CROWDSTRIKE
Investor Relations

CrowdStrike Signal Delivers the Next Evolution of AI-Powered Threat Detection

August 6, 2025

Now GA, new self-learning detection engines surface threats undetectable for others – connecting subtle activity into prioritized leads to accelerate investigation, hunting, and response

AUSTIN, Texas--(BUSINESS WIRE)--Aug. 6, 2025-- Black Hat USA 2025, Las Vegas -- CrowdStrike (NASDAQ: CRWD) today announced the general availability of CrowdStrike Signal, a new class of AI-powered detection engines that surface the undetectable threats others miss – before they escalate. Signal uses self-learning models for every host to understand what's normal in that environment across time, systems, and users. It pinpoints subtle, early-stage threat activity and connects related behaviors – before traditional tools act. By identifying weak signals that deviate from the norm and building high-confidence, prioritized leads, Signal accelerates the Falcon® platform's AI advantage and empowers security teams to investigate, hunt, and stop threats earlier in the kill chain.

Modern attacks often begin with low-signal activity that appears benign in isolation. Traditional rule-based systems ignore these behaviors because they lack the context to tell what's suspicious and what's just noise. Even newer AI approaches apply scoring only after a detection has occurred.

Signal learns what's normal across the environment and continuously updates its understanding of standard activity as conditions change – identifying what deviates and linking early-stage behaviors with downstream activity. By analyzing behavior earlier in the threat lifecycle and correlating subtle activity across time, CrowdStrike turns fragmented signals into a small number of prioritized, AI-generated leads that expose threats buried in the noise and jumpstart response. Born on the endpoint, Signal lays the foundation for next-generation detection across identity, cloud, and third-party data.

"CrowdStrike pioneered AI-native cybersecurity, and continues to deliver the innovation driving the industry forward. Signal is our latest breakthrough, built to detect how modern adversaries actually operate," said Elia Zaitsev, chief technology officer, CrowdStrike. "Today's attackers spread subtle signals over time to stay under the radar. Signal is designed to catch what others overlook, connecting the dots across systems and time to paint the full picture."

Signal Through the Noise
Behind Signal is a new family of statistical time series models that analyze billions of daily events within each customer's environment. By linking signals across time and systems, Signal filters out repetitive activity and surfaces what's truly unusual. This correlation builds high-confidence patterns that reveal stealthy attacker behavior before others can, giving defenders a clear starting point to act.

- **Self-learning AI to Understand the Customer Environment:** Signal continuously models behavior for each user, host, and process, adapting over time to surface meaningful deviations. Unlike static rules or pre-trained models, it delivers early-stage detection without manual configuration or constant adjustment.
- **Real-time Detection of Stealthy Tradecraft Others Miss:** Signal links subtle behaviors often used by attackers – but also commonly seen on benign hosts – such as the use of living-off-the-land tools for reconnaissance or applications running from temporary directories. This low-signal activity may appear benign in isolation, but analyzed earlier, over time and context, it reveals attacker activity that would otherwise go unnoticed.
- **High-confidence Leads Reduce Alert Volume, Accelerate Response:** Signal condenses a vast number of behaviors and detections into a small set of high-fidelity leads. It surfaces early indicators of compromise, reduces false positives, and groups related activity into a single starting point to eliminate manual triage and speed investigation, hunting, and response.

CrowdStrike Signal is now generally available. To learn more, read our blog 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/20250805619969/en/

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

Source: CrowdStrike