# Inteligencia Artificial: la aliada para frenar el auge de ciberdelitos según IMMUNE Technology Institute

**Con el avance continuo de la tecnología se generan nuevas oportunidades para los ciberdelincuentes, que aprovechan cada brecha emergente para desarrollar tácticas más complejas y realizar ataques altamente focalizados**

La integración de la Inteligencia Artificial está transformando la ciberseguridad ofreciendo capacidades predictivas y proactivas a tiempo real, lo cual permite identificar patrones de comportamiento malicioso y adaptarse a las ofensivas, estableciendo así un nuevo estándar en la seguridad digital.

La ciberseguridad es una prioridad indiscutible para individuos, empresas y gobiernos. A medida que se desarrollan avances tecnológicos, se abren nuevas puertas para los delincuentes cibernéticos, que aprovechan las brechas y vulnerabilidades emergentes para idear tácticas más sofisticadas y ataques más específicos.

El robo de datos, la suplantación de identidad y las estafas económicas por internet están a la orden del día. Tanto es así que, en 2022 en España, tal y como recoge un informe del Ministerio del Interior, los ciberdelitos aumentaron un 22% respecto al año anterior, y no parece que en este año la cifra vaya a ser menor.

Ante el avance de este tipo de delitos, empresas, organismos e instituciones toman medidas para proteger la privacidad y ofrecer una mayor seguridad a los usuarios. Es en este campo donde toma especial relevancia la Inteligencia Artificial, que ha emergido como un aliado poderoso en la lucha contra las amenazas digitales, revolucionando el campo de la ciberseguridad.

"La inteligencia artificial está transformando la ciberseguridad. Su capacidad predictiva, impulsada por el aprendizaje automático y los modelos de análisis avanzado, permite no solo identificar patrones sutiles de comportamiento malicioso, sino también adaptar las defensas en tiempo real. De esta manera, se está estableciendo un nuevo estándar en la defensa proactiva", explica Miguel Rego, director del área de Ciberseguridad en IMMUNE Technology Institute.

La revolución de la IA en el avance contra los ciberdelincuentes

Desde el análisis de grandes volúmenes de datos hasta la identificación de patrones, la IA ha potenciado las capacidades de detección y respuesta en tiempo real. Estos sistemas inteligentes pueden no sólo reconocer y aislar comportamientos anómalos en una red, sino también anticipar posibles amenazas mediante la observación de tendencias, patrones o incoherencias que

podrían pasar desapercibidas para los métodos de seguridad convencionales. Esta capacidad de análisis contextual y respuesta automática ha elevado el umbral de eficacia en la defensa cibernética, estableciendo un estándar más alto para la seguridad digital en un entorno caracterizado por su rápida evolución.

Este enfoque basado en el uso de la inteligencia artificial como herramienta para hacer frente a los ciberdelincuentes no solo se limita a la etapa inicial de inicio de sesión, sino que se integra de manera continua a lo largo de la experiencia del usuario. Al monitorear constantemente los patrones de comportamiento, la IA puede adaptarse dinámicamente a medida que el usuario interactúa con la plataforma. Esto implica un análisis constante de cada sesión iniciada, evaluando la autenticidad de las transacciones, el acceso a datos sensibles y las actividades inusuales.

"En IMMUNE somos conscientes de la creciente importancia que está adquiriendo la Inteligencia Artificial en este campo, tanto a nivel del usuario como empresarial. Por eso, creemos que formar a los alumnos en esto les proporcionará los conocimientos necesarios para satisfacer la demanda de perfiles profesionales que las empresas buscan, con el fin de ofrecer respuestas a usuarios cada vez más preocupados", concluye Rego.

E l Bootcamp Ciberseguridad & Inteligencia Artificial incorpora un módulo de Prompt Engineering mediante el cual el estudiante entenderá las posibilidades de uso de las diferentes herramientas de IA como GPT, Bard, o GitHub Copilot, cómo hacer un buen prompt, y en qué consisten los prompts categorizados aplicados a la ciberseguridad.

Hay que tener en cuenta que el uso de la IA en ciberseguridad plantea desafíos éticos y de privacidad ya conocidos. La necesidad de asegurar la transparencia y la responsabilidad en el desarrollo y aplicación de algoritmos es crucial para evitar posibles riesgos, marcando así punto de inflexión en la defensa digital. Su integración continua y el desarrollo ético son fundamentales para fortalecer la resiliencia cibernética.