Sophos lanza la única solución XDR que integra la seguridad de *endpoints,* servidores, *firewalls* y correo electrónico

CIUDAD DE MÉXICO. 5 de mayo de 2021.- Sophos, líder mundial en ciberseguridad de última generación, anunció hoy el lanzamiento de la única solución de **detección y respuesta extendida (XDR, por sus siglas en inglés *Extended Detection and Response*)** que recopila, y correlaciona los datos de seguridad de *endpoints*, *firewalls,* servidores y correo electrónico para un análisis profundo que deriva en una mejor identificación, investigación y combate de amenazas.

"*Estamos viendo un nivel extraordinariamente alto de* ransomware *complejo y otros delitos cibernéticos, así como una urgencia por la necesidad de una ciberseguridad tanto integral como eficaz*", dijo Dan Schiappa, director de productos de Sophos. "*Sophos XDR es una nueva solución proactiva contra los ataques más sofisticados que aprovechan múltiples puntos de acceso para ingresar, moverse lateralmente para evadir la detección y hacer daño*".

Ataques con 'esteroides'

Sophos también publicó el estudio que detalla un ataque que comenzó cuando los ciberdelincuentes comprometieron un servidor Exchange utilizando el reciente *exploit* ProxyLogon.

La investigación muestra cómo los atacantes se movieron lateralmente a través de la red utilizando diferentes métodos de acceso; durante dos semanas robaron las credenciales de las cuentas, sembraron un punto de apoyo en varias máquinas, implementaron una herramienta comercial de acceso remoto para ingresar a la red y posteriormente propagaron varios programas maliciosos.

Lo anterior hizo que el equipo de ciberseguridad de la compañía no pudiera seguir el ritmo del ataque, que los acechaba desde distintos flancos, un problema común para el 54% de los gerentes de TI, quienes admiten que los ciberataques son demasiado avanzados para que sus equipos los manejen por sí mismos, de acuerdo con Sophos. Es por eso que contar con una solución de XDR que realice la defensa nativa de distintos puntos de forma integral, y no paralelamente como se realiza tradicionalmente, es fundamental.

Análisis profundo de amenazas con un conjunto de datos enriquecido

Sophos XDR amplía la visibilidad a los equipos de defensa con un conjunto de datos más rico basado en el portafolio de soluciones de la empresa. Su enfoque único combina el análisis de datos externos al dispositivo y del lago de data proporcionando la información contextualizada más amplia y profunda que los analistas de seguridad pueden aprovechar a través de Sophos Central y a través de interfaces de programación de aplicaciones (API) abiertas para la

transferencia a la información de seguridad, además de la gestión de eventos; orquestación, automatización y respuesta de seguridad (SOAR); automatización de servicios profesionales (PSA); y sistemas de gestión vía control remoto (RMM).

El lago de datos incluye la información crítica obtenida por Intercept X, Intercept X for Server, Sophos Firewall y Sophos Email. Sophos Cloud Optix y Sophos Mobile se incorporarán a finales de este año.

"Sophos XDR proporciona una visibilidad total de datos de nuestros endpoints*, lo que nos permite detectar fácilmente los incidentes que padecen y determinar su alcance con la data nueva e histórica que esta herramienta pone a nuestro alcance*", dijo Alistair Knowles, analista de seguridad cibernética de Ted Baker.

Sophos lanzó también una nueva versión de Sophos EDR, enfocada en *endpoints*, que ahora ofrece visibilidad de siete días de datos alojados en la nube (actualizables a 30) y 90 días de datos en el dispositivo.

La ciberseguridad evolucionó: ecosistema adaptable y abierto

Las soluciones XDR y EDR forman Sophos ACE, un ecosistema abierto de ciberseguridad adaptativa (*Adaptative Cybersecurity Ecosystem*) que es una nueva arquitectura de seguridad que optimiza la prevención, detección y respuesta a amenazas.

Sophos ACE aprovecha la automatización y el análisis de datos, así como la aportación colectiva de los productos, socios, clientes y otros vendedores de la industria para crear una protección que mejora continuamente, un círculo virtuoso que está en constante aprendizaje y avance.

Este ecosistema se basa en información procesable de sus soluciones, así como la inteligencia de amenazas de SophosLabs, Sophos AI y el equipo de Sophos Managed Threat Response. Las API abiertas permiten a los clientes, socios y desarrolladores crear herramientas y soluciones que interactúan con el sistema y aprovechar las integraciones existentes. Sophos lidera la industria con este enfoque y ya está integrado a muchos proveedores.

"Los atacantes se están volviendo más sofisticados y la única forma de mantenerse al día es con la automatización impulsada por la inteligencia artificial para analizar y reaccionar más rápido, en conjunto con analistas humanos para correlacionar múltiples sospechas e interpretar su verdadero significado", explica Schiappa. "*Sophos ACE es una evolución de nuestro enfoque de seguridad y llega en un momento crucial, dada la situación mundial que el año pasado forzó a las empresas a migrar al trabajo remoto y la adopción de la nube"*.

Sophos XDR y la actualización de EDR estarán disponibles a nivel global desde el 19 de mayo a través de los socios de Sophos. Los socios y clientes pueden administrar fácilmente todas las soluciones de productos en la plataforma Sophos Central basada en la nube a través de una única interfaz de usuario.

###

Sobre Sophos

Como líder mundial en seguridad cibernética de última generación, Sophos protege a más de 400,000 organizaciones en más de 150 países de las amenazas cibernéticas más avanzadas de la actualidad. Desarrolladas por SophosLabs, un equipo global de inteligencia contra amenazas cibernética y ciencia de datos, las soluciones basadas en inteligencia artificial y nativas de la nube de Sophos ofrecen seguridad a endpoints (computadoras portátiles, servidores y dispositivos móviles) y redes contra las diversas técnicas de ciberdelincuencia que están en constante evolución, incluidos ransomware, malware, exploits, extracción de datos, incumplimientos de adversarios activos, phishing y más. Sophos Central, una plataforma de administración nativa de la nube, integra toda la cartera de productos de próxima generación de Sophos, incluida la solución de endpoint Intercept X y el Firewall XG, en un único sistema de "seguridad sincronizada" accesible a través de un conjunto de APIs.

Sophos ha impulsado la transición a la ciberseguridad de última generación, aprovechando las capacidades avanzadas en la nube, el aprendizaje automático, las API, la automatización, la respuesta ante amenazas y más, para brindar protección de nivel empresarial a organizaciones de cualquier tamaño. Sophos vende sus productos y servicios exclusivamente a través de un canal global de más de 53,000 socios y proveedores de servicios administrados (MSP). Sophos también pone a disposición de los consumidores sus innovadoras tecnologías comerciales a través de Sophos Home. La compañía tiene su sede en Oxford, Reino Unido. Para obtener más información visita www.sophos.com.

Síguenos en:

Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/