Sophos integra Cloud Optix a XDR para ampliar su alcance a múltiples nubes

CIUDAD DE MÉXICO. 27 de diciembre de 2021.- Sophos anunció que su herramienta Extended Detection and Response (XDR) añadió la capacidades Cloud Optix (solución de seguridad en la nube de Sophos) para acceder a registros de actividad de Microsoft Azure (Azure) y Google Cloud Platform (GCP) junto con Amazon Web Services (AWS).

Lo anterior ayuda a los equipos de seguridad a ver un panorama más amplio en cuanto al ambiente de nube pública se refiere. De ese modo, XDR ya puede detectar, evaluar y fortalecer las cargas de trabajo en la nube y el acceso de los usuarios frente a vulnerabilidades y configuraciones erróneas de seguridad.

Las nuevas fuentes de datos de Cloud Optix en Sophos XDR ahora permiten investigar fácilmente las actividades de la API, la CLI y la consola de administración del entorno de nube de AWS, Azure y GCP. Mediante consultas prescritas y totalmente personalizables, los encargados de TI pueden descubrir intentos de acceso iniciales al entorno a través de roles comprometidos, así como recursos de usuario recién creados que indican persistencia dentro del entorno, y tácticas de infiltración.

Utilizando los hallazgos de Cloud Optix como indicadores, XDR hace uso del lago de datos de Sophos para investigar las vulnerabilidades de la carga de trabajo descubiertas por Sophos Intercept X para los agentes de protección. En este escenario, Cloud Optix alerta sobre estas vulnerabilidades de acceso y Sophos XDR inicia rápidamente las investigaciones para identificar la cantidad de intentos de autenticación en esas instancias.

De ese modo, los encargados de seguridad pueden actuar con confianza para eliminar el acceso y prevenir un ataque, con Cloud Optix proporcionando instrucciones de corrección guiadas para reducir el tiempo medio de resolución de las vulnerabilidades. Esta seguridad multi nube conectada desde una consola central ayuda a los equipos a ver el panorama general durante las investigaciones, lo que facilita la identificación rápida de riesgos y la prevención proactiva de incidentes.

Mejoras de Cloud Optix

Esta última actualización de Sophos Cloud Optix también incluye una variedad de adiciones para mejorar la supervisión de la seguridad en la nube y la respuesta de cumplimiento:

- **Anomalías de la actividad de AWS:** los nuevos modelos de Sophos AI analizan continuamente los registros de actividad de los usuarios de AWS CloudTrail. Esto permite a Cloud Optix plantear un escenario de la actividad de los usuarios individuales para identificar tanto los cambios accidentales como la actividad maliciosa. Hace que los eventos de AWS CloudTrail sean vistos de forma clara y detallada, identificando

anomalías de alto riesgo, tales como acciones realizadas fuera del horario laboral normal y aquellas nunca antes realizadas.

Con esta actualización, se ayuda a los equipos de ciberseguridad a concentrarse en investigar patrones de comportamiento de alto riesgo que podrían conducir a incidentes de seguridad en una fracción del tiempo que les tomaba antes.

- **Instancias de integración de Jira:** ahora, con una cuenta de Cloud Optix, cada entorno de nube estará vinculado a una plataforma del software empresarial Jira. De ese modo, se puede conectar a esta herramienta a cada uno de los entornos de nube de forma independiente o hacerlo de forma conjunta, todos hacia una sola plataforma de gestión de la empresa.

- **Visualización de Azure IAM:** ahora se pueden visualizar las relaciones entre los roles de IAM, los usuarios de IAM y los servicios en Azure para simplificar la administración de roles complejos e interconectados para varias suscripciones de Azure y Azure AD.

- **Alertas de políticas personalizadas:** ahora Cloud Optix permite crear alertas personalizadas basadas en consultas de búsqueda avanzada. Los análisis comparativos de seguridad futuros generarán alertas cuando se cumplan los criterios de la consulta.

###

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/