Kudelski Security lance un nouveau portefeuille de services dédiés à la sécurité de l'IA

Ce nouveau programme répond à une demande croissante en matière de conseils stratégiques et tactiques permettant aux clients de faire face aux enjeux de sécurité propres à l'utilisation de l'IA au niveau des opérations commerciales et des environnements de travail.

Cheseaux-sur-Lausanne, Suisse, et Phoenix (AZ), États-Unis, 15 octobre, 2024 – Kudelski Security, la division cybersécurité du Groupe Kudelski (SIX: KUD.S), a annoncé aujourd'hui le lancement de nouveaux services de sécurité destinés à l'intelligence artificielle. Le nouveau portefeuille AI Security est une suite complète de services conçus dans le but d'aider les entreprises à se préparer à faire face aux menaces croissantes associées aux systèmes et applications alimentés par l'IA et à en atténuer les risques, permettant ainsi aux utilisateurs d'exploiter cette technologie de manière sécurisée, efficace et en conformité avec les dernières réglementations.

À mesure que les technologies liées à l'IA deviennent partie intégrante des opérations commerciales, celles-ci créent une nouvelle surface d'attaque complexe à disposition de n'importe quel acteur malveillant. Kudelski Security travaille dans le domaine de la sécurité de l'IA depuis plus de cinq ans, grâce à des solutions à la fois sécurisées et propices à l'innovation, et ce bien avant l'avènement des outils d'IA grand public tels que ChatGPT et Microsoft Copilot. En s'appuyant sur sa solide expertise technique et ses compétences en matière de cybersécurité, Kudelski Security a créé un portefeuille de services fournissant une assistance à la fois stratégique et tactique pour sécuriser les applications d'IA ainsi que les systèmes qui y sont associés et, plus largement, les écosystèmes d'exploitation.

« Notre nouveau portefeuille de services dédiés à la sécurité de l'IA répond directement à un besoin urgent de sécuriser tout ce qui concerne cette technologie dont l'évolution est incroyablement rapide. Aujourd'hui, les entreprises naviguent à vue : l'IA présente un potentiel énorme mais aussi des risques importants », a déclaré David Chétrit, CEO de Kudelski Security. « Notre objectif est de faire en sorte que nos clients puissent innover en toute confiance, en sachant que leurs initiatives en matière d'IA reposent sur une base solide dont sécurité, conformité et résilience sont les maîtres-mots ».

Le portefeuille de services dédiés à la sécurité de l'IA comprend :

- **L'élaboration et la mise en œuvre d'une stratégie de sécurité en matière d'IA :** Il s'agit de mettre en place une approche stratégique permettant de relever les défis liés à la gouvernance, à la technologie et à la réglementation de ces nouveaux systèmes, ce qui implique notamment la création d'un cadre de gouvernance adapté et une stratégie de sécurité complète pour assurer la conformité des opérations avec les principes éthiques et les réglementations en vigueur.
- **La mise en conformité avec la loi européenne sur l'IA :** Les clients bénéficient d'un accompagnement et de conseils pour comprendre les tenants et aboutissants des réglementations concernées, qui sont en constante évolution dans ce domaine, et pour garantir la conformité de leurs actions avec la loi européenne sur l'IA. Ceci leur permettra notamment d'accroître la compétitivité de leur entreprise à l'international ainsi que de renforcer la confiance de toutes les parties prenantes.
- **Une évaluation des menaces et des risques liés à l'IA :** Le portefeuille offre une évaluation en profondeur des applications d'IA, y compris l'analyse de l'architecture qui leur est associée. En

analysant des menaces spécifiques, en identifiant les éventuels problèmes et en les classant par ordre de gravité, le service de Kudelski Security permet d'atténuer les menaces au moment opportun.

- **Evaluation de sécurité des applications AI:** Ces tactiques de sécurité offensives adaptées aux applications alimentées par l'IA ont recours à de grands modèles de langage (LLM) pour identifier les vulnérabilités et y remédier, permettant ainsi de renforcer la confiance dans la sécurité et l'intégrité des systèmes déployés.

« L'évolution rapide des outils et des solutions alimentés par l'IA a créé un besoin urgent de réduire les surfaces d'attaque et de diminuer les risques liés à la sécurité », a déclaré Nathan Hamiel, Directeur de la recherche chez Kudelski Security et membre du comité d'examen de Black Hat®, au sein duquel il apporte son expertise en AI, ML, et data science. « Nos compétences en matière de sécurité de l'IA permettent d'identifier et d'atténuer ces risques en utilisant la modélisation avancée des menaces et le Red Teaming pour nous assurer de la capacité des systèmes d'IA à faire face aux vulnérabilités connues et inconnues, et ainsi garantir une intégration sécurisée de l'IA dans toutes les opérations essentielles ».

Alors que les entreprises continuent d'adopter l'IA à un rythme effréné, le portefeuille de services dédiés à la sécurité de l'IA de Kudelski Security offre l'assurance d'une conception et d'un déploiement des technologies de l'IA en toute sécurité. Cette approche proactive permet non seulement d'atténuer les risques, mais aussi de garantir que les systèmes d'IA fonctionnent en toute sécurité et en conformité avec les réglementations de l'industrie.

Pour de plus amples informations à propos du portefeuille de services dédiés à la sécurité de l'IA de Kudelski Security, rendez-vous sur https://kudelskisecurity.com/services/ai-security-services/

À propos de Kudelski Security

Kudelski Security est le partenaire privilégié des sociétés conscientes des questions de sécurité, offrant conseil et solutions innovantes en matière de cybersécurité. Notre approche, consistant à envisager des partenariats à long terme avec nos clients, nous permet d'évaluer leur situation sécuritaire de manière continue afin de leur recommander des solutions qui leur permettront de réduire leurs risques business, de maintenir le niveau de conformité et d'accroître le niveau global de sécurité. Avec des clients classés au Fortune 500, comprenant des entreprises et des organisations gouvernementales en Europe et aux États-Unis, nous répondons aux besoins les plus complexes grâce à un ensemble unique de solutions comprenant conseils, technologie, services de sécurité managés et innovation personnalisée. Pour de plus amples informations, veuillez consulter le site Internet www.kudelskisecurity.com.

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