CROWDSTRIKE
Investor Relations

CrowdStrike Sets Record for Fastest Threat Detection in MITRE Engenuity's ATT&CK® Evaluations: Managed Services-Round 2

June 18, 2024

CrowdStrike detects advanced adversary attack in real-world, closed-book simulation in just four minutes, six to 11 times faster than competitive vendors; scores highest in detection coverage at 98%

AUSTIN, Texas--(BUSINESS WIRE)--Jun. 18, 2024-- CrowdStrike (NASDAQ: CRWD) set a new speed benchmark for cybersecurity threat detection, identifying and alerting on a sophisticated eCrime adversary attack in just four minutes during the closed-book MITRE Engenuity's ATT&CK® Evaluations: Managed Services-Round 2. CrowdStrike Falcon® Complete MDR operates at the speed of the adversary, detecting the security incident six to 11 times faster than competitive vendors, while scoring the highest in detection coverage at 98 percent.

MITRE's closed book evaluation emulated a real-world eCrime attack without giving the vendors prior knowledge of the threat scenario – creating the most accurate assessment of a vendor's capabilities. In this scenario, prevention capabilities of the Falcon agent were not permitted and the Falcon platform was operating in detect-only mode, meaning no automated actions could be taken to kill processes. In this rigorous setting, CrowdStrike reported 42 out of the 43 (98%) adversary techniques. MITRE recorded CrowdStrike's mean-time-to-detect (MTTD) – the average time between when a specific attack activity was performed and an email alert regarding that activity was received – at a record-breaking four minutes, setting a new benchmark for speed in threat detection.

"Stopping breaches requires security teams to operate at the speed of the adversary. The Falcon platform's unique cloud-born, AI-native architecture with one intelligent sensor delivers the best analyst experience and the fastest, most effective cybersecurity outcomes in the industry," said Michael Sentonas, President of CrowdStrike. "Multiple platforms and stitched-together solutions are hard to use, create operational complexity, and slow security teams down when speed matters most. This is evident in testing scenarios and even more so in real-world environments. The powerful combination of CrowdStrike's elite team of experts, the Falcon platform, and our knowledge of the adversary is unmatched in delivering the speed and efficacy needed to stop breaches."

Additional Resources

- To learn more about how CrowdStrike achieved 98% coverage scores and set the benchmark in threat detection time, read our blog.
- For full results and more information about the evaluations, visit here.
- To register for the CrowdStrike CrowdCast on the MITRE ATT&CK® Evaluation: Managed Services on June 27, 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 | Twitter | 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/20240617088058/en/

Jake Schuster
CrowdStrike Corporate Communications

press@crowdstrike.com

Source: CrowdStrike