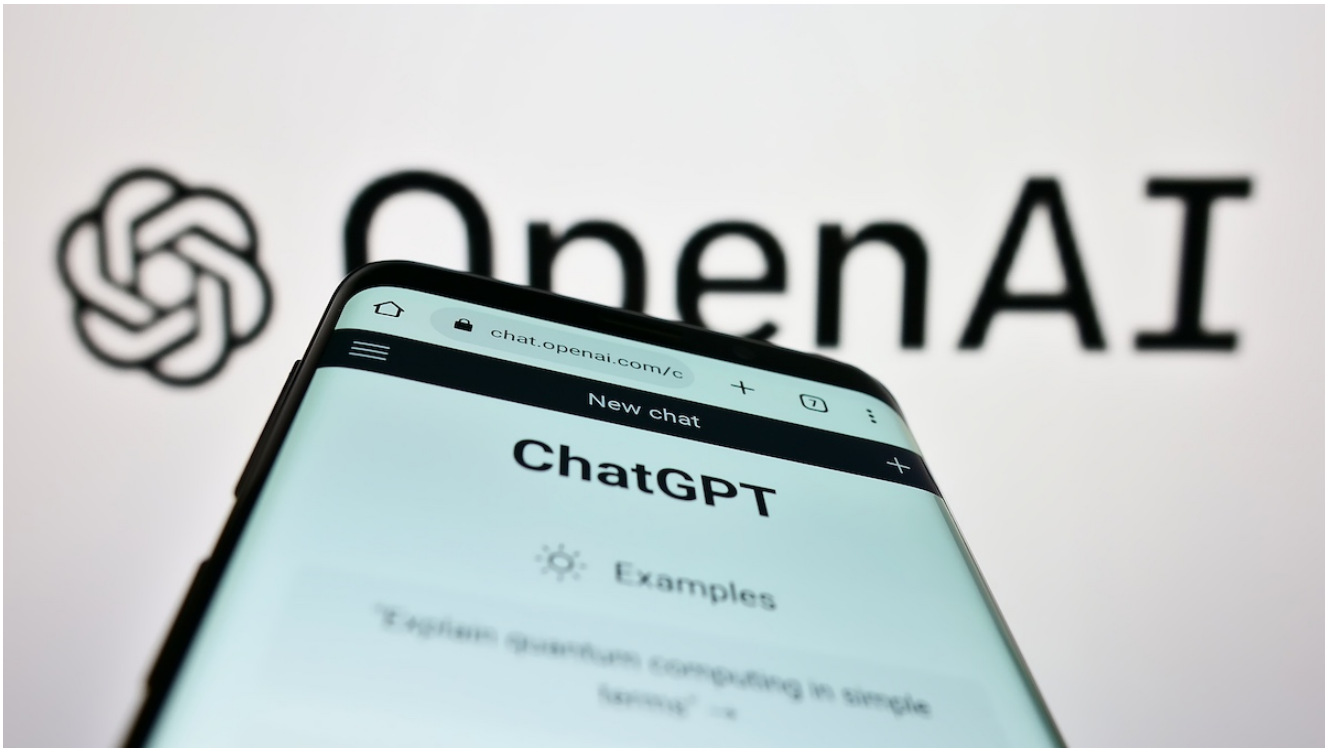
KPMG Tackles AI Security With Cranium Spinout



Consulting giant KPMG on Wednesday announced the spinout of a venture-backed startup building technology to secure AI (artificial intelligence) applications and deployments.

The new startup, called Cranium, emerged from the company's KPMG Studio incubator with an undisclosed minority stake investment from SYN Ventures.

The startup is being run by former Prevalent chief executive Jonathan Dambrot and has ambitious plans to be a big player in a future where AI models – and the data flowing through them – need to be secured.

Cranium says it is building "an end-to-end AI security and trust platform" capable of mapping AI pipelines, validating security, and monitoring for adversarial threats. The company said the technology integrates with existing environments without interrupting the way organizations work to test, train, and deploy AI models.

Cranium is also pitching a playbook that security teams can use alongside the software to protect AI systems and adhere to existing U.S. and EU regulatory standards.

The spinout comes alongside the heady launch of OpenAI's ChatGPT app and a race among software providers big and small to embrace the powerful capabilities of LLM (language learning models) and generative AI.

Software giant Microsoft has debuted an AI-powered security analysis tool to automate incident response and threat hunting tasks, showcasing a security use-case generative AI chatbots.

The new tool, called Microsoft Security Copilot, is powered by OpenAI's newest GPT-4 model and will be trained on data from Redmond's massive trove of telemetry signals from enterprise deployments and Windows endpoints.

Cranium's Dambrot believes the dramatic speed of generative AI adoption will push major regulatory bodies to set guidelines for organizations deploying AI systems and he wants his new company to find revenues in that ecosystem.

"Cranium brings visibility, trust, and a new level of security to cybersecurity and data science teams when it comes to the entire AI ecosystem of any organization," Dambrot said.

Related: Microsoft Puts ChatGPT to Work on Automating Cybersecurity

Related: ChatGPT Data Breach Confirmed; Vulnerable Component Exploted

Related: ChatGPT Integrated Into Security Products as Industry Tests Capabilities

Related: ChatGPT and the Growing Threat of Bring Your Own AI to the SOC

KPMG Tackles AI Security With Cranium Spinout