# Trojan Horse Security Announces Expanded Cybersecurity Research and Updated Assessment Insights

*Company expands AI-driven security research and testing programs to address rising global threats across critical industries.*

Trojan Horse Security announces expanded AI cybersecurity and penetration testing research capabilities.

WASHINGTON, DC, UNITED STATES, November 28, 2025 / EINPresswire.com/ -- Trojan Horse Security, a Washington-based cybersecurity research and assessment firm, announced updates to its ongoing global research initiatives focused on emerging cyber risks, AI-driven analysis, and modern penetration-testing methodologies. The firm, headquartered near the White House, supports organizations worldwide by studying threat patterns affecting high-risk sectors and releasing findings intended to inform industry professionals, policymakers, and technical teams.

> Understanding emerging cyber threats requires continuous research and field testing, especially as attackers adopt AI-driven techniques."
>
> *Trojan Horse Security Spokesperson*

Trojan Horse Security reports a continued rise in the sophistication of cyber threats targeting enterprise networks, healthcare systems, financial environments, and public-sector infrastructure. In response, the company has expanded several of its research-focused assessment programs to better analyze vulnerabilities influenced by AI, automation, and advanced intrusion techniques.

A spokesperson for Trojan Horse Security said the firm's mission centers on evaluating how modern attack methods are evolving. "Cyber threats continue to shift rapidly, and our research is designed to help organizations understand the emerging risks that influence security planning and preparedness," the spokesperson said.

As part of its public-education efforts, the firm has released updated summaries covering several areas of current cybersecurity study, including:

• AI-assisted security evaluation—research into how machine-learning tools can support threat identification
• Modern penetration-testing methodologies—observations on techniques used to analyze complex digital infrastructure
• Vulnerability and risk-assessment frameworks—findings on common organizational exposure points
• Web-application security considerations—analysis of issues affecting online systems and customer-facing platforms
• Cyber risks in healthcare environments—trends seen within hospitals and clinical-care networks
• Security concerns in financial and digital-asset ecosystems—research on attacks impacting banks, exchanges, and high-volume transactional systems
• Use of drones and robotics in security-testing environments—how unmanned systems are being used in physical-access and infrastructure studies
• Risk considerations for legal, accounting, and professional-services firms—insights into data handling and confidentiality requirements
• Regional observations related to cyber resilience, including island-nation and Caribbean infrastructure considerations

To support broader industry understanding, Trojan Horse Security has also released a set of educational videos discussing topics such as data-center security considerations, critical-infrastructure vulnerabilities, drone-based field assessments, healthcare cyber risks, and trends affecting financial and professional-services organizations.

Trojan Horse Security has previously been referenced in international media, including coverage by the Daily Mail, which provided an external look at cybersecurity operations and the evolving threat landscape.

“Our goal is to contribute research that helps organizations better interpret the challenges shaping today’s digital environment,” the spokesperson added. “Sharing these findings supports industry dialogue and helps strengthen future security planning.”

Additional information and educational resources are available through Trojan Horse Security’s global research and assessment programs.

Bernard Brier
Trojan Horse Security
+1 202-507-5773
contactus@trojanhorsesecurity.com
Visit us on social media: