Sophos adquiere Braintrace para impulsar el ecosistema de ciberseguridad adaptable con la tecnología Network Detection and Response (NDR) de Braintrace

- *Las soluciones Network Detection and Response (NDR) proporcionan visibilidad en patrones de tráfico de red sospechosos, agregando inteligencia de amenazas novedosa a los servicios Managed Threat Response (MTR) y Rapid Response de Sophos, así como a las soluciones de Extended Detection and Response (XDR) y al lago de datos.*

CIUDAD DE MÉXICO. 22 de julio de 2021 - Sophos, líder mundial en ciberseguridad de última generación, anunció hoy que ha adquirido Braintrace, con lo que mejora aún más su ecosistema de ciberseguridad adaptativa gracias a la tecnología de detección y respuesta de red denominada 'Network Detection and Response' (NDR) patentada por la compañía. El NDR de Braintrace proporciona una visibilidad profunda de los patrones de tráfico de red, incluido el tráfico cifrado y los ataques Man-in-the-Middle (MitM) método mediante con el que los cibercriminales utilizan a un 'hacker intermediario' para interceptar la comunicación entre la víctima y sus datos sin que lo noten. Ubicada en Salt Lake City, Utah, Braintrace se fundó en 2016 y es una empresa privada.

Como parte de la adquisición, los desarrolladores de Braintrace, los científicos de datos y los analistas de seguridad se han unido a los equipos globales de Managed Threat Response (MTR) y Rapid Response de Sophos. El negocio de servicios de MTR y respuesta rápida se ha expandido rápidamente, estableciendo a Sophos como uno de los proveedores de ciberseguridad más grandes y de más rápido crecimiento en el mundo, con más de 5,000 clientes activos.

La tecnología NDR de Braintrace apoyará a los analistas de MTR y Rapid Response, así como a los clientes de Extended Detection and Response (XDR) de Sophos mediante la integración en el Ecosistema de Ciberseguridad Adaptable, que sustenta todos los productos y servicios de la firma. La tecnología de Braintrace también servirá como plataforma de lanzamiento para recopilar y reenviar datos de eventos de terceros desde firewalls, proxies, redes privadas virtuales (VPN) y otras fuentes. Estas capas adicionales de visibilidad e ingestión de eventos mejorarán significativamente la detección, búsqueda y respuesta de amenazas y actividades sospechosas.

"*No se puede proteger lo que no se sabe que existe y las empresas de todos los tamaños a menudo calculan mal la dimensión de los ataques, tanto en las instalaciones como en la nube. Los atacantes se aprovechan de esto, a menudo persiguiendo activos débilmente protegidos como medio de acceso inicial. Los defensores se benefician de un 'sistema de control de tráfico aéreo' que ve toda la actividad de la red, revela activos desconocidos y desprotegidos, además de exponer al malware evasivo de manera más confiable que los sistemas de protección contra*

intrusos (IPS)”, dijo Joe Levy, director de tecnología de Sophos. “*Estamos particularmente emocionados de que Braintrace haya creado esta tecnología para brindar mejores resultados de seguridad a sus clientes de Detección y Respuesta Administradas (MDR). Es difícil superar la eficacia de las soluciones creadas por equipos de profesionales y desarrolladores capacitados para resolver problemas de ciberseguridad del mundo real".*

Sophos implementará la tecnología NDR de Braintrace como una máquina alimentada desde puntos de acceso de prueba de red, para inspeccionar todo el tráfico de datos dentro de las redes. Estas implementaciones ayudan a descubrir amenazas dentro de cualquier tipo de red, incluidas aquellas que permanecen cifradas, y sirven como complemento a las capacidades de descifrado de Sophos Firewall. Además alimenta una variedad de modelos de aprendizaje automático entrenados para detectar patrones de red sospechosos o maliciosos, como conexiones a servidores de Comando y Control (C2), movimiento lateral y comunicaciones con dominios sospechosos. Dado que Braintrace desarrolló su tecnología NDR específicamente para monitoreo predictivo y pasivo, también proporciona captura de paquetes de red inteligente que los administradores de seguridad de TI y los cazadores de amenazas pueden usar como evidencia de respaldo durante las investigaciones. La nueva técnica de predicción y análisis NDR será patentada próximamente.

De acuerdo con Gartner *“En comparación con los enfoques tradicionales, donde el comportamiento malicioso se define en forma de factores prediseñados y motores de detección que inspeccionan el tráfico en busca de coincidencias, NDR adopta un enfoque diferente. En lugar de solo inspeccionar el tráfico con una lista de cargas útiles o comportamientos defectuosos conocidos, se enfoca en buscar patrones desconocidos en el tráfico de la red, calculando una probabilidad de que esa anomalía sea maliciosa*” indica Gartner sobre la tecnología de Braintrace. “*Los algoritmos de aprendizaje automático que se encuentran en el núcleo de muchos productos NDR ayudan a detectar el tráfico anómalo que a menudo se pasa por alto con otras técnicas de detección. Las capacidades de respuesta automatizada opcionales ayudan a descargar parte de la carga de trabajo de los equipos de respuesta de incidentes*” añade.

“*NDR es fundamental para el éxito en la búsqueda de amenazas. Es nuestro diferenciado y será aprovechado por los analistas para encontrar, interrumpir y remediar ciberataques”,* dijo Bret Laughlin, CEO y cofundador de Braintrace*. “Con nuestra propia tecnología NDR, el equipo de ciberseguridad responde más rápido y con mayor precisión debido a la visibilidad automatizada en tiempo real y la verificación de amenazas que tienen en el tráfico cifrado. Creamos la tecnología NDR desde cero para la detección y ahora, con Sophos, encajará en un sistema completo para brindar detección y respuesta en un ecosistema de múltiples proveedores*".

La tecnología NDR de Braintrace es un componente clave para defenderse de los ciberataques de hoy y del futuro. La investigación de Sophos demuestra cómo los adversarios cambian de táctica de forma agresiva y constante para evadir la detección y ejecutar sus ataques. NDR ayuda a descubrir el tráfico malicioso de malware, como CobaltStrike, BazaLoader y TrickBot,

que podrían generar ransomware y otros ataques. Esta visibilidad permite a los analistas y cazadores de amenazas anticiparse a cualquier posible ataque, incluidos los recientes REvil y DarkSide.

Sophos planea introducir la tecnología NDR de Braintrace para MTR y XDR en la primera mitad de 2022.

####

Sobre Braintrace
Braintrace es un proveedor de seguridad de fuente única que se especializa en el desarrollo de soluciones personalizadas y de vanguardia para sus clientes con su tecnología Network Detection and Response (NDR). Además de proporcionar Detección y Respuesta Extendida (XDR) y servicios de TI, Braintrace tiene una vasta experiencia en asesorar a los clientes en amplias áreas de riesgos comerciales relacionados con la seguridad, incluido el cumplimiento gubernamental y las cuestiones normativas. Con este conocimiento, Braintrace está posicionado para proporcionar experiencia y tecnología únicas para ayudar a las empresas de cualquier industria a mantenerse seguras. Más información está en braintrace.com.

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/