Sophos actualiza su EDR para que las empresas se anticipen a los ciberataques

CIUDAD DE MÉXICO 11 de junio de 2020.- Sophos, empresa líder en ciberseguridad de última generación, presentó una nueva versión de su Endpoint Detection and Response (EDR), que hará más rápida y fácil para los analistas de ciberseguridad la tarea de identificar y neutralizar las amenazas para las organizaciones, lo que permite anticiparse a los ciberataques de forma rápida y segura.

La firma también publicó una nueva investigación llamada 'Una mirada al interior del creciente y complejo Botnet Kingminer', que resalta la importancia de la inteligencia artificial para detectar amenazas de ciberseguridad. Dicho botnet opera mediante intentos de acceso al servidor con credenciales de inicio de sesión masivos y Sophos detectó que utiliza el exploit EternalBlue, usado en el ransomware de alcance mundial 'WannaCry' registrado en mayo de 2017.

Sophos explica que Kingminer utiliza muchos de los atributos y tácticas de otros atacantes avanzados para obtener acceso al servidor, evidencia de la necesidad de un EDR que sea capaz de detectar y anticiparse de forma rápida a ataques masivos, acción que sin esta solución tardaría meses. Recientemente, la firma publicó en su informe 'Estado del Ransomware 2020' que solo el 24% de las organizaciones víctimas de ransomware pudieron detectar un ataque antes de que pudiera cifrar sus datos internos.

"*Los ciberdelincuentes están sumando cada vez más formas de propagar y capitalizar sus ataques, además de expandirlos a medida que las organizaciones se mueven hacia la nube y habilitan fuerzas de trabajo remotas. Los servidores están insuficientemente protegidos, tienen vulnerabilidades y las empresas no cuentan con las soluciones necesarias para detener a los criminales"*, consideró Dan Schiappa, director de producto de Sophos. "*Nuestro EDR actualizado ayuda a identificar esos ataques, previniendo a los servidores y equipos de TI de las empresas y dando visibilidad total en donde anteriormente no había demasiada atención. Las capacidades de consulta de Sophos EDR permiten a las organizaciones buscar indicadores en la data del pasado y determinar el estado actual del sistema, un nivel de inteligencia fundamental para comprender los cambios en el comportamiento de los atacantes y reducir el tiempo en el que los virus permanecen en el sistema*".

Sophos EDR ofrece una amplia visibilidad del sistema de la organización, lo que permite a los profesionales de ciberseguridad responder rápidamente a los indicios de amenaza, mejorar su búsqueda de indicadores de ciberataques y responder anticipada y rápidamente. Las nuevas características de Sophos EDR son:

Live Discover: Identifica la actividad pasada y presente con hasta 90 días de retención de datos. Las consultas SQL listas para usar permiten a los administradores responder a la búsqueda de amenazas y preguntas de TI, y pueden ser seleccionadas de una biblioteca de opciones pre escritas y totalmente personalizadas por los usuarios. Este motor de consulta flexible proporciona acceso a algunas de las grabaciones de actividad del endpoint más detalladas que se mejoran aún más con Sophos, gracias a su tecnología de *deep learning*.

Live Response: Con esta solución, el Sophos EDR permite al cliente responder de manera remota y acceder al endpoint y servidores utilizando su interfaz de línea de comandos. También permite reiniciar dispositivos, instalar y desinstalar software, finalizar procesos, ejecutar scripts, editar archivos de configuración, entre otras, todo de forma remota.

"Sophos EDR es un multiplicador de la fuerza que brindan las herramientas de seguridad de una compañía para hacer el trabajo de todo un equipo de ciberseguridad sin necesidad de agregar personal adicional", indicó Ryan Miller, director de TI de Mission Search. "*Esta nueva versión reduce drásticamente el tiempo que lleva detectar y responder a incidentes, lo que nos ahorra un promedio de cuatro a cinco horas por día. Las consultas son fáciles y se simplificó el proceso de investigar los incidentes y sospechas, que anteriormente era complejo y largo"*, añadió.

Sophos EDR funciona con la red neuronal de aprendizaje profundo de Sophos, que está capacitada en cientos de millones de muestras y ejemplos de indicadores de amenazas. Esa inteligencia artificial aplicada a la ciberseguridad rastrea, analiza y reconstruye más de 400,000 muestras de malware todos los días. La herramienta está disponible en Sophos Intercept X Advanced y es compatible con Windows, MacOS y Linux. Sus nuevas características se gestionan en la plataforma Sophos Central basada en la nube para compartir información en tiempo real con el resto de los productos de Sophos, de manera sincronizada.

####

Sobre Sophos

Como líder mundial en seguridad cibernética de última generación, Sophos protege de las amenazas cibernéticas más avanzadas de la actualidad a más de 400,000 organizaciones de todos los tamaños en más de 150 países. Desarrolladas por SophosLabs -un equipo global de inteligencia de amenazas y ciencia de datos-, las soluciones basadas en la nube y en IA de Sophos aseguran endpoints (computadoras portátiles, servidores y dispositivos móviles) y redes contra las técnicas de ciberataque que están evolución, incluyendo ransomware, malware, exploits, extracción de datos, violaciones de adversarios activos, phishing, entre otras. Sophos Central, plataforma de administración nativa de la nube, integra la cartera completa de productos de última generación de Sophos, incluida la solución de endpoint Intercept X y el firewall de próxima generación XG, en un único sistema de "seguridad sincronizada" accesible a través de un conjunto de APIs.

Sophos ha impulsado la transición hacia la ciberseguridad de próxima generación, aprovechando las capacidades avanzadas en la nube, el aprendizaje automático, las API, la automatización, la respuesta ante amenazas administradas 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 47,000 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, y cotiza en la Bolsa de Londres con el símbolo "SOPH". Más información disponible en www.sophos.com

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