Sophos Network Detection and Response (NDR)

Monitorización y análisis continuos del tráfico de red para identificar recursos no autorizados, dispositivos desprotegidos, amenazas internas y ataques de día cero.

Por qué NDR

- NDR detecta la actividad maliciosa en lo más profundo de la red que los endpoints y firewalls no pueden ver.
- NDR analiza el tráfico en lo más profundo de la red y es un componente fundamental en cualquier estrategia de defensa exhaustiva.
- Detecta la actividad procedente de dispositivos desconocidos o no gestionados, recursos no autorizados, nuevos servidores C2 de día cero o movimientos de datos inusuales.

Resumen de Sophos NDR

- Sophos NDR es un complemento para Sophos MDR y Sophos XDR.
- Funciona a la perfección con Sophos Firewall para ofrecer lo último en detección y respuesta.
- Las alertas se pasan instantáneamente a los analistas de Sophos MDR y XDR para que las investiguen y respondan mediante la función de respuesta a amenazas activas de Sophos Firewall.
- Se despliega como un dispositivo virtual que se conecta a un switch físico o virtual en la red corporativa.

Precios por usuarios + servidores

10 000 usuarios

\+ 1000 servidores

= 11 000 usuarios y servidores de NDR

Precios inferiores a los de las soluciones NDR independientes

El software del dispositivo virtual está incluido en la suscripción

Descuentos por volumen integrados

Por qué elegir Sophos NDR

- Integración completa con Sophos MDR, XDR y Firewall para ofrecer lo último en detección y respuesta
- Cinco motores de detección diferentes para ofrecer la máxima visibilidad de las amenazas de red
- Un enfoque al Machine Learning único y patentado que identifica el malware en el tráfico cifrado
- Detección de algoritmos de generación de dominios (DGA) que no requiere información sobre amenazas adicional
- Potente análisis de riesgos para detectar actividad anómala e identificar patrones que justifican una investigación más a fondo

Sophos NDR: Ofrezca resultados superiores en ciberseguridad

Sophos NDR mejora la protección al detectar amenazas y actividad maliciosa que otros productos pasan por alto:

- Dispositivos no autorizados: dispositivos no autorizados y potencialmente maliciosos que se comunican a través de la red.
- Dispositivos desprotegidos: dispositivos legítimos que se pueden utilizar como punto de entrada.
- Amenazas internas: descubra tráfico y movimientos de datos anómalos procedentes de usuarios internos.
- Ataques de día cero: detecte intentos de comando y control (C2) por parte de servidores en función de patrones observados en paquetes de sesiones.
- Amenazas de IoT y TO (p. ej., dispositivos médicos y terminales de puntos de venta): supervise los datos de estos dispositivos.

Al combinarse con otra telemetría de seguridad, Sophos NDR permite a los analistas obtener una visión completa del ataque, lo que a su vez permite una respuesta más rápida y exhaustiva.

Por ejemplo:

1. Sophos NDR detecta un dispositivo que se está comunicando en la red interna.
2. La protección para endpoints no está administrando ningún dispositivo conocido.

CONCLUSIÓN: Hay un dispositivo no administrado comunicándose en la red.

ACCIÓN DE MDR: investigar si se trata de una infracción de las políticas por parte de un usuario interno o de un adversario malicioso.

Preguntas de aproximación

- ¿Tiene actualmente alguna solución de monitorización del tráfico de la red (p. ej., Darktrace, Security Onion, Thinkst Canary)?
- ¿Tiene actualmente algún portátil u otros dispositivos sin protección para endpoints (p. ej., en un laboratorio, terminales POS o dispositivos IoT)?
- ¿Supervisa el tráfico de red tras su firewall?
- ¿Cómo supervisa el comportamiento de los usuarios internos?
- ¿Cómo supervisa el movimiento de datos «normal»?
- ¿Realiza detecciones de recursos periódicas en toda su red?
- ¿Puede identificar sistemas nuevos o no autorizados en su red?
- ¿Tiene visibilidad del tráfico cifrado en toda su red? ¿Tiene actualmente la capacidad de determinar si este tráfico es malicioso?

23-11-06-DA-(MP)

SOPHOS