Sophos X-Ops: la nueva fusión de especialistas en cibercrimen

- *Sophos X-Ops une los expertos de tres equipos de especialistas de la compañía líder en ciberseguridad de última generación para ayudar a las organizaciones a defenderse contra los ciberataques.*

CIUDAD DE MÉXICO. 20 de julio de 2022.- Sophos, líder mundial en ciberseguridad de última generación, anunció el lanzamiento de Sophos X-Ops, una nueva unidad interoperativa que unifica al resto de los equipos establecidos de expertos en ciberseguridad de la compañía (SophosLabs, Sophos SecOps y Sophos IA) De ese modo, dichos equipos de especialistas se complementarán en una sola unidad para ayudar a las organizaciones a defenderse mejor de los ciberataques, que cada vez son más complejos.

Sophos X-Ops aprovecha la inteligencia de amenazas predictiva, mediante información en tiempo real de cada uno de los equipos antes mencionados, y a su vez hace que estas tres células trabajen en conjunto para ofrecer capacidades de protección, detección y respuesta más sólidas e innovadoras.

Sophos también publicó "OODA: Sophos X-Ops Takes on Burgeoning SQL Server Attacks", una investigación sobre el aumento de los ataques contra servidores Microsoft SQL sin parches y cómo los atacantes usaron un sitio de descarga falso y herramientas de acceso remoto del mercado gris, para distribuir múltiples familias de ransomware.

Sophos X-Ops identificó los ataques al combinar su conocimiento sobre los incidentes, y realizar un análisis conjunto para tomar medidas de contención, neutralizando rápidamente a los adversarios.

"La ciberseguridad moderna se está convirtiendo en un deporte de equipo altamente interactivo y, a medida que la industria ha madurado, han surgido las especializaciones necesarias en análisis, ingeniería e investigación. Las operaciones integrales escalables ahora deben incluir desarrolladores de software, ingenieros de automatización, analistas de malware, ingenieros inversos, ingenieros de infraestructura en la nube, respondedores de incidentes, ingenieros y científicos de datos, y muchos otros expertos", dijo Joe Levy, director de tecnología y productos de Sophos.

"Hemos unificado tres equipos maduros y reconocidos a nivel mundial dentro de Sophos para proporcionar esta amplitud de experiencia crítica en materia y procesos. Unidos como Sophos X-Ops, pueden aprovechar las fortalezas de cada uno, incluido el análisis de la telemetría mundial de más de 500,000 clientes, las capacidades de detección, respuesta y remediación de amenazas líderes en la industria, y la inteligencia artificial rigurosa para mejorar de manera

medible la detección y respuesta a amenazas. Los atacantes a menudo están demasiado organizados y son demasiado avanzados para combatir sin la experiencia combinada única y la eficiencia operativa de un grupo de trabajo conjunto como Sophos X-Ops", añadió.

En marzo de 2022, el director del FBI, Christopher Wray, dijo que *"lo que la asociación nos permite hacer es golpear a nuestros adversarios en todos los puntos, desde las redes de las víctimas hacia atrás. el camino a las propias computadoras de los piratas informáticos, porque cuando se trata de la estrategia cibernética del FBI, sabemos que tratar de pararse en la portería y bloquear tiros no va a hacer el trabajo.*

"Estamos interrumpiendo tres cosas: los actores de amenazas, su infraestructura y su dinero. Y tenemos el impacto más duradero cuando trabajamos con todos nuestros socios para interrumpir los tres juntos".

Sophos X-Ops está adoptando un enfoque similar: recopila y opera con inteligencia de amenazas de sus propios grupos multidisciplinarios para ayudar a detener a los atacantes, prevenir o minimizar los daños del ransomware, el espionaje u otros delitos cibernéticos que pueden afectar a organizaciones de todos los tipos y tamaños, así como trabajar con las fuerzas del orden para neutralizar la infraestructura del atacante.

Si bien los equipos internos de Sophos ya comparten información de forma habitual, la creación formal de Sophos X-Ops impulsa un proceso más rápido y simplificado, necesario para contrarrestar a los adversarios que se mueven con la misma rapidez.

"La ciberseguridad efectiva requiere una colaboración sólida en todos los niveles, tanto interna como externamente; es la única manera de descubrir, analizar y contrarrestar ciberactores maliciosos a gran velocidad y escala. La combinación de estos equipos separados en Sophos X-Ops demuestra que Sophos comprende este principio y está actuando en consecuencia", dijo Michael Daniel, presidente y director ejecutivo de Cyber Threat Alliance.

Sophos X-Ops también proporciona una base interoperativa más sólida para la innovación, un componente esencial de la ciberseguridad debido a los agresivos avances en el cibercrimen organizado. Al entrelazar la experiencia de cada grupo, Sophos es pionero en el concepto de un Centro de Operaciones de Seguridad (SOC) asistido por inteligencia artificial (IA), que anticipa las intenciones de los analistas de seguridad y proporciona acciones defensivas relevantes. Sophos cree que este enfoque acelerará drásticamente los flujos de trabajo de seguridad y la capacidad de detectar y responder más rápidamente a indicadores de compromiso nuevos y prioritarios.

"Los adversarios han descubierto cómo trabajar en conjunto para comercializar ciertas partes de los ataques y, al mismo tiempo, crear nuevas formas de evadir la detección y aprovechar las debilidades de cualquier software para explotarlo en masa", dijo Craig Robinson, vicepresidente de investigación de IDC, Servicios de seguridad. "*Combinar la capacidad de abarcar una amplia gama de experiencia en inteligencia de amenazas con funciones asistidas por IA en el*

SOC permite a las organizaciones predecir y prepararse mejor para ataques inminentes y futuros".

###

Sobre Sophos

Sophos es un líder mundial en ciberseguridad de próxima generación y protege a más de 500.000 organizaciones y millones de consumidores en más de 150 países de las ciberamenazas más avanzadas de la actualidad. Con tecnología de inteligencia de amenazas, inteligencia artificial y aprendizaje automático de SophosLabs y SophosAI, Sophos ofrece una amplia cartera de productos y servicios avanzados para proteger a los usuarios, las redes y los puntos finales contra ransomware, malware, exploits, phishing y una amplia gama de otros ciberataques. Sophos proporciona una única consola de gestión integrada basada en la nube, Sophos Central, la pieza central de un ecosistema de ciberseguridad adaptable que cuenta con un lago de datos centralizado que aprovecha un amplio conjunto de API abiertas disponibles para clientes, socios, desarrolladores y otros proveedores de ciberseguridad. Sophos vende sus productos y servicios a través de socios revendedores y proveedores de servicios administrados (MSP) en todo el mundo. Sophos tiene su sede en Oxford, Reino Unido. Hay 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/