CrowdStrike Introduces Industry's First AI-Powered Indicators of Attack for CrowdStrike Falcon Platform to Uncover the Most Advanced Attacks

Trained on the world's richest threat intelligence, new detection and response capabilities proactively protect organizations against emerging adversary techniques

AUSTIN, Texas & LAS VEGAS--(BUSINESS WIRE)--Aug. 10, 2022-- CrowdStrike (Nasdaq: CRWD), a leader in cloud-delivered protection of endpoints, cloud workloads, identity and data, today introduced the industry's first AI-powered Indicators of Attack (IoAs), new innovations for fileless attack prevention at scale and enhanced visibility for stealthy cloud intrusions. Delivered on the CrowdStrike Falcon platform and powered by the CrowdStrike Security Cloud, these new detection and response capabilities stop emerging attack techniques and enable organizations to optimize the threat detection and response lifecycle with speed, scale and accuracy.

More than a decade ago, CrowdStrike invented IoAs, which brought a fundamentally new approach to stopping breaches based on real adversary behavior, irrespective of the malware or exploit used in an attack. CrowdStrike has also pushed the boundaries of applying AI in cybersecurity to identify and stop the most advanced, emerging attacks. Now, CrowdStrike is leveraging powerful AI techniques to create new IoAs at machine speed and scale.

"CrowdStrike leads the way in stopping the most sophisticated attacks with our industry-leading Indicators of Attack capability, which revolutionized how security teams prevent threats based on adversary behavior, not easily changed indicators," said Amol Kulkarni, chief product and engineering officer at CrowdStrike. "Now, we are changing the game again with the addition of AI-powered Indicators of Attack, which enable organizations to harness the power of the CrowdStrike Security Cloud to examine adversary behavior at machine speed and scale to stop breaches in the most effective way possible."

The Falcon platform's new capabilities include:

Industry's first AI-powered IoAs

Organizations today are under pressure to defend expanding attack surfaces against emerging threats and adversary tradecraft. With the Falcon platform, organizations can:

- **Detect new classes of attacks, faster than ever:** Find emerging attack techniques with new IoAs created by continuously learning AI models trained on real-world adversary behavior and the world's richest threat intelligence.
- **Drive automated prevention with high-fidelity detections:** Shutdown attacks based on a chain of behaviors, irrespective of the specific malware or tools used, with cloud-native AI models constantly delivered to the Falcon agent with newly-found IoAs.
- **Activate IoAs at cloud scale, trained on human-led expertise:** Synthesize insights with AI-powered IoAs from CrowdStrike's world-renowned threat hunting team to minimize false positives, maximize analyst productivity and deploy threat hunting at scale.

Of note, AI-powered IoAs have identified over 20 never-before-seen adversary patterns, which have been validated by experts and enforced on the Falcon platform for automated detection and prevention.

New innovations for fileless attack prevention at scale

According to the 2022 CrowdStrike Global Threat Report, 62% of all attacks are malware-free. These fileless attacks can be carried out entirely in memory, creating a blindspot for threat actors to exploit. With the Falcon platform, organizations can:

- **Prevent the most advanced fileless attacks:** Stop advanced persistent threats (APT) and prevalent tools, like Cobalt Strike, with advanced memory scanning techniques that augment best-of-breed AI/ML and IoA detections with lightning fast scanning of all memory at unprecedented scale.
- **Leave bloated memory scanning behind:** Shed the heavy resource constraints of legacy approaches that made memory scanning a non-starter with high-performance memory scanning techniques, optimized for Intel CPU/GPUs.
- **Initiate memory scans on behavior, not a fixed schedule:** Automate scans with behavior-based triggers to find and stop fileless attack patterns in real time, not after a potential breach.

Enhanced visibility for stealthy cloud intrusions

As Linux environments, data and applications have moved to the cloud, adversaries have also moved to the cloud to open backdoors, steal sensitive data and conceal their movement. With the Falcon platform, organizations can:

- **Hunt stealthy rootkits and reduce dwell time:** Identify malicious activity early in the kill chain with deep Linux kernel visibility to fuel threat hunting and investigation of hidden, emerging Linux attacks.
- **Bolster managed cloud threat hunting**: Disrupt the most sophisticated threats in cloud environments with new kernel

telemetry events for Falcon OverWatch experts, building on CrowdStrike's recently announced Falcon OverWatch Cloud Threat Hunting service.

"Using CrowdStrike sets Cundall apart as one of the more advanced organizations in an industry that typically lags behind other sectors in IT and cybersecurity adoption," said Lou Lwin, CIO at Cundall. "Today, attacks are becoming more sophisticated and if they are machine-based attacks, there is no way an operator can keep up. The threat landscape is ever-changing. So, you need machine-based defenses and a partner that understands security is not 'one and done.' It is evolving all the time."

According to Forrester[1], "No security tool can detect every attack. Cybersecurity pits adversaries against defenders. Defensive technologies rely on rules, heuristics, and outliers to find evil. Those technologies lack one essential component that threat hunting introduces: the creativity of the practitioners defending enterprise environments."

These capabilities are generally available for Falcon Prevent (NGAV) and Falcon Insight (EDR) customers.

Additional Resources

- For more information on the new capabilities for the CrowdStrike Falcon platform, please visit our blog.
- For more information on the CrowdStrike Falcon platform, please visit our website.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms 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 | Twitter | LinkedIn | Facebook | Instagram
Start a free trial today: https://www.crowdstrike.com/free-trial-guide/

---

[1]Threat Hunting 101: Providing A Meaningful Definition For Threat Hunting, Forrester Research, Inc., July 15, 2022

View source version on businesswire.com: https://www.businesswire.com/news/home/20220810005192/en/

Kevin Benacci
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike