

SOPHOS

Sophos adquiere a Refactr para añadir automatización y orquestación de seguridad a sus soluciones MTR y XDR

- Refactr automatiza aún más la plataforma de ciberseguridad adaptable de la firma, que sustenta todas las soluciones de productos, servicios, inteligencia de amenazas y lago de datos de Sophos

CIUDAD DE MÉXICO. 03 de agosto de 2021.- [Sophos](#), líder mundial en ciberseguridad de última generación, anunció hoy que ha adquirido a Refactr, firma que desarrolla y comercializa una plataforma de automatización DevSecOps versátil que cierra la brecha entre el conjunto de prácticas de desarrollo de software DevOps y la ciberseguridad. Con sede en Bellevue, Washington, Refactr se fundó en 2017 y es una empresa privada.

A medida que los equipos de DevOps y de seguridad continúan adoptando enfoques de "TI como código" para administrar sus entornos, la capacidad de Refactr para automatizar cualquiera de esos procesos permite a los equipos volverse más escalables. Por ejemplo, con la plataforma de Refactr, los equipos de DevOps pueden aumentar los flujos de trabajo existentes de integración, entrega e implementación continua y los equipos de ciberseguridad pueden aprovechar el generador visual de arrastrar y soltar de la plataforma. Refactr lidera tanto en el sector privado como en el público y gubernamental, incluyendo al [Centro para la Seguridad de Internet](#) y la [Plataforma Uno de la Fuerza Aérea](#) de Estados Unidos.

Sophos está optimizando la plataforma de automatización DevSecOps de Refactr para agregar capacidades de Respuesta y Automatización de Orquestación de Seguridad (SOAR) a sus soluciones [Managed Threat Response \(MTR\)](#) y [Extended Detection and Response \(XDR\)](#). Las capacidades SOAR también ayudarán a automatizar el [ecosistema de ciberseguridad adaptable de Sophos](#), que sustenta todas las soluciones de productos, servicios, inteligencia de amenazas y lago de datos de Sophos.

De acuerdo con Gartner: *"El mercado de la tecnología de seguridad, en general, está en un estado de sobrecarga, con presión sobre los presupuestos, escasez de personal y demasiadas soluciones puntuales. Los clientes a menudo mencionan problemas con una sobrecarga de eventos o alertas, complejidad y duplicación de herramientas. En general, la automatización promete resolver muchos de estos problemas y, en ciberseguridad, SOAR es el vehículo principal para esta funcionalidad". Gartner señala además que: "los casos de uso propuestos para SOAR incluyen todo, desde la automatización de tareas rutinarias de seguridad hasta la simplificación de flujos de trabajo complejos y de nicho. Con la preparación adecuada, el compromiso de las habilidades y los recursos adecuados y una planificación cuidadosa centrada en el caso de uso, SOAR puede cumplir las promesas de reducción de la sobrecarga de eventos, mayor precisión de detección, escalabilidad del equipo, reducción del tiempo de detección y mejores operaciones de seguridad en general".*

SOPHOS

Es importante mencionar que el [Active Adversary Playbook 2021](#) de Sophos ha identificado que existen correlaciones claras y directas entre las cinco herramientas principalmente utilizadas por cibercriminales, por los administradores de TI y los profesionales de seguridad, sus tareas diarias. El informe también reveló que 37 grupos de ataque utilizaron más de 400 herramientas diferentes entre ellos. El tiempo medio de permanencia del atacante antes de la detección fue de 11 días, lo que les brinda hasta 264 horas para actividades maliciosas, desde movimiento lateral, reconocimiento, descarga de credenciales, exfiltración de datos y más. Detección temprana y respuesta a través de la automatización son funciones que pueden ayudar a minimizar estas estadísticas y mejorar la seguridad contra los atacantes que buscan constantemente nuevas formas de entrar y afianzarse.

“Las soluciones SOAR de primera generación han hecho avanzar nuestra industria de manera significativa, pero ahora estamos siendo testigos de una evolución en la que cada vez más empresas se están convirtiendo en firmas de software y nuestras soluciones de seguridad deben evolucionar en paralelo. Como hemos visto en incidentes recientes en la cadena de suministro, los atacantes se dirigen cada vez más a los canales de desarrollo de software y los defensores necesitan la capacidad de desplazarse más como lo hacen los atacantes. La industria necesita SOAR para madurar y convertirse en soluciones DevSecOps más capaces y generalizables, y la adquisición de Refactr por parte de Sophos nos ayudará a liderar el camino”, dijo Joe Levy, director de tecnología de Sophos. “Con Refactr, Sophos acelerará la integración de capacidades SOAR avanzadas en nuestro ecosistema de ciberseguridad adaptativa, la base de nuestro producto XDR y servicio MTR. Proporcionaremos un espectro completo de manuales de estrategias automatizados para nuestros clientes y socios, desde operaciones totalmente programables, junto con amplias integraciones con soluciones de terceros a través de nuestro programa de alianzas tecnológicas para trabajar con los diversos entornos de TI de la actualidad”.

Sophos continuará desarrollando y ofreciendo la plataforma de Refactr a su base actual y creciente de socios y organizaciones que desean crear automatizaciones de seguridad y TI personalizadas. La edición de la [versión pública](#) de Refactr continuará disponible también.

“Creamos la plataforma Refactr para que todas las organizaciones puedan ofrecer efectivamente las DevSecOps a través de la automatización integral de la seguridad. Nuestra plataforma fue diseñada específicamente para ser versátil, interoperable y fácil de usar. Los equipos de ciberseguridad ahora pueden colaborar con herramientas DevOps para construir fácilmente integraciones complicadas de seguridad y automatización de TI”, dijo Michael Fraser, CEO y cofundador de Refactr. “Nuestra misión es permitir que el DevSecOps se convierta en el enfoque moderno de la automatización, donde los casos de uso de ciberseguridad como SOAR y XDR, entre otros, se conviertan en bloques de construcción para las soluciones DevSecOps. Ya estamos viendo el éxito en proporcionar a las organizaciones nuestra tecnología emergente, incluido el Centro para la Seguridad de Internet y la Fuerza Aérea de los Estados Unidos. Estamos orgullosos de lo que logramos en Refactr y

SOPHOS

emocionados por la siguiente parte de nuestro viaje con Sophos para ayudar a crear un mundo más seguro a través de DevSecOps”.

Todo el equipo de desarrolladores e ingenieros de Refactr se ha unido a Sophos. Además de la oferta continua de la plataforma Refactr, Sophos planea comenzar a ofrecer opciones SOAR a principios de 2022.

###

Sobre Sophos

Sophos es la empresa líder mundial en ciberseguridad de última generación, que 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 para la detección 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, redes y endpoints contra ransomware, malware, exploits, phishing y una amplia gama de ciberataques. Sophos proporciona una plataforma única de gestión integral basada en la nube llamada Sophos Central, el eje 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 distribuidores y proveedores de servicios administrados (MSP) en todo el mundo. Sophos tiene su sede en Oxford, Reino Unido. Para más información, ingresa a www.sophos.com.

Síguenos en:

Facebook: <https://www.facebook.com/SophosLatam/>

Twitter: <https://twitter.com/SophosLatAm>

LinkedIn: <https://www.linkedin.com/company/sophos/>