguridad.

- Identifique servidores con RDP y SSH habilitados y grupos de seguridad en la nube con puertos de red que se han dejado abiertos, y supervise e inventarie hosts en la nube pública, contenedores y más.
- Acceda de forma remota a los servidores, deshabilite RDP/SSH y busque servidores escuchando en puertos abiertos.

Cumplimiento

Identifique y resuelva problemas de cumplimiento de ámbito local y en la nube.

- Busque archivos confidenciales y evalúe configuraciones para entornos de AWS, Azure y GCP.
- Acceda de forma remota a dispositivos para eliminar archivos confidenciales y mantener configuraciones en la nube seguras de acuerdo con los indicadores de referencia del CIS.

Despliegue de proyectos

Compruebe si los proyectos de TI se han desplegado en todos dispositivos.

- Vea si se ha implementado el software en los dispositivos para evaluar el progreso durante el despliegue.
- Acceda a los dispositivos de forma remota para garantizar el despliegue correcto y reiniciar si es necesario para hacer los cambios pertinentes.

Problemas de red en la oficina (requiere XDR)

Vea y rectifique problemas de red en todas sus oficinas.

- Entienda por qué una oficina tiene problemas de red que ralentizan el rendimiento.
- Identifique qué aplicación provoca el problema.

Gestión de dispositivos (requiere XDR)

Identifique y entienda los dispositivos del entorno de TI de su empresa.

- Vea los dispositivos no administrados y no protegidos como portátiles, móviles y dispositivos IoT.
- Obtenga una visibilidad adicional de los dispositivos heredados o no administrables como equipos médicos especializados.

Espere lo inesperado (requiere XDR)

Con 30 días de almacenamiento en la nube, no sufrirá las consecuencias de los eventos inesperados.

- Revise los últimos 30 días para identificar actividad inusual en un dispositivo extraviado.
- Averigüe qué ha ocurrido con un dispositivo incluso si se han borrado sus datos o se ha destruido.

Casos de uso de búsqueda de amenazas

Localice amenazas sutiles y esquivas y límpielas rápidamente. Estos son solo algunos casos de uso de ejemplo:

Ataques de red

Identifique los procesos que intentan acceder a la red de forma inusual.

- Detecte procesos que intenten conectarse a puertos no estándar o tráfico saliente inusual procedente de una carga de trabajo en la nube.
- Analice grupos de seguridad en la nube para identificar recursos expuestos a la Internet pública.
- Acceda de forma remota al dispositivo o la carga de trabajo, finalice el proceso y compruebe si hay propagación lateral.

Archivos modificados

Identifique elementos que se hayan modificado de manera inesperada.

- Identifique procesos que hayan modificado archivos o claves de registro recientemente.
- Acceda al dispositivo de forma remota, examine los cambios y tome medidas.

Scripts ofuscados

Los ataques sin archivos y basados en memoria son un vector de ataque común.

- Profundice en los detalles de las ejecuciones inesperadas de PowerShell.
- Acceda remotamente al dispositivo, ejecute herramientas forenses adicionales y detenga los procesos sospechosos.

Procesos camuflados

Algunos procesos maliciosos se camuflan para evitar ser detectados.

- Detecte procesos que se hayan camuflado.
- Acceda remotamente al dispositivo, detenga procesos sospechosos y ejecute herramientas forenses.

Plataforma MITRE ATT&CK

La plataforma MITRE ATT&CK es una plantilla que suele utilizarse para identificar las técnicas de ataque.

- Utilice consultas propias o de Sophos para identificar tácticas y técnicas de ataque utilizadas por los adversarios.
- En función de la técnica identificada, centre su investigación en posibles segundos ataques o en áreas que deben volver a comprobarse.

Alcance de los incidentes

Comprenda el impacto de un incidente y qué dispositivos y usuarios se han visto afectados.

- Identifique los dispositivos que han seguido un enlace desde un correo electrónico de phishing.
- Vea qué dispositivos han descargado archivos del sitio web de phishing, acceda a ellos de forma remota y realice la limpieza.

Amplíe los periodos de investigación (requiere XDR)

Utilice 30 días de datos en la nube además de 90 días de almacenamiento de datos en el dispositivo.

- Investigue 30 días de datos sin necesidad de volver a conectar el dispositivo.
- Vea qué ha ocurrido con los dispositivos incapacitados en un ataque.

Utilice datos de red detallados (requiere XDR)

Incorpore datos de red en su búsqueda e investigación de amenazas.

- Correlacione tráfico malicioso bloqueado con otros indicadores de peligro para entender un ataque más amplio.
- Utilice detecciones ATP e IPS desde el firewall para investigar hosts y dispositivos sospechosos.

Utilice datos de correo electrónico detallados (requiere XDR)

Integre la información del correo electrónico para obtener una mayor visibilidad de su entorno.

- Compare la información de encabezado del correo electrónico con otros indicadores de peligro para entender mejor un incidente.
- Identifique archivos sospechosos y elimínelos rápidamente desde dispositivos y buzones de correo de O365.

Para obtener más información sobre Sophos XDR, EDR y las potentes funciones de protección de Intercept X, visite **es.sophos.com**.

26-03-21 UC-ES (MP)

SOPHOS