# Kudelski Security Launches New AI Security Service Portfolio

*The new program responds to a growing demand for strategic and tactical advice that enable customers to address the unique security challenges of applying AI in business operations and environments.*

**Cheseaux-sur-Lausanne, Switzerland and Phoenix (AZ), U.S., October 15, 2024** – Kudelski Security, the cybersecurity division within the Kudelski Group (SIX:KUD.S), today announced the launch of new security capabilities applied to Artificial Intelligence. The AI Security portfolio is a comprehensive suite of services designed to help businesses prepare for and mitigate the growing threats associated with AI-powered systems and applications enabling users to leverage the technology securely, effectively, and in compliance with emerging regulations.

As AI technologies become integral to business operations, they introduce a new and complex attack surface that malicious actors can exploit. Kudelski Security has been focused on AI security for over five years, enabling innovation without compromising security long before the advent of mainstream AI tools like ChatGPT and Microsoft Copilot. Leveraging this extensive technical and cybersecurity expertise, the business has developed a portfolio of services that provides both strategic and tactical support to secure AI applications, their associated systems, and the broader operating ecosystem.

“Our new AI Security Services portfolio is a direct response to the urgent need for robust security frameworks in the rapidly evolving AI landscape. Businesses today are navigating uncharted territories where AI offers tremendous potential but also raises significant risks” said David Chétrit, CEO of Kudelski Security “Our goal is to ensure that our clients can innovate with confidence, knowing that their AI initiatives are built on a foundation of security, compliance, and resilience."

The AI Security Services Portfolio includes:

- **AI Security Strategy Development and Implementation:** A strategic approach to address governance, technical, and regulatory challenges, including the creation of a tailored governance framework and comprehensive security strategy to ensure compliance with ethical principles and regulations.
- **EU AI Act Compliance:** Advisory support to navigate the evolving regulatory landscape and ensure compliance with the EU AI Act, enhancing global competitiveness and stakeholder trust.
- **AI Threat and Risk Assessment**: A thorough evaluation of AI applications, including their associated architecture, assessing specific threats, identifying issues, and ranking them by criticality, ensuring timely mitigation.
- **AI Application Security Testing:** Offensive security tactics tailored for AI-powered applications using Large Language Models (LLMs) to identify and address vulnerabilities, boosting confidence in the security and integrity of deployed systems.

“The rapid evolution of AI-powered tools and solutions has created a pressing need to reduce attack surfaces and lower security risks,” said Nathan Hamiel, Sr. Director of Research at Kudelski Security and Black Hat® track lead for AI, machine learning and data science. “Our AI Security capabilities are designed to identify and mitigate these risks, using advanced threat modeling and red teaming to ensure

AI systems are robust against both known and unknown vulnerabilities, enabling secure integration into critical operations."

As businesses continue to adopt AI at a rapid pace, Kudelski Security's AI Security Services portfolio provides the assurance that security is an integral part of the design and deployment of AI technologies. This proactive approach not only mitigates risks but also ensures that AI systems operate safely and in compliance with industry regulations.

For more information about Kudelski Security's AI Security Services Portfolio, visit https://kudelskisecurity.com/services/ai-security-services/

**About Kudelski Security**

Kudelski Security is the premier advisor and cybersecurity innovator for today's most security-conscious organizations. Our long-term approach to client partnerships enables us to continuously evaluate their security posture to recommend solutions that reduce business risk, maintain compliance and increase overall security effectiveness. With clients that include Fortune 500 enterprises and government organizations in Europe and across the United States, we address the most complex environments through an unparalleled set of solution capabilities including consulting, technology, managed security services and custom innovation. For more information, visit www.kudelskisecurity.com.

**Media Contact**

Christina Anderson
Senior Director, Global Communications
Christina.anderson@kudelskisecurity.com