Informe de la solución

Sophos NDR

Visibilidad crítica en lo más profundo de la red

Sophos Network Detection and Response, disponible para Sophos MDR y Sophos XDR, detecta la actividad maliciosa en lo más profundo de la red que los endpoints y firewalls no pueden ver. Sophos NDR analiza continuamente el tráfico en busca de patrones sospechosos, como actividad inusual que se origina en dispositivos desconocidos o no administrados, recursos no autorizados, nuevos servidores C2 de día cero o movimientos de datos inesperados.

Casos de uso

1 | VISIBILIDAD CRÍTICA

Resultado deseado: obtenga una visibilidad crítica de la actividad de red que otros productos no pueden ver.

Solución: Sophos NDR funciona junto con sus endpoints y firewalls gestionados para supervisar la actividad de red en busca de patrones sospechosos y maliciosos que esos endpoints y firewalls no pueden ver. Detecta flujos de tráfico anormales de sistemas no gestionados, dispositivos IoT, recursos no autorizados, amenazas internas, ataques de día cero desconocidos y patrones inusuales en lo más profundo de la red.

2 | DETECCIÓN TEMPRANA

Resultado deseado: cinco motores de detección independientes funcionan en tiempo real para identificar amenazas con mayor prontitud.

Solución: Sophos NDR incluye cinco motores de detección independientes que funcionan juntos en tiempo real para detectar rápidamente tráfico sospechoso o malicioso, con tecnologías como el Deep Learning, la inspección detallada de paquetes, el análisis de cargas cifradas, el análisis de nombres de dominio y potentes analíticas. Nuestro análisis exclusivo proporciona solamente alertas de alto valor para que no tenga que lidiar con excesivo ruido.

3 | RESPUESTA AUTOMÁTICA

Resultado deseado: detenga automáticamente los adversarios activos y las amenazas al instante.

Solución: la automatización entre productos de Sophos como Sophos NDR, Sophos XDR, Sophos MDR y Sophos Firewall proporciona una respuesta inmediata para frenar en seco las amenazas activas. Cuando Sophos NDR identifica un indicador de peligro, una amenaza activa o un adversario, los analistas reciben una alerta inmediata y pueden enviar al instante un feed de amenazas a Sophos Firewall para iniciar una respuesta automatizada que aísle el host comprometido.

4 | GESTIÓN MEDIANTE UNA ÚNICA CONSOLA

Resultado deseado: dedique menos tiempo a gestionar su seguridad de redes.

Solución: con Sophos Central, dispondrá de una única plataforma de administración en la nube para todos sus productos de Sophos, incluidos NDR, XDR, endpoints, firewalls y mucho más. Contará con herramientas potentes y completas que se sirven de nuestro exhaustivo Data Lake para buscar amenazas entre productos, gestionar una respuesta temprana, generar informes y realizar auditorías. Esto en última instancia significa que dedicará menos tiempo a gestionar la seguridad de sus redes.

Identifique recursos desprotegidos y no autorizados

Descubra movimientos de datos inusuales y amenazas internas

Detecte ataques de día cero desconocidos

Obtenga más información y pruebe Sophos NDR
es.sophos.com/ndr

2023-11-06 DS-ES (MP)