



## Sophos lanza su nuevo servicio de gestión y respuesta ante amenazas

*La nueva oferta de búsqueda, detección y respuesta de amenazas está impulsada por Machine Learning y análisis de expertos para neutralizar las amenazas de ciberseguridad más avanzadas*

**Ciudad de México a 8 de octubre de 2019.** – [Sophos](#) (LSE: SOPH), líder mundial en [seguridad de redes y terminales](#), anunció el lanzamiento de [Sophos Managed Threat Response \(MTR\)](#), un servicio de administración integral de búsqueda, detección y respuesta ante amenazas. Este servicio de reventa proporciona a las organizaciones un servicio dedicado de seguridad 24/7 para neutralizar las amenazas más sofisticadas y complejas.

Esta clase de amenazas incluyen atacantes activos, los cuales aprovechan ataques sin archivos y herramientas de administrador como PowerShell para escalar privilegios, filtrar datos y difundirlos lateralmente -como se explica en el artículo de [SophosLabs Uncut sobre el malware Lemon Duck PowerShell](#)-. Atentados como estos son difíciles de detectar, ya que involucran un adversario activo que utiliza herramientas legítimas para fines perjudiciales, por lo que el Managed Threat Response elimina esta amenaza por completo.

*“Los delincuentes cibernéticos están adaptando sus métodos y lanzando cada vez más ataques híbridos, los cuales combinan la automatización con el ingenio humano interactivo para evadir con mayor efectividad su detección. Una vez que logran establecerse, emplean técnicas ‘[living off the land](#)’ y otros métodos engañosos que requieren la interacción humana para descubrir e interrumpir sus ataques”,* señaló Joe Levy, director de Tecnología de **Sophos**. *“En su mayoría, otros servicios de MDR simplemente notifican a los clientes sobre posibles amenazas y luego los dejan solos para gestionar este problema. **Sophos MTR** no solo mejora los equipos con inteligencia adicional sobre amenazas, experiencia incomparable en productos y cobertura ininterrumpida, sino que también brinda a sus clientes la opción de tener un equipo altamente capacitado que tome medidas específicas para neutralizar amenazas, incluso las más sofisticadas”.*

Basado en [Intercept X Advanced](#) con detección y respuesta de punto final (EDR), **Sophos MTR** fusiona *machine learning* con análisis de expertos para mejorar la detección y eliminación de amenazas, además de realizar una investigación más profunda de alertas y acciones específicas. Estas capacidades innovadoras se basan en la adquisición de **Sophos** de la tecnología de [Rook Security](#) y [DarkBytes](#), la cual además incluye:

- **Búsqueda de amenazas dirigida por expertos: Sophos MTR** anticipa el comportamiento de atacantes e identifica nuevos indicios de peligros. **Sophos** busca y valida de manera proactiva incidentes potenciales e investiga eventos

casuales y adyacentes para descubrir nuevas amenazas que antes no podían detectarse.

- **Detección de adversidad avanzada:** **Sophos MTR** utiliza técnicas de investigación comprobadas para diferenciar el comportamiento legítimo de las tácticas, técnicas y procedimientos (TTP) utilizados por los atacantes. Junto con la telemetría mejorada de Sophos Central, que proporciona una imagen detallada y completa de las actividades adversas como parte del servicio, se puede determinar el alcance y la gravedad de las amenazas para una respuesta rápida.
- **Respuesta humana acelerada por máquina:** un equipo altamente capacitado de expertos de clase mundial genera y aplica inteligencia para detectar amenazas, y toma medidas para interrumpir, contener y neutralizar ataques de forma remota con rapidez y precisión.
- **Descubrimiento de activos y orientación prescriptiva del estado de la seguridad:** **Sophos MTR** proporciona información valiosa sobre activos administrados y no administrados, vulnerabilidades para evaluaciones de impacto mejor informadas y *threat hunting*. Además, la orientación prescriptiva y procesable para abordar debilidades de configuración y arquitectura permite a las organizaciones mejorar de manera proactiva su posición de seguridad con defensas reforzadas.

**Sophos MTR** puede personalizarse con diferentes niveles de servicio y modos de respuesta, esto para satisfacer las necesidades únicas y cambiantes de organizaciones de todos los tamaños y niveles de madurez. A diferencia de muchos servicios MDR que se centran en el monitoreo y la notificación de amenazas, **Sophos MTR** escala rápidamente y toma medidas contra las amenazas en función de las preferencias de cada organización.

**Sophos MTR** ya se encuentra disponible a través de [socios registrados de Sophos](#) en todo el mundo. Obtenga más [noticias de Sophos](#) y visite [Sophos.com](#) para obtener información adicional.

#### **Lo que dicen nuestros socios y analistas de la industria:**

*"Las empresas enfrentan ataques sofisticados desde todas las direcciones, por lo que es absolutamente crítico que no solo puedan detectar amenazas, sino que también respondan a ellas rápidamente",* dijo Aaron Sherrill, analista Senior de Seguridad de Información en 451 Research. *"Muchos proveedores afirman que ofrecen capacidades de respuesta, pero en realidad, pocos toman las medidas necesarias para eliminar las amenazas como parte de sus ofertas de detección y respuesta administradas (MDR).*

**Sophos MTR** *combina la consistente protección de punto final, con la experiencia humana y la inteligencia sobre recopilación de amenazas de [SophosLabs](#) para crear una oferta completamente nueva que satisfaga una creciente necesidad del mercado".*

*"La única forma de protegerse contra las amenazas avanzadas de hoy es combinar las mejores herramientas con las mentes humanas más brillantes",* dijo Jeremy Weiss, líder de Práctica de Seguridad Cibernética en CDW. *"Sophos Managed Threat Response es un parteaguas en el mercado, ya que combina el aprendizaje automático con el análisis*

*humano para obtener un enfoque evolucionado para la protección proactiva de seguridad. Esta oferta personalizable fortalece nuestras capacidades de búsqueda de amenazas existentes y nos ayuda a proteger mejor a nuestros clientes".*

*"El cibercrimen no duerme, por eso, las organizaciones necesitan protección las 24 horas", dijo Ken Hamilton, presidente y CEO de [Total Tech International Inc.](#) "Con Sophos Managed Threat Response, los clientes de Total Tech pueden estar seguros que están cubiertos, incluso durante el segundo y tercer turno que son notoriamente difíciles de cubrir. Las recomendaciones del estado de seguridad brindan un enorme valor adicional, ya que nos permite tomar medidas inmediatas para mejorar nuestras defensas".*

# # #

### **Sobre Sophos**

Como líder mundial en seguridad cibernética de próxima generación, **Sophos** protege a casi 400 mil organizaciones de todos los tamaños en más de 150 países de las amenazas cibernéticas más avanzadas de la actualidad. Desarrollado por SophosLabs -un equipo global de *Threat Intelligence* y *Data Science*- las soluciones nativas de la nube y mejoradas por IA de Sophos, aseguran protección en puntos finales (computadoras portátiles, servidores y dispositivos móviles) y redes contra tácticas y técnicas ciberdelictivas en evolución, incluidas las filtraciones de adversarios activos y automáticos, ransomware, malware, exploits, exfiltración de datos, phishing y más. La galardonada plataforma basada en la nube de Sophos Central integra toda la cartera de productos de **Sophos**, desde la solución de punto final, Intercept X, hasta el Firewall XG, en un único sistema llamado Seguridad Sincronizada. Los productos de **Sophos** están disponibles exclusivamente a través de un canal global de más de 47 mil socios y proveedores de servicios gestionados (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 bajo el símbolo "SOPH". Más información está disponible en [www.sophos.com](http://www.sophos.com)

### **Síguenos en:**

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

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

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

Instagram: <https://www.instagram.com/sophossecurity/?hl=es-la>

Youtube: <https://www.youtube.com/user/SophosProducts>

### **Contacto**

Mario García  
[mario@another.co](mailto:mario@another.co)  
M.: 55 3930 2474

Mariana Mondragón  
[mariana.mondragon@another.co](mailto:mariana.mondragon@another.co)