CrowdStrike Achieves 100% Protection, 100% Visibility, and 100% Detection in MITRE Engenuity ATT&CK® Evaluations Enterprise Round 5

CrowdStrike's AI-powered Falcon Platform stopped 13 of 13 protection scenarios spanning every stage of an attack, without relying on prior knowledge or legacy signatures

AUSTIN, Texas--(BUSINESS WIRE)--Sep. 20, 2023-- CrowdStrike (Nasdaq: CRWD), announced its results in Round 5 of the MITRE Engenuity ATT&CK® Evaluations Enterprise. In this latest round, the CrowdStrike Falcon® Platform achieved 100% coverage scores across protection, visibility, and analytic detections, an industry-first, never achieved on any previous MITRE Engenuity ATT&CK Enterprise evaluation.

As the leader in AI-powered cybersecurity, the CrowdStrike Falcon platform stopped 13 of 13 protection scenarios spanning every stage of an attack, without relying on prior knowledge or legacy signatures. The evaluation demonstrated the power of a modern, AI-powered platform, rigorously testing CrowdStrike's pioneering EDR, XDR, identity protection, and threat intelligence capabilities, all delivered through a single, powerful agent that consolidates point products to stop breaches.

In this latest round of evaluations, the MITRE Engenuity ATT&CK team chose to emulate the tactics, techniques and procedures (TTPs) of Turla, which CrowdStrike classifies as VENOMOUS BEAR, a sophisticated Russia-based adversary assessed to be attributable to the Federal Security Service (FSB) of the Russian Federation and known for its targeted intrusions, innovative stealth and its adaptability and willingness to evolve behaviors and tools to achieve campaign objectives.

As the pioneer of cloud-native Endpoint Detection and Response, the CrowdStrike Falcon platform empowers customers to stop breaches. MITRE Engenuity's ATT&CK® Evaluation: Enterprise further validates CrowdStrike's market leadership and superior customer outcomes with 100% visibility and 100% analytic detection coverage across all 19 steps and 143 tested substeps of VENOMOUS BEAR's tactics and techniques, validating the platform's superior efficacy and deep context for faster, better security outcomes.

"CrowdStrike is the foundational cybersecurity platform for the modern AI and cloud powered world. Hitting the 100% coverage hat trick across protection, visibility, and detection in MITRE Engenuity's evaluation validates the superior security outcomes we deliver across every stage of an attack," said Michael Sentonas, President of CrowdStrike. "We're proud to break new ground in this evaluation, achieving a "perfect three" across MITRE Engenuity's coverage categories, and demonstrating our platform's AI-powered protection and industry-leading visibility and detection to stop breaches faster, with absolute accuracy, and far less time and effort."

NOTE: The views and opinions expressed in this release are those of CrowdStrike and do not necessarily reflect the views or positions of any entities they represent.

Additional Resources

- To learn more about how CrowdStrike achieved 100% coverage scores across protection, visibility, and analytic detections, read our blog.
- For full results and more information about the evaluations, visit the MITRE Engenuity website.
- Join our upcoming CrowdCast: MITRE ATT&CK Enterprise Evaluation: Inside the Round 5 Results

About MITRE Engenuity

MITRE Engenuity, a subsidiary of MITRE, is a tech foundation for public good. MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE Engenuity brings MITRE's deep technical know-how and systems thinking to the private sector to solve complex challenges that the government alone cannot solve. MITRE Engenuity catalyzes the collective R&D strength of the broader U.S. federal government, academia, and private sector to tackle.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with 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/

View source version on businesswire.com: https://www.businesswire.com/news/home/20230920640419/en/

Kevin Benacci
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike