Publicado en CDMX el 20/12/2023

# [Vehículos eléctricos e Inteligencia Artificial, entre los principales riesgos de ciberseguridad para 2024](http://www.notasdeprensa.es)

## Timothy Liu, Director de Tecnología y Co-fundador de Hillstone Networks, comparte que al pasar página a otro año, es un buen momento para revisar lo que probablemente sucederá en ciberseguridad en 2024

 Para Timothy Liu, Director de Tecnología y Co-fundador de Hillstone Networks, desde una perspectiva general, muchas cosas seguirán siendo iguales: el ransomware y las fugas de datos persistirán como las principales preocupaciones, pero las nuevas tecnologías y vectores de amenazas asegurarán que los programas de seguridad sigan siendo de vital importancia. De acuerdo con el experto, el año pasado se experimentó una explosión en el uso de inteligencia artificial (IA) tanto en el ámbito del consumidor como en el empresarial con herramientas como ChatGPT, Bing, Bard y otros, y aunque la IA es una tecnología bastante antigua, lleva tiempo utilizándose en diversos sectores, incluida la ciberseguridad, desde hace una década o más.  "El campo de la IA sigue siendo como el "salvaje oeste", aunque la regulación está en proceso. Mientras tanto, existen múltiples vectores de amenazas en la IA. Por ejemplo, los datos deben alimentar el modelo de IA, y esos datos se convierten en un nuevo objetivo para hacktivistas y otros actores, así como también potencialmente proporcionar nuevos puntos de entrada a la red", comentó Liu. El phishing y otras tácticas de ingeniería social son otra área para observar. En el pasado, los ataques de phishing eran bastante fáciles de identificar debido a errores ortográficos, mala gramática y lenguaje rebuscado. Ahora, con la IA, estas tácticas se han vuelto más pulidas, precisas y selectivas. "Por ejemplo, imagine recibir un mensaje de voz deepfake, generado por IA, de su and #39;CEO and #39; solicitando información confidencial. ¿Cómo respondería?", señaló el co-fundador de Hillstone Networks. Liu también señaló que se ha hablado de la proliferación de dispositivos periféricos durante mucho tiempo, comenzando con las VPN SSL y el BYOD (traiga su propio dispositivo). Pero recientemente se ha producido una aceleración de nuevos endpoints, como dispositivos IoT (Internet de las cosas), instalaciones y trabajadores remotos conectados por 5G, e incluso VE (Vehículos Eléctricos) interconectados a la red. "Todo esto trae una evolución del panorama de amenazas de ciberseguridad, con un entorno nuevo y rico en objetivos para los hackers. Por supuesto, todavía se necesita proteger la infraestructura existente, pero ahora esas defensas deben extenderse mucho más allá del borde de red tradicional para cubrir nuevas superficies de ataque y nuevos puntos de entrada", explicó. Finalmente, señaló que la transformación de la confianza digital y seguridad jugará un papel importante, ya que cada vez más, los negocios dependen de transacciones digitales en todo el espectro; por lo tanto, construir la confianza digital se ha vuelto vital. Las Operaciones de Seguridad, o SecOps, están comenzando a recibir mucha más atención como un medio para pasar de una postura de preintrusión a postintrusión; de simplemente detectar ataques a una respuesta y mitigación contundentes. Como resultado, ha habido un mayor énfasis en herramientas como SIEM (información de seguridad y gestión de eventos) y XDR (detección y respuesta extendida), este último agrega datos de otros dispositivos de seguridad, normaliza, correlaciona y analiza para descubrir posibles amenazas.

**Datos de contacto:**

Carlos Soto

CEMPR Digital

5532322068

Nota de prensa publicada en: [https://www.mexicopress.com.mx/vehiculos-electricos-e-inteligencia-artificial\_1](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Inteligencia Artificial y Robótica Comunicación Software Ciberseguridad Innovación Tecnológica



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)