CROWDSTRIKE
Investor Relations

CrowdStrike Extends the Agentic SOC to Detect and Stop the Agent Insider Threat

November 4, 2026

New Agent Insider Threat Detection recognizes abnormal agent behavior even when no rule is broken; coordinated multi-agent investigations now generally available

AUSTIN, Texas & BARCELONA, Spain--(BUSINESS WIRE)--Nov. 4, 2026-- **Fal.Con Europe 2026** -- CrowdStrike (NASDAQ: CRWD) today introduced agentic SOC innovations to detect the new insider threat: enterprise AI agents that act faster than any human can respond. Agent Insider Threat Detection exposes abnormal agent behavior and routes deviations into coordinated, multi-agent investigations that run across every domain at the same time. The verdict lands in seconds, and the new Falcon Guardian AI Kill Switch terminates the agent immediately.

“AI agents can be both an insider threat and an adversary,” said Michael Sentonas, president of CrowdStrike. “One acts without authorization from inside your walls. The other is weaponized against you from outside. Stopping the insider means knowing the moment an agent turns, investigating across every domain, and shutting it down at machine speed. That's the next evolution of the agentic SOC.”

The Threat on Your Payroll

Organizations are deploying thousands of AI agents, each with system-level access to sensitive data and the autonomy to act on it. You pay this insider in tokens. Every day, we see agents take actions they were never authorized to take. The hardest case is the agent that is manipulated or drifts from its intended behavior and never breaks a rule. Policy and log-based tools miss it because there is no violation to catch, and they can’t tell a rogue agent from the person running it.

Agent Insider Threat Detection in Falcon Next-Gen SIEM learns the normal behavior of every AI agent and the person who runs it and flags deviations even when no policy is violated. The detection routes directly into coordinated investigations where expert-trained agents work simultaneously across endpoint, identity, SaaS, cloud, and network. Shared context across every domain and agents trained on years of stopping breaches separate real threats from noise, turning a deviation into a verdict defenders can trust at machine speed. Unveiled at Fal.Con U.S. in September 2026, coordinated multi-agent investigations are now generally available, with new innovations coming soon.

Available Today

- **Coordinated Multi-Agent Investigations:** Expert-trained agents investigate every domain simultaneously on shared context, weighing evidence the way elite analysts do and converging on a trusted verdict with visible reasoning and justification to back it up.
- **Single-Governed Automation Workspace:** Charlotte Agentic SOAR brings agents, workflows, and custom applications into one workspace. Teams set the autonomy level for each, from human approval to fully autonomous execution.
- **Human-in-the-Loop Gates:** When an agent invokes a sensitive tool, it pauses and raises an Action Request. Analysts approve, reject with a documented reason, or inspect the full agent trace.
- **Agent Interruption:** Analysts pause or stop a Charlotte AI or AgentWorks running agent mid-task to prevent unauthorized action and runaway spend.

Introducing Agent Insider Threat Detection and New Innovations

- **Agent Insider Threat Detection (Q4):** Learns the normal behavior of every AI agent and its owner, flags deviations even when no policy is violated, and feeds that risk into the same score Falcon Next-Gen SIEM builds for the owner and host. Abnormal behavior routes straight into a coordinated investigation.
- **AI Ecosystem Detections (Q4):** Detect attacks across the AI estate, including LLM API abuse, stolen API keys, and the compromise of coding assistants, MCP servers, and agent frameworks.
- **Expanded Triage Coverage (Q4):** Triage agents extend to Falcon Guardian, Cloud, Shield (SaaS), Data Security, and custom detections. The same agentic analysis applied to adversary threats now applies to compromised and misaligned AI agents.
- **Agent and Workflow Approvals (Q4):** Approval gates extend beyond individual tool calls to entire agents, apps, and workflows.
- **Policy-Drift Agent Guardrails (FY28, Q1):** Falcon Guardian screens every Charlotte AI and AgentWorks interaction for policy drift, unauthorized tool calls, and out-of-bounds data access, catching the moment an agent steps outside its intended scope.
- **AI Credit Visibility and Control (Q4):** Admins see the credits every SOC agent and workflow consumes in real time, halt consumption mid-run, and raise or deny limits when an agent hits its cap.
- **Federated Search Expansion:** New connectors let teams search agent data across GovCloud, Dynatrace, Databricks, and Snowflake (GA); Splunk, Elastic, and Cribl Lake (Q4), with no re-ingestion.

The Next Evolution of the Agentic SOC

The agent is the insider threat, the adversary, and the defender. The agentic SOC detects it, investigates it, and stops it at machine speed.

To learn more about Agent Insider Threat Detection and CrowdStrike's agentic SOC innovations, 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/20261104432041/en/

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

Source: CrowdStrike