CrowdStrike Launches New Services to Secure AI Systems and Operationalize AI in the SOC

August 6, 2025

AI Systems Security Assessment and AI for SecOps Readiness expand CrowdStrike's industry-leading AI Security Services portfolio, helping organizations reduce risk and stop breaches in the AI era

AUSTIN, Texas & LAS VEGAS--(BUSINESS WIRE)--Aug. 6, 2025-- **Black Hat USA 2025** – CrowdStrike (NASDAQ: CRWD) today announced two new expert-led offerings as part of its expanding AI Security Services portfolio: AI Systems Security Assessment and AI for SecOps Readiness. Expanding on CrowdStrike's AI Red Team Services introduced in 2024, these services help organizations secure the AI systems powering modern business and safely integrate AI into security operations.

As organizations adopt LLMs, copilots, and agentic tools, they face a rapidly expanding attack surface with new risks such as shadow AI, misconfigurations, and autonomous agents acting as non-human identities operating with privileged access. At the same time, adversaries are using AI to automate reconnaissance, generate highly effective phishing content, and bypass traditional defenses. CrowdStrike's new AI Security Services deliver expert-led guidance for operating securely in the AI era, helping organizations both secure AI and use AI to accelerate detection, response, and decision making across the SOC.

"Security teams are under pressure on both sides, to protect rapidly evolving AI systems and to bring AI into the SOC without introducing new risk," said Tom Etheridge, chief global services officer, CrowdStrike. "These services are purpose-built to meet that dual challenge head-on, combining the power of the Falcon platform, threat intelligence, and expert guidance to help organizations reduce risk, improve resilience, and move faster with confidence."

AI Systems Security Assessment

The AI Systems Security Assessment provides organizations with a clear understanding of how AI is being used across their environment, where risk exists, and how to strengthen governance and protections. Built on the foundation of CrowdStrike's AI Red Team Services and Falcon® platform capabilities such as Falcon® Shield, Falcon Cloud Security AI-SPM, and AI Model Scanning, this new service brings technical depth and real-world insight into securing AI systems. Key capabilities include:

- **AI Risk Discovery Powered by Falcon:** Provides real-time visibility into AI usage across SaaS, cloud, and endpoint environments – surfacing shadow AI, misconfigurations, and hidden exposure, including autonomous agents with privileged access, through Falcon-native telemetry.
- **Threat-informed AI Testing:** Assesses model and system risk using internal benchmarking tools that emulate real-world adversary tactics.
- **Actionable AI Governance and Architecture Guidance:** Delivers strategic recommendations to improve governance and secure the architecture for LLMs and agent-based systems – reducing risk and complexity across AI deployments.

AI for SecOps Readiness

The AI for SecOps Readiness service helps security teams safely and effectively use AI to operate at machine speed across detection, investigation, and response workflows. As adversaries accelerate with AI, defenders must modernize their operations to keep pace. This service helps organizations assess AI readiness, prioritize use cases, and develop a secure path to AI adoption. Key capabilities include:

- **SOC Readiness Assessment:** Evaluates staffing, tooling, workflows, and governance to assess AI readiness across detection, investigation, and response.
- **Use Case Identification and Design:** Pinpoints high-impact opportunities to apply AI – from alert triage to investigation – tailored to organizational maturity and operating environment.
- **Strategic Guidance and Architecture Planning:** Includes reference architectures, integration strategies, and "build vs. buy" recommendations to support responsible, scalable AI adoption.
- **Actionable Roadmap for AI in the SOC:** Delivers a prioritized integration plan for both Falcon-native and third-party AI tools – with clear guidance to reduce risk, streamline adoption, and drive operational outcomes.

To learn more about how CrowdStrike helps organizations secure AI systems and transform security operations, read our blog, visit us online, or stop by the CrowdStrike Black Hat booth #2733.

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 | X | 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/20250805964896/en/

Media Contact
Jake Schuster
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike