CrowdStrike Unveils Agentic Adversary Emulation on the Falcon Platform to Identify and Close Exploitable Attack Paths

November 4, 2026

Powered by CrowdStrike SafeMind, offensive AI emulates how real adversaries chain vulnerabilities and weaknesses to reach critical assets, drives prioritized remediation, and validates attack paths are closed

AUSTIN, Texas & BARCELONA, Spain--(BUSINESS WIRE)--Nov. 4, 2026-- **Fal.Con Europe 2026 --** CrowdStrike (NASDAQ: CRWD) today unveiled Agentic Adversary Emulation, powered by SafeMind, the company's family of purpose-built security models and harnesses. The new offering red teams a customer's environment like an agentic adversary, chaining vulnerabilities and weaknesses into exploitable paths to an organization's critical assets. CrowdStrike then drives prioritized remediations and re-runs the attack to validate each path is closed.

"The agentic adversary uses AI to operate at a speed and scale no human can match. These are preventable gaps that go unprevented," said Adam Meyers, head of counter adversary operations at CrowdStrike. "Now defenders can find and close them before the adversary does. That is offense in the service of defense."

The Adversary is Now Agentic

Adversaries weaponize agents to discover, chain, and exploit vulnerabilities at machine speed. CrowdStrike's 2026 Agentic AI Campaign report documented an agent chaining a single vulnerability into cluster-admin access and exfiltrating 726 databases, with no human at the keyboard. Point-in-time pen tests and periodic assessments cannot keep pace. Defenders need purpose-built frontier AI to find and close exploitable paths before adversaries can take them, then prove the fix worked.

Autonomous Offensive Security Powered by SafeMind

SafeMind is trained on Falcon sensor telemetry, expert-labeled threat intelligence, and frontline experience from CrowdStrike's analysts and incident responders tracking adversaries and stopping breaches. Combined with each customer's Falcon environmental context, Agentic Adversary Emulation automates offensive security from attack to remediation to validation:

- **Purpose-Built Offensive AI:** Red Tempest, SafeMind's offensive model, operates like an autonomous attacker. Its harness orchestrates thousands of steps to chain weaknesses, adapt around defenses, and pursue objectives in controlled, customer-approved testing environments.
- **Adversary-Informed Emulation:** CrowdStrike intelligence on more than 290 tracked adversaries, emerging agentic threats, and newly disclosed vulnerabilities grounds offensive testing in how real-world adversaries operate.
- **Falcon Environmental Context and Prioritization:** Combines vulnerabilities, misconfigurations, and identity gaps into exploitable paths to critical assets, pinpointing where a single control can break the attack chain.
- **Closed-Loop Remediation and Validation:** CrowdStrike generates compensating controls to close attack paths, from patches and configuration fixes to new detections. Red Tempest re-runs the attack to validate the fix.

Attack, Harden, Validate on One Platform

CrowdStrike is advancing autonomous offensive security beyond finding exploitable weaknesses to continuously strengthening the defenses that stop them. Finding an attack path is not the same as closing it, and an offensive tool cannot defend the environment it just tested. CrowdStrike unifies purpose-built offensive and defensive AI, real-world adversary intelligence, and Falcon environmental context on one platform, from sensor to harness to model.

Agentic Adversary Emulation is available in early access for select customers through Project QuiltWorks partners. To learn more, visit here.

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 | Instagram
Start a free trial today: https://www.crowdstrike.com/trial

© 2026 CrowdStrike, Inc. All rights reserved. CrowdStrike and CrowdStrike Falcon are marks owned by CrowdStrike, Inc. and are registered in the United States and other countries. CrowdStrike owns other trademarks and service marks and may use the brands of third parties to identify their products and services.

Forward-Looking Statements

This release includes discussion of unreleased services or features. Any unreleased services or features referenced here are still in development and subject to change. Customers should make their purchase decisions based upon features that are currently available.

View source version on businesswire.com: https://www.businesswire.com/news/home/20261104932077/en/

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

Source: CrowdStrike