cybereason®

End Cyber Attacks

From Endpoints to Everywhere

Qui sommes-nous ?

1000+

Employés

1 à 500,000+

Déploiement Endpoint

CE QUE DISENT LES ANALYSTES :

‘Leader’ dès la 2e appartition au MQ Gartner EPP

100% ATT&CK protection et couverture Linux dans l’évalutation MITRE ATT&CK

Cybereason dans la santé en France

- Plus de 200 000 endpoints sécurisés dans différents centres hospitaliers
- Présent au marché UGAP
- Présent au marché UNIHA
- Présent au marché CAIH

Pourquoi Cybereason ?

- EPP/EDR Next Gen avec un agent unique
- Compatibilité EDR avec tous les EPP du marché
- Malop : Corrélation et remédiation EDR intelligente et multi-machines
- Faible consommation des ressources et faible empreinte réseau
- Large couverture d’OS (Windows XP, 2003, 2008 ; Mac et Linux)
- Taux de faux positif faible

2022 EPP GARTNER MAGIC QUADRANT LEADER.

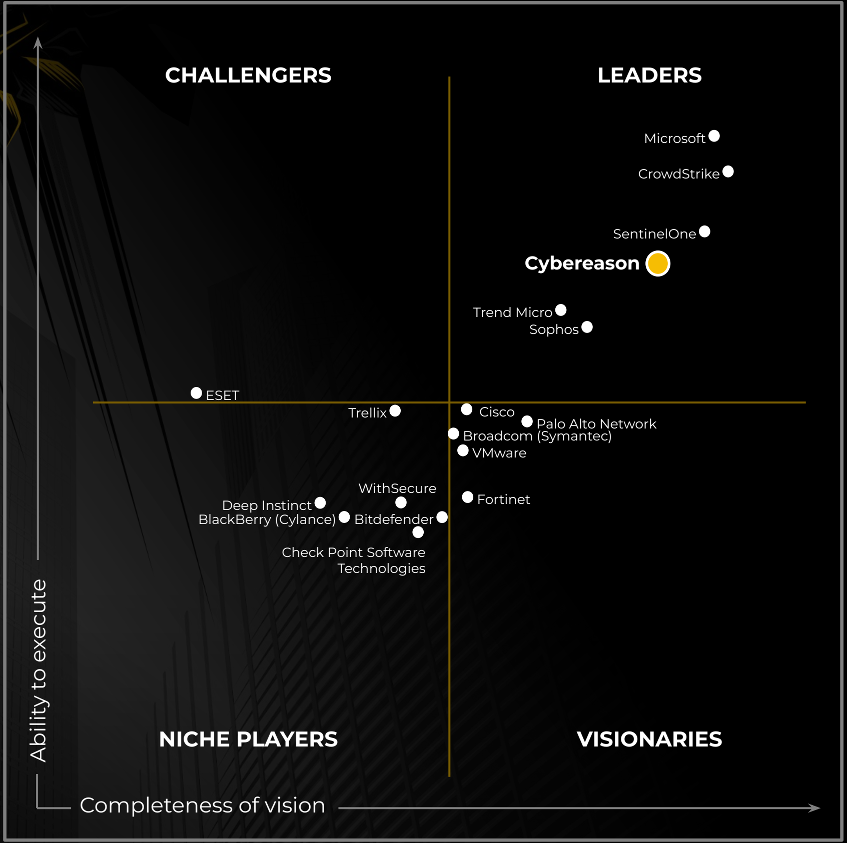
THE REASON?

Unprecedented leap from ‘Visionary’ to **‘Leader’**

Undefeated against ransomware

Highest ever recorded score in the **MITRE ATT&CK testing**

Only Cybereason **reduces alerts by 10X**



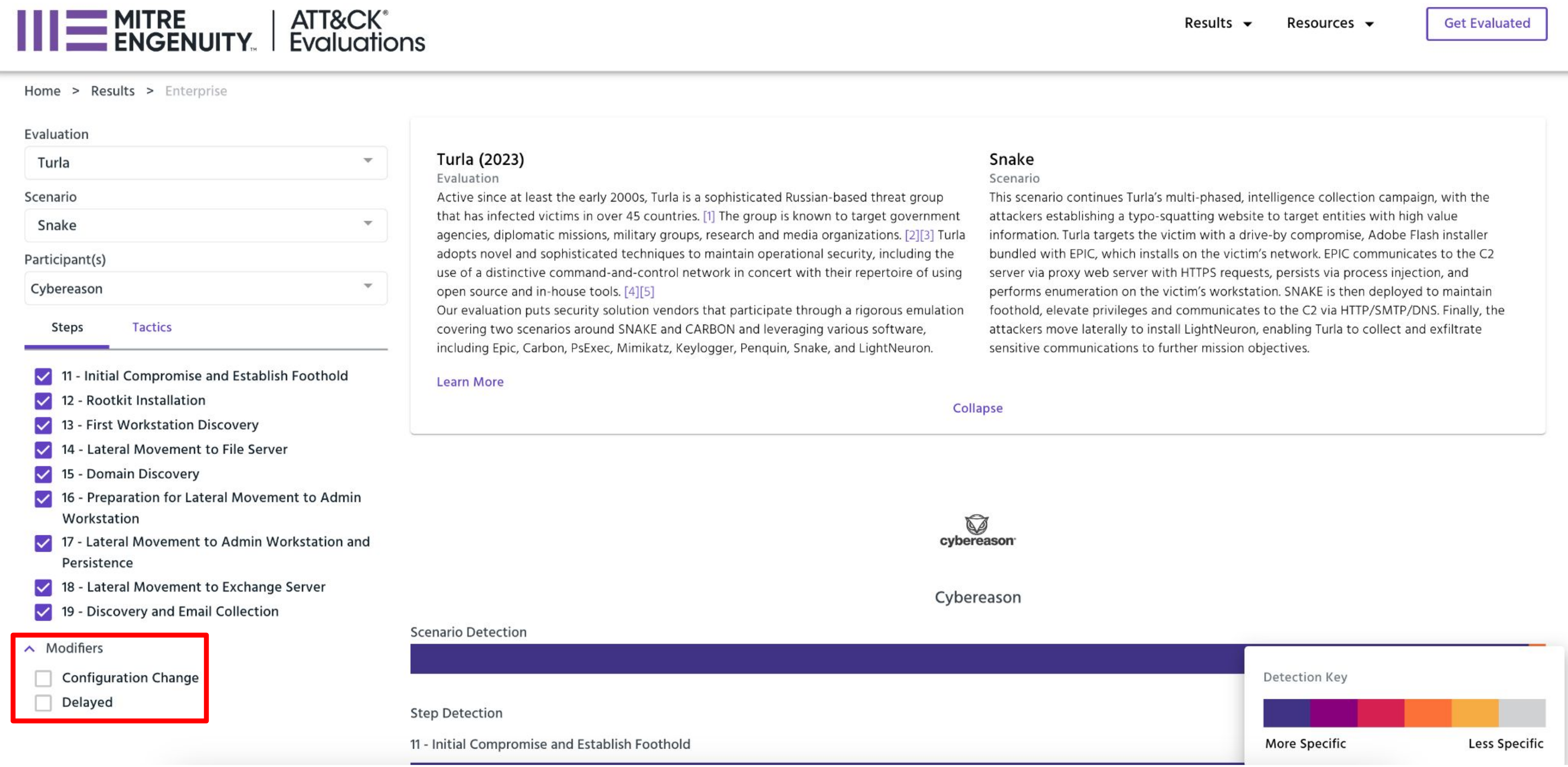
cybereason

MITRE ATT&CK 2023 TURLA EVALUATION

Top Performance in All Categories

100% Protection	Blocked 13/13 Protection Tests
100% Detection	Detected 19/19 Attack Steps
100% Visibility	Revealed 143/143 Attacker Sub-Steps
100% Real Time	No Delayed Attack Detections
100% Out of the Box	No Configuration Changes Needed

https://attackevals.mitre-engenuity.org/results/enterprise?vendor=cybereason&evaluation=turla&scenario=2



Home > Results > Enterprise

Evaluation

Turla

Scenario

Snake

Participant(s)

Cybereason

Steps Tactics

- ☑ 11 - Initial Compromise and Establish Foothold
- ☑ 12 - Rootkit Installation
- ☑ 13 - First Workstation Discovery
- ☑ 14 - Lateral Movement to File Server
- ☑ 15 - Domain Discovery
- ☑ 16 - Preparation for Lateral Movement to Admin Workstation
- ☑ 17 - Lateral Movement to Admin Workstation and Persistence
- ☑ 18 - Lateral Movement to Exchange Server
- ☑ 19 - Discovery and Email Collection

Modifiers

- □ Configuration Change
- □ Delayed

Turla (2023)

Evaluation

Active since at least the early 2000s, Turla is a sophisticated Russian-based threat group that has infected victims in over 45 countries. [1] The group is known to target government agencies, diplomatic missions, military groups, research and media organizations. [2][3] Turla adopts novel and sophisticated techniques to maintain operational security, including the use of a distinctive command-and-control network in concert with their repertoire of using open source and in-house tools. [4][5]

Our evaluation puts security solution vendors that participate through a rigorous emulation covering two scenarios around SNAKE and CARBON and leveraging various software, including Epic, Carbon, PsExec, Mimikatz, Keylogger, Penquin, Snake, and LightNeuron.

Learn More

Snake

Scenario

This scenario continues Turla's multi-phased, intelligence collection campaign, with the attackers establishing a typo-squatting website to target entities with high value information. Turla targets the victim with a drive-by compromise, Adobe Flash installer bundled with EPIC, which installs on the victim's network. EPIC communicates to the C2 server via proxy web server with HTTPS requests, persists via process injection, and performs enumeration on the victim's workstation. SNAKE is then deployed to maintain foothold, elevate privileges and communicates to the C2 via HTTP/SMTP/DNS. Finally, the attackers move laterally to install LightNeuron, enabling Turla to collect and exfiltrate sensitive communications to further mission objectives.

Collapse

Cybereason

Scenario Detection

Step Detection

11 - Initial Compromise and Establish Foothold

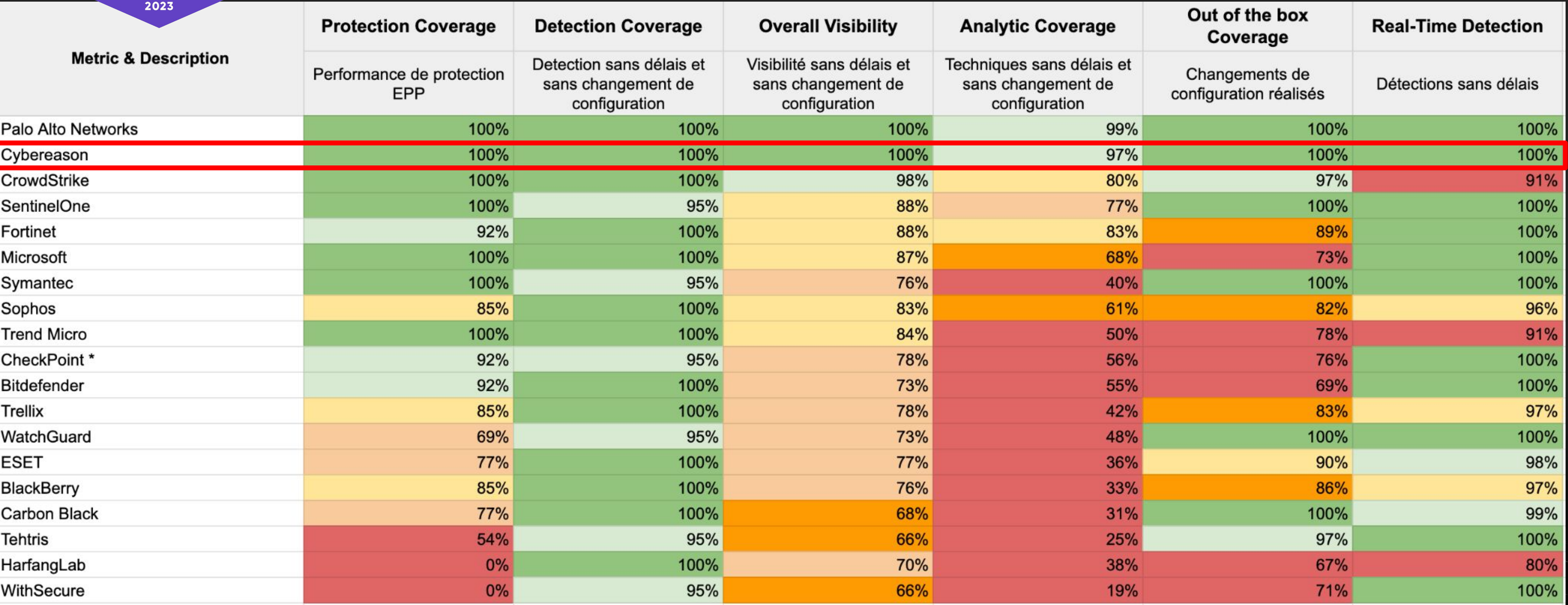
Detection Key

🟦 🟪 🟥 🟧 🟨 ⬜

More Specific Less Specific

MITRE ENGENUITY
ATT&CK® EVALUATIONS
Enterprise
TURLA
2023

ATT&CK Enterprise Evaluations 2023



Metric & Description	Protection Coverage	Detection Coverage	Overall Visibility	Analytic Coverage	Out of the box Coverage	Real-Time Detection
	Performance de protection EPP	Detection sans délais et sans changement de configuration	Visibilité sans délais et sans changement de configuration	Techniques sans délais et sans changement de configuration	Changements de configuration réalisés	Détections sans délais
Palo Alto Networks	100%	100%	100%	99%	100%	100%
Cybereason	100%	100%	100%	97%	100%	100%
CrowdStrike	100%	100%	98%	80%	97%	91%
SentinelOne	100%	95%	88%	77%	100%	100%
Fortinet	92%	100%	88%	83%	89%	100%
Microsoft	100%	100%	87%	68%	73%	100%
Symantec	100%	95%	76%	40%	100%	100%
Sophos	85%	100%	83%	61%	82%	96%
Trend Micro	100%	100%	84%	50%	78%	91%
CheckPoint *	92%	95%	78%	56%	76%	100%
Bitdefender	92%	100%	73%	55%	69%	100%
Trellix	85%	100%	78%	42%	83%	97%
WatchGuard	69%	95%	73%	48%	100%	100%
ESET	77%	100%	77%	36%	90%	98%
BlackBerry	85%	100%	76%	33%	86%	97%
Carbon Black	77%	100%	68%	31%	100%	99%
Tehtris	54%	95%	66%	25%	97%	100%
HarfangLab	0%	100%	70%	38%	67%	80%
WithSecure	0%	95%	66%	19%	71%	100%

cybereason®

THANK YOU.