Tantalum Security Launches Unified Platform to Deliver Continuous AI & Expert-Driven Adversary Simulation Services

Cybersecurity veterans launch unified platform for continuous AI & expert-powered penetration testing, active defense, and ongoing risk remediation guidance

HOUSTON, TX, UNITED STATES, March 17, 2026 /EINPresswire.com/ -- Tantalum Security, a bleeding-edge adversary simulation and active-defense cybersecurity firm, today announced the official launch of its AI-enabled adversary simulation platform, which combines AI-enabled, expert-led continuous penetration testing with ongoing risk remediation guidance. The company's tagline, "Where Elite Cyber Offense Meets Elite Cyber Defense," captures its commitment to improving the security posture of organizations not just through continuous sophisticated adversary simulation and ongoing resilient security posture management, but also through expert engineer-guided risk remediation to quickly improve security posture and incident response maturity.

> "Organizations must not only understand their security posture better on a continuous basis; they also need to quickly remediate the discovered risks across a rapidly growing technology footprint."
>
> *Christian Scott, Founder & CEO, Tantalum Security*

Founded by cybersecurity veterans with decades of experience working with Fortune 1000 companies providing thousands of penetration tests, social engineering campaigns, and cyber assessments, Tantalum Security helps address a growing gap in the market: defending against sophisticated AI-augmented threats, mitigating technology sprawl, and quickly hardening information systems.

The Tantalum Security unified platform brings together every type of penetration test and cyber risk assessment that's AI and expert-driven, with ongoing guidance from real technologists who

have secured thousands of these systems. Additionally, the platform was built from the ground up to support enterprises, providing a plethora of integrations such as JIRA, ServiceNow, Azure DevOps, Tenable, Snowflake, Microsoft 365, Azure, AWS, and many more, including a full REST API and MCP support.

Christian Scott, CEO of Tantalum Security, demostrating real-time deep fake face and voice cloning at GAIM Ops West

Christian Scott, CEO of Tantalum Security, speaking at GAIM Ops West about AI-powered hackers

The Tantalum Security platform was built to be friendly for small and medium-sized businesses as well, providing all of these same capabilities, including enterprise SSO out of the box, at no additional cost, with no features gated.
Tantalum Security's goal is to not just drive down the mean-time to detection (MTTD) of cyber risks but also the mean-time to remediation (MTTR).

"When you support the unified adversary emulation tech stack with white-glove guidance from 100% USA-based A+ technologists, it completely changes the cyber outcomes for customers and drives real results."
— Donna Ciccone, COO, Tantalum Security

Tantalum Security's leadership team brings more than 15 years of open-source contributions, community outreach, and cyber research with its launch. The Tantalum Security team is the creator and maintainer behind Legion, a semi-automated pentesting framework included in Kali Linux. Legion is one of a small handful of pentesting tools in Kali Linux that support MCP for AI-driven penetration testing, reflecting Tantalum Security's commitment to innovation and open-source.

Incorporating these AI-enabled capabilities and more, Tantalum Security allows clients in their pentesting engagements to define adversary profiles, speed, and stealth, letting Tantalum simulate anything from a noisy smash-and-grab to a slow, patient APT campaign. The result is continuous security coverage rather than a one-time snapshot model. Furthermore, Tantalum Security's service portfolio extends well beyond traditional penetration testing. Tantalum Security conducts real-time deepfake social engineering assessments using AI-generated face and voice

cloning, AI red-team testing for LLM and machine learning systems, incident response capability testing, active defense operations, and strategic cyber advisory.

Late last year, at GIAM Ops West 2024, the Tantalum Security team demonstrated the impact of AI-powered adversaries live on stage. On the opening day of the keynote, Tantalum Security demonstrated real-time face and voice cloning that can be used in sophisticated social engineering attacks and lead to account takeover (ATO) attacks. On the closing day, in a keynote, Tantalum Security demonstrated a 100% AI-powered pentesting agent that hacked into a simulated private equity firm's systems and laterally moved in real time.

"Where other cyber firms focus on just selling AI pentesting, which often trains off of customer data, can provide mixed results and suffer quality issues, we thought it would be best to make an open frame that's baked into Kali Linux to give folks a choice. In reality, I think our sweet sauce is bringing the AI, People, and Platform together to achieve much more than just an AI pentest."
— Shane Scott, CTO, Tantalum Security

Tantalum Security continues to expand the capabilities of its cybersecurity platform and ecosystem to protect organizations in an incredibly complex and challenging threat landscape. For organizations looking to learn more about Tantalum Security, they can visit https://tantalum.security.

Donna Ciccone
Tantalum Security
+1 646-647-2064
press@tantalum.security
