CROWDSTRIKE
Investor Relations

CrowdStrike Delivers Industry-First Managed Threat Hunting Across Third-Party Data

April 28, 2025

Falcon Adversary OverWatch now hunts across third-party data in Falcon Next-Gen SIEM, extending expert-driven detection across every attack surface to stop stealthy adversaries

AUSTIN, Texas & SAN FRANCISCO--(BUSINESS WIRE)--Apr. 28, 2025-- RSA 2025 - CrowdStrike (NASDAQ: CRWD) today introduced Falcon® Adversary OverWatch Next-Gen SIEM, the first and only solution to bring managed threat hunting to third-party data. This breakthrough innovation extends the visibility of CrowdStrike's elite threat hunters into unmanaged attack surfaces adversaries have long exploited. By leveraging third-party data ingested by Falcon® Next-Gen SIEM, CrowdStrike delivers 24/7 expert detection beyond endpoints, identity and cloud environments to stop breaches across every attack surface.

Adversaries strike from all angles, and once inside, they move laterally with alarming speed. Groups like FAMOUS CHOLLIMA embed malicious insiders to operate from within. Others, like OPERATOR PANDA exploit unmanaged infrastructure, edge devices and siloed systems like firewalls, VPNs and email gateways – where traditional tools lack visibility. By extending managed threat hunting to third-party data, CrowdStrike delivers faster detection, broader coverage and even greater speed in stopping breaches.

"Today's adversaries move incredibly fast and thrive on the complexity of modern environments. They exploit the sprawl of IT and security tools to give them an edge, while defenders are left to stitch together disjointed data to try and find signals in the noise," said Adam Meyers, head of counter adversary operations at CrowdStrike. "With OverWatch now hunting across third-party data, we're eliminating the blind spots that adversaries rely on, delivering unified visibility, expert-led detection and the early insight needed to stop breaches."

Transform the SOC with Falcon Adversary OverWatch and Next-Gen SIEM

CrowdStrike's latest innovations set a new standard for modern security operations. Powered by the AI-native CrowdStrike Falcon® cybersecurity platform, Falcon Adversary OverWatch uses deep adversary expertise and industry-leading threat intelligence to rapidly uncover evasive threats. Falcon Next-Gen SIEM unifies native and third-party data, real-time intelligence and AI-driven automation to deliver comprehensive visibility, high-fidelity alerts and machine speed response. New innovations include:

- **Expert-Led Threat Hunting Across all Attack Surfaces:** Integrates real-time, 24/7 threat hunting from Falcon Adversary OverWatch with first-party endpoint, identity, cloud and third-party data from Falcon Next-Gen SIEM. Expands coverage across unmanaged infrastructure that adversaries often exploit to expose hidden threats.
- **UEBA and Case Management for Falcon Next-Gen SIEM:** Analyzes user behavior with advanced machine learning to uncover insider threats and stealthy adversaries once they're on the network. With AI-driven risk scoring, entity resolution and automated workflows, security teams can reduce false positives, connect related activities across data sources and investigate in a centralized platform to respond faster.
- **Unified Identity Security and Next-Gen SIEM:** The powerful combination of Falcon® Identity Protection and Falcon Next-Gen SIEM enables security teams to detect and prioritize identity-based threats in real time, while Falcon Fusion SOAR automates Active Directory actions – like disabling compromised accounts and MFA enforcement – to respond at machine speed.
- **CrowdStrike Pulse Services:** To help customers drive SOC transformation, CrowdStrike Pulse Services reduces active risk with targeted offerings such as ransomware readiness planning, high-value asset protection strategies and cyber resiliency uplift. Delivered through modular, expert-led engagements, Pulse helps teams improve response times and build more resilient operations.

To learn more about CrowdStrike's latest SOC innovations:

- Visit booth N-6144 at RSA
- Read our blog
- Register for the virtual event, SOC in Fast-Forward: Powered by AI. Driven by Experts.

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/20250428827888/en/

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

Source: CrowdStrike