MITRE ENGENUITY | paloalto NETWORKS | CORTEX XDR

The data doesn't lie.

Only Cortex XDR® delivers 100% Protection and 100% Detection in the MITRE Engenuity ATT&CK® Evaluations.

- No configuration changes
- No delayed detections
- No bias

MITRE ENGENUITY RESULTS | READ THE E-BOOK

Trying to prevent cyberattacks? Think like a cyberattacker.

MITRE Engenuity Enterprise ATT&CK Evaluations, held annually, mirror real-world threat tactics, techniques, and procedures of active and dangerous global threat groups. The result is a series of unbiased and transparent insights — crucial for CISOs and security professionals as they evaluate endpoint solutions in the ever-evolving threat.

3 outcomes identified in the MITRE Engenuity Evaluation

VISIBILITY
The completeness of a solution's ability to observe potentially malicious actions

DETECTION
The actions a solution can accurately identify as malicious

PROTECTION
The malicious actions a solution can prevent once identified

Turla vs. Cortex XDR

Obliterating threat groups right out of the box.

As one of the most sophisticated nation-state threat actors, Turla is a well-funded threat group that is part of the Russian FSB. They have infected victims in over 45 countries, targeting government agencies, military groups, and diplomatic missions as well as research and media organizations.

MITRE Engenuity emulated the tactics, techniques, and procedures (TTPs) and tools commonly used by the Turla threat group. Palo Alto Networks used only the Cortex XDR Pro Endpoint agent on Windows and Linux.

THREAT GROUP
Turla, also known as: G0010, Pensive Ursa, IRON HUNTER, Group 88, Belugasturgeon, Waterbug, WhiteBear, Snake, Krypton, Venomous Bear.

ORIGIN
Russia

EXPLOITS / TACTICS
Covert exfiltration and deception tactics include water holing of government websites, custom rootkits, and stealth command-and-control network infrastructure.

TARGETS
Infected victims in over 45 countries across government agencies, military groups, diplomatic missions, education and research institutions, pharmaceutical companies, and media organizations.

We don't take 100% lightly.

ONLY Cortex XDR from Palo Alto Networks achieved:

100% Visibility
With the **highest quality detections evaluated** (142 of 143 detections as Technique-level detections)

+

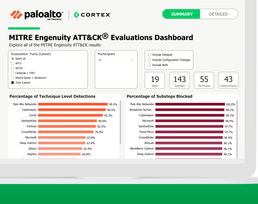
100% Protection
With all **129 substeps blocked** in the evaluation during the earliest stage

+

100% Detection
With **zero configuration changes** and **zero delayed detections**

While other vendor solutions tout 100% success in this year's evaluation, each falls short on at least one Detection or Prevention in critical stages. Only Cortex XDR from Palo Alto Networks provided 100% Protection and 100% Detection for every one of the individual malicious substeps that were taken.

MITRE ENGENUITY RESULTS



Want a deeper look at the results? Take a drive through the data:

- Explore an interactive view of the results without vendor spin.
- View and compare results across all vendors from this year and past years of the evaluations.
- Include or remove detections resulting from configuration changes or delayed detections.

EXPLORE THE DATA

Cortex XDR delivers the industry's most effective endpoint security by analyzing data from any source to stop sophisticated attacks.

Eliminate blind spots with total visibility across your environment.

Simplify security operations to cut mean time to respond (MTTR).

Harness the scale of the cloud for advanced AI, ML, and analytics.

Lower costs by consolidating tools and improving SOC efficiency.

Proven endpoint protection
Block advanced malware, exploits, and fileless attacks with the industry's most comprehensive endpoint security stack. Our lightweight agent stops threats with Behavioral Threat Protection, AI, and cloud-based analysis.

Laser-accurate detection
Pinpoint evasive threats with patented behavioral analytics. Cortex XDR uses machine learning to profile behavior and detect anomalies indicative of an attack. Analytics surface adversaries attempting to blend in with legitimate users.

Lightning-fast investigation & response
Investigate threats faster than ever before by getting a complete picture of each attack with incident management. You can view the root cause of any alert with a single click and swiftly stop attacks across your environment.

Ready to learn more?

REQUEST A DEMO

paloalto NETWORKS | CORTEX XDR

3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com/cortex