[notasdeprensa.jpg](http://www.mexicopress.com.mx)Publicado en Ciudad de México el 24/08/2022

# [IA gana terreno en ciberseguridad: Hillstone Networks](http://www.notasdeprensa.es)

## Las técnicas avanzadas de IA y ML, como el análisis de Big Data, pueden ayudar a detectar el malware y las amenazas avanzadas con un gran grado de precisión, incluidas las mutaciones y variantes

La Inteligencia Artificial (IA) gana cada vez más protagonismo y una de las tecnologías que contribuye a ello es el aprendizaje profundo, a través de redes neuronales artificiales, que ha logrado resultados significativos en los campos de computación, exploración de múltiples lenguajes y procesos autónomos. Además, las técnicas de IA son muy prometedoras en las áreas de análisis, detección y respuesta a las amenazas, su capacidad para aplicar técnicas avanzadas de análisis y basadas en la lógica puede aliviar en gran medida la carga de los administradores de seguridad y permitirles tomar medidas razonables y eficaces en respuesta a los ataques y amenazas. El análisis del comportamiento de usuarios y entidades (UEBA), por ejemplo, puede ayudar a detectar a personas internas malintencionadas, así como atacantes externos hostiles que se infiltran en la red y sus activos. Por otro lado, el análisis del tráfico de la red es otra área en la que la IA puede brillar; el volumen del tráfico de la red suele ser masivo y llevar a cabo un análisis exhaustivo y continuo que sólo con esfuerzos humanos sería no solo difícil, sino imposible. Hillstone Networks, proveedor líder de soluciones de seguridad de red y gestión de riesgos, detalló que las técnicas avanzadas de IA y ML, como el análisis de Big Data, pueden ayudar a detectar el malware y las amenazas avanzadas con un gran grado de precisión, incluidas las mutaciones y variantes. De hecho, unificando estas tecnologías se pueden mejorar los procesos de automatización de seguridad codificando muchas tareas rutinarias y repetitivas en flujos de trabajo, lo que permite al personal del SOC centrarse en la resolución de amenazas y en otros esfuerzos de misión crítica. Otros métodos para aprovechar la IA son el uso de redes neuronales recurrentes para identificar vulnerabilidades de programas binarios, la agrupación de gráficos para permitir la detección de bots, basada en algoritmos generadores de dominio (DGA), el monitoreo multicapa (MLP) para detectar tráfico de red anormal, entre otras. La IA está ganando terreno en la lucha contra las ciberamenazasSi se repasan los casos de uso de la IA se observará que cada uno de ellos se centra en la detección basada en el comportamiento. Independientemente de sus tácticas evasivas, el malware casi siempre muestra ciertos comportamientos, a menudo sutiles, que pueden discernirse analizando las enormes cantidades de datos que se generan en una red típica. Y eso es precisamente lo que la IA y el ML hacen muy bien: digerir, correlacionar y analizar enormes cantidades de datos para detectar pequeños matices o indicadores de amenaza, que luego se pueden presentar al equipo de seguridad para que los investigue. La IA puede ayudar a agilizar los procesos y a realizar tareas repetitivas, a reducir de forma inteligente los falsos positivos y a disminuir la carga de trabajo del sobrecargado personal de TI y de seguridad.

**Datos de contacto:**

Carlos Soto

5532322068

Nota de prensa publicada en: [https://www.mexicopress.com.mx/ia-gana-terreno-en-ciberseguridad-hillstone](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Inteligencia Artificial y Robótica E-Commerce Software Ciberseguridad Ciudad de México

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

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