Palo Alto Networks Achieves 100% Prevention and 100% Detection in the MITRE Engenuity ATT&CK Enterprise Evaluations (Round 4)

March 31, 2022

Cortex XDR blocked all stages in the protection evaluation and detected all 19 steps in both attack scenarios

SANTA CLARA, Calif., March 31, 2022 /PRNewswire/ -- Palo Alto Networks (NASDAQ: PANW), a leader in endpoint security, today announced it has successfully completed the MITRE Engenuity ATT&CK® Round 4 Evaluation — achieving 100% Prevention and 100% Detection of attacksCortex XDR® was evaluated for its ability to protect and detect simulations of the Wizard Spider and Sandworm threat groups real-world attacks.

Detecting and mitigating real-world threats is the ultimate validation of a security solution. According to MITRE, Wizard Spider is a financially motivated Russia-based threat group that has been conducting ransomware campaigns against a variety of organizations, ranging from major corporations to hospitals. MITRE describes Sandworm as a Russian threat group known for carrying out notable attacks such as the 2015 and 2016 targeting of Ukrainian electrical companies and 2017's NotPetya attacks.

Cortex XDR received outstanding results in all measures, including:

- 100% prevention against all attacks in the protection phase of the evaluation.
- 100% detection of all 19 attack steps.
- Over 98% of attack substeps were identified with "technique level analytics detections."
- Over 98% visibility of all adversarial activity across both attack scenarios.

These outstanding results are founded on Cortex XDR's industry-leading endpoint telemetry collection that fuels our behavioral threat protection and cloud based analytics. All (100%) of the detections Cortex XDR delivered were classified as technique-level detections, the highest value detections available in the evaluation. Cortex XDR automates the investigation process, delivering complete attack stories that are able to clearly reveal the how, what and why of an attack and give the analyst the critical insight they need for rapid and complete remediation.

"Cortex XDR is a leading solution for the industry, and we're thrilled to have achieved such landmark results again in this year's MITRE evaluation," said Gonen Fink, senior vice president, Cortex products at Palo Alto Networks. "MITRE Engenuity results are the best measure of security product effectiveness for today's threats and an important vendor evaluation criteria for customers. Our performance is a testament to the continuing innovation we bring to Cortex XDR and proof of our ability to provide customers with outstanding protection. We value the threat-informed approach MITRE takes that helps drive the industry forward, making it a safer, more secure world."

"This latest round indicates significant product growth from our vendor participants. We are seeing greater emphasis in threat informed defense capabilities, which in turn has developed the infosec community's emphasis on prioritizing the ATT&CK Framework," said Ashwin Radhakrishnan, acting general manager of ATT&CK Evaluations at MITRE Engenuity.

For more information, please read our "2022 MITRE Engenuity ATT&CK Evaluations Results" blog and view the results here.

About MITRE Engenuity

MITRE Engenuity, a subsidiary of MITRE, is a tech foundation for the 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 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 national and global challenges, such as protecting critical infrastructure, creating a resilient semiconductor ecosystem, building a genomics center for public good, accelerating use case innovation in 5G, and democratizing threat-informed cyber defense.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

View original content to download multimedia:https://www.prnewswire.com/news-releases/palo-alto-networks-achieves-100-prevention-and-100-detection-in-the-mitre-engenuity-attck-enterprise-evaluations-round-4-301515285.html

SOURCE Palo Alto Networks, Inc.