Publicado en CDMX el 31/05/2022

# [El futuro de la IA en el desarrollo de soluciones de ciberseguridad según Hillstone Networks](http://www.notasdeprensa.es)

## La tecnología de inteligencia artificial puede mejorar las capacidades de detección, protección y respuesta ante ciberamenazas

 Hillstone Networks, proveedor líder de soluciones de seguridad de red y gestión de riesgos, comparte la importancia de utilizar soluciones de ciberseguridad basadas en Inteligencia Artificial, así como su visión del futuro de esta tecnología y los beneficios que puede aportar en la lucha contra las amenazas cibernéticas. En términos de seguridad de la red, el uso de la tecnología de inteligencia artificial ha madurado mucho y ha proliferado en la industria de la ciberseguridad. Tal es el caso de PCA o análisis de componentes principales, el cual puede identificar automáticamente las características de uso de las APIs para descubrir vulnerabilidades de día cero. 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 perceptrón multicapa (MLP) para detectar tráfico de red anormal, etc. Aunque la IA no está avanzada hasta el punto de funcionar de forma autónoma, puede mejorar en gran medida los flujos de trabajo de seguridad, renunciando a las tareas más mundanas y repetitivas de los equipos de seguridad, permitiéndoles, de esta manera, centrar sus esfuerzos en cuestiones más críticas para el negocio que requerirían inteligencia humana. Bajo este escenario Hillstone Networks considera que a lo largo del año más proveedores dedicarán más recursos a la investigación en profundidad sobre cómo la tecnología de inteligencia artificial puede mejorar las capacidades de detección, protección y respuesta de sus productos. Asimismo se incrementará el uso de redes neuronales profundas para extraer automáticamente las características de los datos en bruto del lado de la red y del lado del host. Esto ayudará a mitigar la dependencia de los expertos en seguridad para extraer las características de los datos, que pueden automatizarse. Como resultado, los expertos en seguridad podrán emplear su tiempo en tareas más estratégicas y urgentes. Dado que la metodología de los ataques de caja negra se encuentra todavía en una fase temprana de desarrollo, en la actualidad no existe un método fiable para juzgar el rendimiento de los modelos de aprendizaje automático. Por lo tanto, el aprendizaje de muestras pequeñas sigue siendo muy valioso para el sector de la seguridad de redes. Además, se debe considerar que el marco general de las redes neuronales profundas necesita una inspección más profunda.Por último, la tecnología de detección de amenazas basada en el modelo de redes neuronales gráficas merece atención. Un modelo de red neuronal gráfica (GNN) puede aprender de los datos estructurados en forma de gráfico, a diferencia de los datos tradicionales más lineales. Al aprender los patrones de flujo de los ataques, el modelo GNN puede detectar dinámicamente los ataques incluso cuando modifican intencionadamente el tamaño de los paquetes y los tiempos de llegada para despistar a los métodos de detección tradicionales.

**Datos de contacto:**

Carlos Soto

5532322068

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

Categorías: Inteligencia Artificial y Robótica Software Ciberseguridad



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