
MITRE ATT&CK
MITRE
ATT&CK
MITRE ATT&CK

CORTEX XDR | paloalto NETWORKS

MITRE, MITRE Engenuity ATT&CK

Eirik Valderhaug

Sr. Consulting Engineer -
Cortex - EMEA & LATAM

Link to the LinkedIn Live Webinar Recording

Agenda

1. MITRE, MITRE ATT&CK, MITRE ENGENUITY
2. Brief Background on MITRE ATT&CK & MITRE Engenuity Evaluations
3. Deep Dive into the Turla Evaluation and Results & and a History
4. The current state of the ATT&CK Evaluations
5. Demos

I will be using Palo Alto Networks' products at certain times to illustrate the MITRE ATT&CK FRAMEWORK and functionalities - as well as MITRE's own sources.

MITRE, MITRE ATT&CK, MITRE ENGENUITY

MITRE: Nonprofit organization for research.

MITRE ATT&CK: Cyberattack behavior framework by MITRE.

MITRE Engenuity Evaluations: Tests cybersecurity vendors against ATT&CK.

CORTEX XDR | paloalto NETWORKS

MITRE Corporation Overview

Non-Profit
Operates as a non-profit organization, prioritizing public welfare over profit.

FFRDCs
Runs multiple Federally Funded Research and Development Centers for the U.S. government.

Expertise
Specializes in systems engineering, cybersecurity, artificial intelligence, and healthcare.

Innovation
Develops solutions for complex, public sector challenges to benefit society.

CORTEX XDR® | paloalto® NETWORKS

Goal 1: Advancing Public Interest

Challenges
Focuses on long-term issues impacting national security, public safety, and health.

Non-Profit
Works as a non-profit, ensuring projects focus on public good over financial gain.

Impact
Designs solutions to address critical national and global concerns.

Benefit
Ensures that technological solutions serve the broader public interest.

Goal 2: Technical Expertise

Cybersecurity
Provides expertise in cybersecurity to enhance national resilience to threats.

AI
Develops and implements AI solutions to solve complex technical issues.

Advisory
Offers research and technical advice to support U.S. federal agencies.

Solutions
Solves complex, technical challenges with innovative technologies.

CORTEX XDR | paloalto NETWORKS

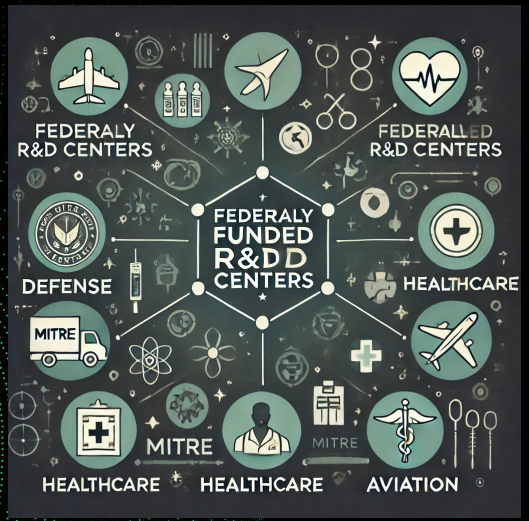
Goal 3: Federally Funded R&D Centers

Centers
Operates multiple FFRDCs supporting diverse public sectors.

Defense
Includes the National Security Engineering Center, focused on national defense.

Aviation
Manages the Center for Advanced Aviation System Development for safe skies.

Healthcare
Runs the CMS Alliance to Modernize Healthcare, enhancing public health services.



CORTEX XDR® | paloalto® NETWORKS

Goal 4: Cybersecurity Leadership

Framework
Developed the MITRE ATT&CK framework, a leading cybersecurity tool.

Detection
Creates tools to help detect and counter cyber threats effectively.

Resilience
Builds resources for organizations to strengthen their cybersecurity posture.

Awareness
Promotes cybersecurity awareness and readiness across industries.

CORTEX XDR | paloalto NETWORKS

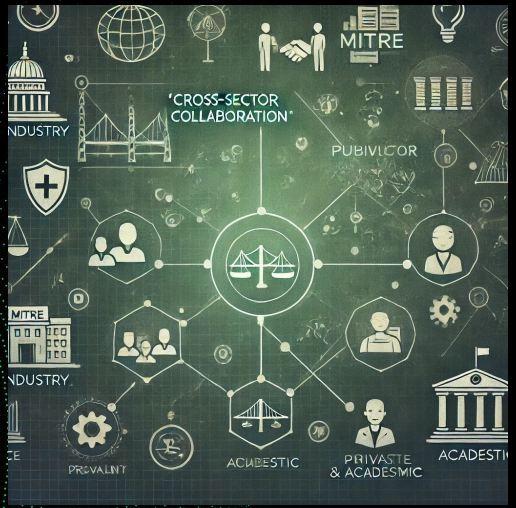
Goal 5: Cross-Sector Collaboration

Bridges
Connects public and private sectors to tackle complex issues.

Partnership
Collaborates with academia, industry, and government on common challenges.

Infrastructure
Focuses on securing critical infrastructure, like energy and transportation.

Ethics
Works on responsible AI and ethical technology use across sectors.



CORTEX XDR | paloalto NETWORKS

Goal 6: Research and Innovation

Investment
Funds independent R&D to address emerging needs proactively.

Leadership
Stays at the forefront of technology by leading innovative projects.

Solutions
Develops solutions for security, healthcare, and infrastructure resilience.

Public Good
Ensures that innovations directly contribute to societal well-being.

CORTEX XDR | paloalto NETWORKS

MITRE’s Mission and Impact

Welfare
Enhances public welfare through advanced technology solutions.

Security
Strengthens national security by addressing cyber and physical threats.

Resilience
Builds resilience across sectors, from health to infrastructure.

Society
Aims to create a safer, healthier, and more resilient society.

CORTEX XDR® | paloalto® NETWORKS

The MITRE ATT&CK Framework

MITRE Enterprise ATT&CK Framework

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	40 techniques	15 techniques	29 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
									Exploitation of Remote Services	Adversary-in-the-Middle (0/2)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
									Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
									Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
									Remote Service Session Hijacking (0/2)	Automated Collection	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
									Remote Services (0/6)	Browser Session Hijacking	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
									Replication Through Removable Media	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
									Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
									Taint Shared Content	Data from Configuration Repository (0/2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
									Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
										Data from Local System	Non-Application Layer Protocol		Network Denial of Service (0/2)
										Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
										Data from Removable Media	Protocol Tunneling		Service Stop
										Data Staged (0/2)	Proxy (0/4)		System Shutdown/Reboot
										Email Collection (0/3)	Remote Access Software		
										Input Capture (0/4)	Traffic Signaling (0/1)		
										Screen Capture	Web Service (0/3)		
										Video Capture			

Adversaries Tactics

- What are they doing?
- Why are they doing it?

Adversaries Techniques

- How are they doing it

paloalto NETWORKS

CORTEX XDR® | paloalto® NETWORKS

The MITRE Engenuity ATT&CK Evaluations

MITRE Engenuity Enterprise ATT&CK Evaluations

- **Motivation behind the ATT&CK Evaluations?**
  - “Vendors are using ATT&CK to articulate their capabilities, but there is no neutral authority to evaluate their claims”
- **What ARE the ATT&CK Evaluations?**
  - Open, transparent & objective. Methodology and results published openly and clearly
  - Evaluates both Protection and Detection efficacy (Protection starting round 3)
  - Simply a compilation of the detections MITRE Engenuity observes in response to an emulated adversary's tactics and techniques
- **What are they NOT?**
  - Not designed to address noise or false positives
  - No vendor rankings or ratings

CORTEX XDR® | paloalto® NETWORKS

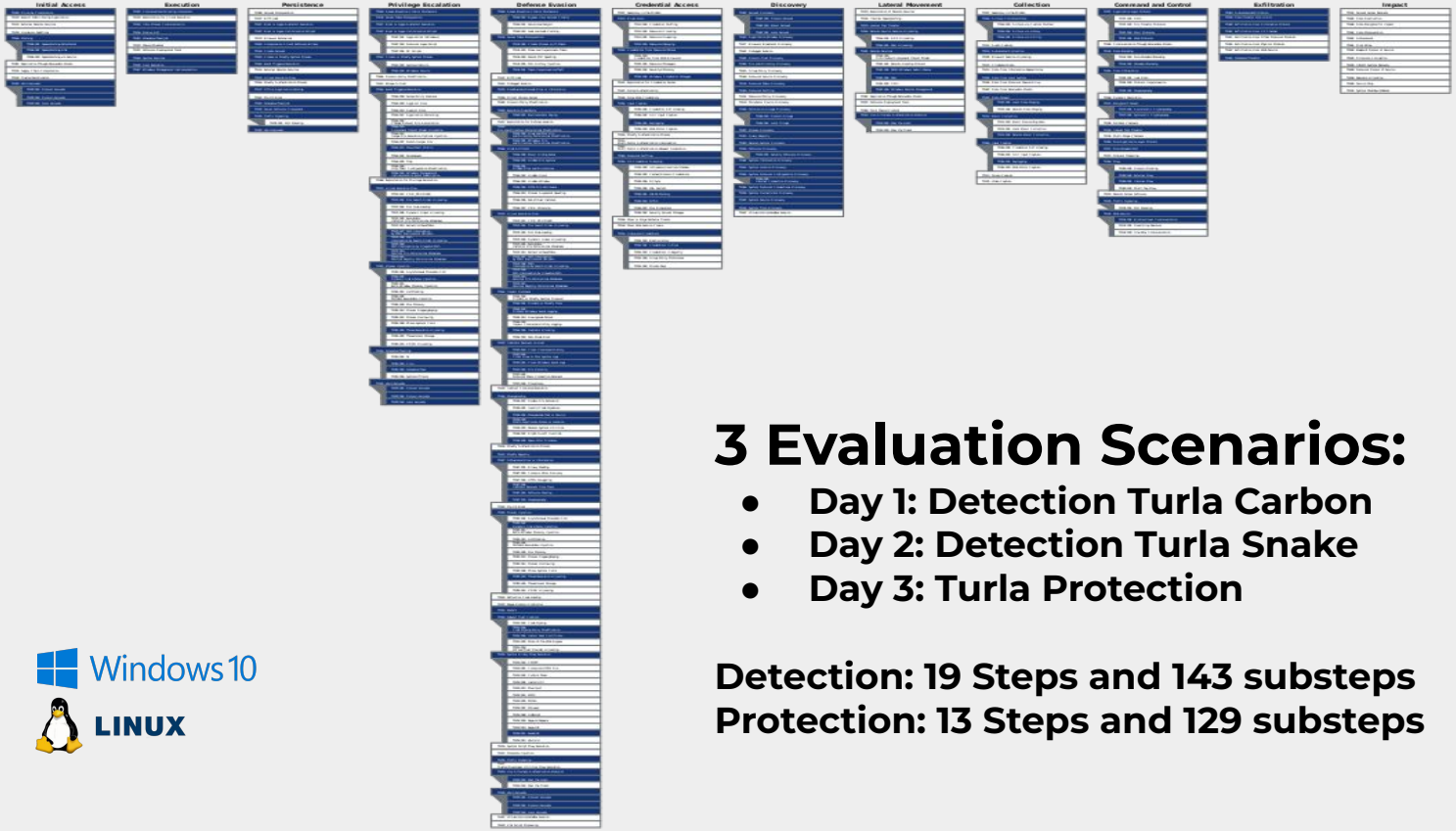
MITRE ATT&CK Enterprise Evaluations Round 5 (Turla)

Enterprise ATT&CK Round 5 Adversary: Turla

- Turla: Russia-based threat group, c16 of Russia's Federal Security Service (FSB)
- Also Known As:
  - MITRE ATT&CK Group ID: G0010
  - Pensive Ursa, IRON HUNTER, Group 88, Belugasturgeon, Waterbug, WhiteBear, Snake, Krypton, Venomous Bear
- Targets: government, embassies, military, education, research and pharmaceutical companies since 2004. Heightened activity seen since mid-2015

- Known For:
  - Targeted intrusions and innovative stealth
  - Infected over 45 countries
  - Numerous custom malware tools: Snake implant/rootkit, Carbon, Capibar
  - CISA Advisory: Hunting Russian Intelligence "Snake" Malware

MITRE ATT&CK Scope: 2023 Turla Evaluation



Windows 10

LINUX

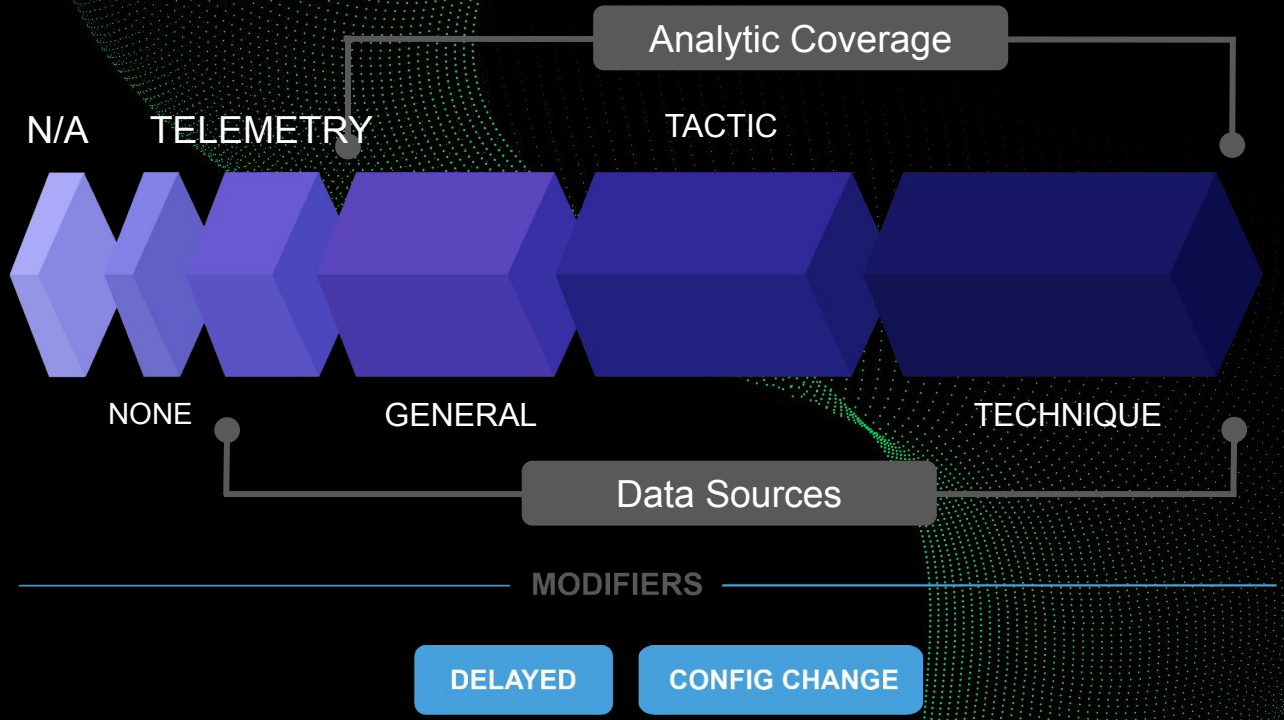
3 Evaluation Scenarios:

- Day 1: Detection Turla Carbon
- Day 2: Detection Turla Snake
- Day 3: Turla Protection

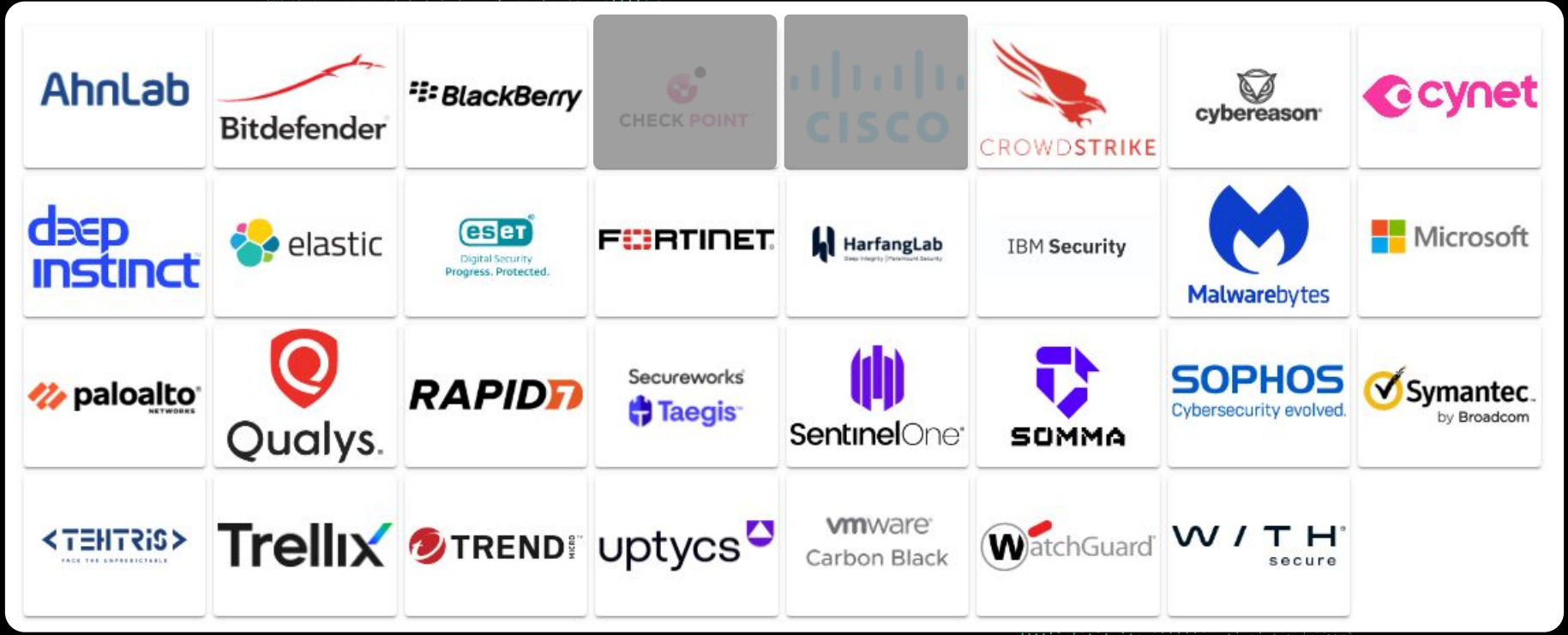
Detection: 19 Steps and 143 substeps
Protection: 13 Steps and 129 substeps

paloalto NETWORKS

MITRE Engenuity
Detection Categories



MITRE ATT&CK Scope: 2023 Turla Evaluation Participants



Note: 31 Vendors listed as Participants, Check Point and CISCO chose not to results published

CORTEX XDR® | paloalto® NETWORKS

MITRE Engenuity ATT&CK Round 5 (Turla) Results

Everyone’s a winner!!!

https://attackevals.mitre-engenuity.org/results/enterprise/

CORTEX XDR® | paloalto® NETWORKS

The State of the Evaluations… And Looking Forward

MITRE Engenuity ATT&CK Evaluation Resources:

- **Learn more about Turla**
  - Unit 42 Threat Group Assessment: Turla (aka Pensive Ursa)
  - Unit 42 The Turla Archives
  - MITRE ATT&CK Framework Details on Turla
  - CISA Advisory on Turla from May 2023: Hunting Russian Intelligence “Snake” Malware

- **2023 MITRE Engenuity ATT&CK Evaluations results**
  - Parker’s Blog: Current State of MITRE Engenuity Evaluations The Good, the Bad, and the Ugly
  - Peter’s Blog: Cortex XDR Results for 2023 MITRE Engenuity ATT&CK Evaluation
  - Interesting 3rd Party Read: eSecurity Planet’s write-up on the MITRE ATT&CK Evaluations 2023
  - Palo Alto Networks’ MITRE Engenuity ATT&CK Evaluations Results dashboard:
    - https://www.paloaltonetworks.com/mitre-results
  - MITRE Engenuity results Page:
    - https://attackevals.mitre-engenuity.org/enterprise/turla/

CORTEX XDR® | paloalto® NETWORKS

Thank You