Kudelski Security lanza una nueva cartera de servicios de seguridad con IA

El nuevo programa responde a una creciente demanda de asesoramiento estratégico y táctico que permita a los clientes afrontar los retos de seguridad únicos que plantea la aplicación de la IA en operaciones y entornos empresariales.

Cheseaux-sur-Lausanne, Suiza y Phoenix (AZ), EE.UU., 15 de octubre, 2024 – Kudelski Security, la división de ciberseguridad del Grupo Kudelski (SIX:KUD.S), ha anunciado hoy el lanzamiento de nueva funcionalidad en seguridad aplicada a la inteligencia artificial. La cartera de seguridad con IA es un conjunto completo de servicios diseñados para ayudar a las empresas a prepararse y mitigar las crecientes amenazas asociadas a los sistemas y aplicaciones basados en IA que permiten a los usuarios aprovechar la tecnología de forma segura, eficaz y en cumplimiento de las normativas emergentes.

A medida que las tecnologías de IA se integran en las operaciones empresariales, aparecen nuevas áreas susceptibles de ataque. Kudelski Security se ha centrado en la seguridad con IA durante más de cinco años, lo que permite la innovación sin comprometer la seguridad mucho antes de la llegada de las principales herramientas de IA como ChatGPT y Microsoft Copilot. Aprovechando esta amplia experiencia técnica y en ciberseguridad, hemos desarrollado una cartera de servicios que proporciona apoyo tanto estratégico como táctico para asegurar las aplicaciones de IA, sus sistemas asociados y el ecosistema operativo más amplio.

"Nuestra nueva cartera de servicios de seguridad de IA es una respuesta directa a la urgente necesidad de marcos de seguridad robustos en el panorama de la IA en rápida evolución. Las empresas de hoy en día navegan por territorios inexplorados donde la IA ofrece un enorme potencial pero también riesgos significativos" dijo David Chétrit, director ejecutivo de Kudelski Security. "Nuestro objetivo es garantizar que nuestros clientes puedan innovar con confianza, sabiendo que sus iniciativas de IA se construyen sobre una base de seguridad, cumplimiento y resiliencia".

La cartera de servicios de seguridad con IA incluye:

- **Desarrollo y aplicación de la estrategia de seguridad con IA:** Un enfoque estratégico para abordar los retos de gobernanza, técnicos y normativos, incluida la creación de un marco de gobernanza a medida y una estrategia de seguridad integral para garantizar el cumplimiento de los principios éticos y la normativa.
- **Cumplimiento de la ley de IA de la UE:** Asesoramiento para navegar por el cambiante panorama normativo y garantizar el cumplimiento de la Ley de Inteligencia Artificial de la UE, lo que mejora la competitividad global y la confianza de las partes interesadas.
- **Evaluación de riesgos y amenazas mediante IA:** Una evaluación exhaustiva de las aplicaciones de IA, incluida su arquitectura asociada, que evalúe las amenazas específicas, identifique los problemas y los clasifique en función de su valor en situaciones críticas, lo que garantiza la resolución oportuna.
- **Pruebas de seguridad para Aplicaciones de IA ?** Tácticas de seguridad ante ataques adaptadas a las aplicaciones impulsadas por IA que utilizan modelos LLM (Large Language Model, por sus

siglas en inglés), para identificar y abordar vulnerabilidades, lo que aumenta la confianza en la seguridad e integridad de los sistemas desplegados.

"La rápida evolución de las herramientas y soluciones impulsadas por IA ha creado una necesidad apremiante de reducir las superficies de ataque y disminuir los riesgos de seguridad", afirmó Nathan Hamiel, director principal de investigación en Kudelski Security y responsable del área black hat® para la ciencia de datos de IA y de modelos de lenguaje. Nuestras capacidades de seguridad de IA están diseñadas para identificar y mitigar estos riesgos, al utilizar modelos avanzados de amenazas y Red Teaming para garantizar que los sistemas de IA sean robustos frente a vulnerabilidades conocidas y desconocidas, lo que permite una integración segura en operaciones críticas".

A medida que las empresas continúan adoptando la IA a un ritmo acelerado, la cartera de servicios de seguridad de IA de Kudelski Security ofrece la garantía de que la seguridad es una parte integral del diseño y el despliegue de las tecnologías de IA. Este enfoque proactivo no solo mitiga los riesgos, sino que también garantiza que los sistemas de IA funcionen de forma segura y conforme a la normativa del sector.

Si desea más información sobre la cartera de servicios de seguridad con IA de Kudelski Security, visite https://kudelskisecurity.com/services/ai-security-services/

Acerca de Kudelski Security

Kudelski Security es el principal asesor e innovador en ciberseguridad para las organizaciones actuales más preocupadas por la seguridad. Nuestro enfoque a largo plazo de las asociaciones con clientes nos permite evaluar continuamente su postura de seguridad para recomendar soluciones que reduzcan el riesgo empresarial, mantengan la conformidad y aumenten la eficacia general de la seguridad. Con clientes que incluyen empresas de Fortune 500 y organizaciones gubernamentales en Europa y en todo Estados Unidos, abordamos los entornos más complejos a través de un conjunto incomparable de capacidades de solución que incluyen consultoría, tecnología, servicios de seguridad gestionados e innovación personalizad Si desea más información, visite www.kudelskisecurity.com.

Contacto de prensa

Christina Anderson
Directora general de Global Communications
Christina.anderson@kudelskisecurity.com