Kudelski Security lanciert neues Service-Portfolio für Cybersicherheit im KI-Bereich

Mit dem neuen Angebot reagiert Kudelski Security auf die wachsende Nachfrage nach strategischer und taktischer Beratung, die es Kunden ermöglicht, sich den besonderen Herausforderungen rund um den Einsatz von KI in Betriebsabläufen und Umgebungen zu stellen.

Cheseaux-sur-Lausanne, Schweiz und Phoenix (AZ), U.S., 15. Oktober 2024 – Kudelski Security, das Cybersecurity-Unternehmen der Kudelski Gruppe (SIX:KUD.S), hat heute die Marktpremiere von neuen, auf den KI-Bereich abgestimmten Cybersicherheits-Services bekanntgegeben. Bei dem neuen „AI Security Services Portfolio" handelt es sich um Services, die speziell darauf ausgerichtet sind, Unternehmen bei der Vorbereitung auf Bedrohungen und Minderung von Risiken im Zusammenhang mit KI-basierten Systemen und Applikationen zu unterstützen. Anwender werden dadurch befähigt, diese Technologien sicher und effizient zu nutzen und entsprechende Vorgaben einzuhalten.

KI-Technologien werden zunehmend zu einem festen Bestandteil zahlreicher Geschäftsabläufe. Dabei bieten sie Hackern jedoch neue und komplexe Angriffsflächen. Kudelski Security beschäftigt sich bereits seit fünf Jahren intensiv mit Cybersicherheit im KI-Bereich und hatte die Unterstützung für Innovation mit kompromissloser Sicherheit schon lange vor dem Erscheinen von KI-Tools wie ChatGPT oder Microsoft Copilot im Programm. Aufbauend auf diesem weitreichenden Fachwissen rund um Technik und Cybersicherheit hat Kudelski Security ein Service-Portfolio geschaffen, das den Anwendern strategisch und taktisch dabei hilft, ihre KI-Applikationen samt angeschlossener Systeme und dem weiteren Betriebssystem-Umfeld wirksam abzusichern.

„Unsere neuen AI Security Services sind die direkte Antwort auf den dringenden Bedarf nach robusten Security-Frameworks angesichts der rasanten Entwicklungen im KI-Bereich. Unternehmen betreten heute Neuland, in dem KI ein enormes Potential bereithält, aber auch erhebliche Gefahren mit sich bringt", so David Chétrit, Kudelski Securitys CEO. „Unser Ziel ist es, sicherzustellen, dass unsere Kunden hier mit Zuversicht innovativ unterwegs sein können, weil sie wissen, dass ihre KI-Initiativen auf einer soliden Grundlage aus Sicherheit, Vorschrifteinhaltung und Resilienz aufbauen."

Kudelski Security AI Security Services Portfolio beinhaltet:

- **Entwicklung und Umsetzung von KI-Sicherheitsstrategien:** Ein strategischer Ansatz zur Bewältigung KI-spezifischer Herausforderungen im Zusammenhang mit Unternehmensführung, Technik und Vorschriften. Dieser beinhaltet die Erstellung eines massgeschneiderten Rahmenkonzepts für die Unternehmensführung ebenso wie eine umfassende Sicherheitsstrategie, die für die Einhaltung von ethischen Prinzipien und Vorgaben sorgen.
- **Konformität mit der KI-Verordnung der EU („AI Act"):** Unterstützende Beratung zur Orientierung im rasch voranschreitenden Bereich der Vorschriften und Regelungen, sowie Sicherstellung der Einhaltung des „EU AI Act" zur Stärkung der globalen Wettbewerbsfähigkeit und des Vertrauens der Stakeholder.
- **Bedrohungs- und Risikobewertung für KI-Anwendungen**: Gründliche Untersuchung und Bewertung eingesetzter KI-Applikationen und deren technischen Umgebungen, einschliesslich Bewertung spezifischer Bedrohungen sowie die Erkennung, Priorisierung und zeitgerechte Entschärfung von Problemen.

- **AI Application Security Testing:** Offensive Cybersicherheits-Taktiken mit spezieller Ausrichtung auf KI-basierte Anwendungen, die Large Language Models (LLMs) nutzen. Ziel ist die Identifizierung und Behebung von Schwachstellen, um das Vertrauen der Benutzer in die Sicherheit und Integrität der eingesetzten Systeme zu stärken.

„Die rasante Weiterentwicklung der KI-Tools und Lösungen hat zu einem akuten Bedarf nach der Reduktion von Angriffsflächen und Risiken geführt," erklärt Nathan Hamiel, Senior Director of Research bei Kudelski Security und Black Hat® Track Lead for AI, ML and Data Science. „Unser Cybersicherheits-Instrumentarium für KI-Anwendungen ist speziell darauf ausgelegt, diese Risiken aufzudecken und zu mindern. Dabei setzen wir fortschrittliches Threat Modeling und Red Teaming-Methoden ein, um sicherzustellen, dass die KI-Anwendungen stabil bezüglich bekannter und unbekannter Schwachstellen sind. Das ist die Voraussetzung für eine sichere Einbindung in kritische Betriebsabläufe".

Während der Einsatz von KI in Unternehmen immer rascher fortschreitet, bietet Kudelski Securitys „AI Security Services Portfolio" die Gewissheit zuverlässiger Cybersicherheit bei der Entwicklung und Bereitstellung von KI-Technologien. Dieser proaktive Ansatz vermindert nicht nur Risiken, sondern sorgt auch dafür, dass KI-Systeme sicher und vorschriftsgemäss betrieben werden.

Für weitere Informationen über das „AI Security Services Portfolio" von Kudelski Security besuchen Sie uns auf https://kudelskisecurity.com/services/ai-security-services/

Über Kudelski Security

Kudelski Security ist Marktführer in der Beratung und Innovation von Cybersicherheit für moderne Unternehmen mit erhöhtem Sicherheitsbedarf. Unser Ansatz ist auf langfristige Partnerschaften mit unseren Kunden ausgelegt. Dadurch können wir fortlaufend deren Sicherheitsprofil bewerten und Lösungen vorschlagen, die für verminderte Geschäftsrisiken sorgen, die Einhaltung von Vorschriften sicherstellen und insgesamt die Effizienz ihrer Sicherheitsmassnahmen erhöhen. In Zusammenarbeit mit unseren Kunden, zu denen auch europäische und US-amerikanische Unternehmen der Fortune 500 zählen, kümmern wir uns um hoch komplexe Unternehmensumgebungen mit unserem branchenweit einzigartigen Lösungsportfolio. Dieses umfasst alle Bereiche von Beratung und Technologien bis Managed Security Services und kundenspezifische Innovationen. Für weitere Informationen besuchen Sie uns auf www.kudelskisecurity.com/de

Medienkontakt

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