CrowdStrike Launches AI Red Team Services to Secure AI Systems Against Emerging Threats

November 7, 2024

Organizations can now assess their AI security posture to defend against model tampering, data poisoning and other AI-based threats with CrowdStrike's elite services team

AUSTIN, Texas & AMSTERDAM--(BUSINESS WIRE)--Nov. 7, 2024-- Fal.Con Europe - CrowdStrike (NASDAQ: CRWD) today launched CrowdStrike AI Red Team Services, reinforcing its leadership in protecting the infrastructure, systems and models driving the AI revolution. Leveraging CrowdStrike's word-class threat intelligence and elite-expertise in real-world adversary tactics, these specialized services proactively identify and help mitigate vulnerabilities in AI systems, including Large Language Models (LLMs), so organizations can drive secure AI innovation with confidence.

As organizations adopt AI at a rapid pace, new threats such as model tampering, data poisoning, sensitive data exposure, and more, increasingly target AI applications and their underlying data. The compromise of AI systems, including LLMs, can result in a breach of confidentiality, reduced model effectiveness and increased susceptibility to adversarial manipulation. Announced at Fal.Con Europe, CrowdStrike's inaugural premier user conference in the region, CrowdStrike AI Red Team Services provide organizations with comprehensive security assessments for AI systems, including LLMs and their integrations, to identify vulnerabilities and misconfigurations that could lead to data breaches, unauthorized code execution or application manipulation. Through advanced red team exercises, penetration testing and targeted assessments, combined with Falcon platform innovations like Falcon Cloud Security AI-SPM and Falcon Data Protection, CrowdStrike remains at the forefront of AI security.

Key features of the service include:

- **Proactive AI Defense**: Identifies vulnerabilities in AI systems, in alignment to industry-standard OWASP Top 10 LLM attack techniques, before adversaries can exploit them, enhancing protection against emerging threats.
- **Real-World Adversarial Emulations**: Delivers tailored attack scenarios specific to each AI application, ensuring systems are tested against the most relevant threats.
- **Comprehensive Security Validation**: Provides actionable insights to strengthen the resilience of AI integrations in an evolving threat landscape.

"AI is revolutionizing industries, while also opening new doors for cyberattacks," said Tom Etheridge, chief global services officer, CrowdStrike. "CrowdStrike leads the way in protecting organizations as they embrace emerging technologies and drive innovation. Our new AI Red Team Services identify and help to neutralize potential attack vectors before adversaries can strike, ensuring AI systems remain secure and resilient against sophisticated attacks."

To learn more about CrowdStrike AI Red Team Services, please visit our blog and website.

About CrowdStrike

CrowdStrike (NASDAQ: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/

Follow us: Blog | Twitter | LinkedIn | Facebook | Instagram

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/

View source version on businesswire.com: https://www.businesswire.com/news/home/20241106828590/en/

Jake Schuster
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike