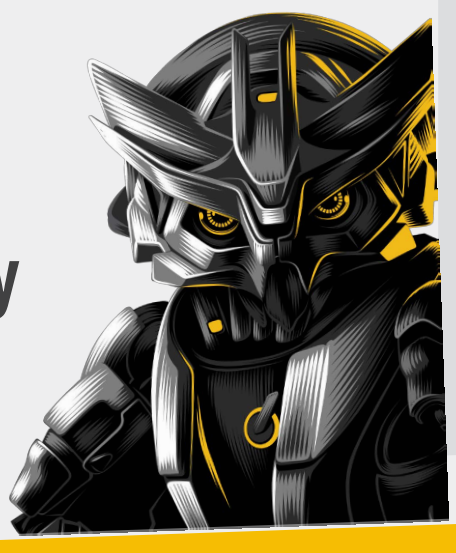
cybereason© | MITRE | ATT&CK®

ENTERPRISE EVALUATION
2024 RESULTS

Gain Operational Excellence and Efficiency for Your SOC!



Sophisticated threat actors are generally effective attacking under-prepared environments. This makes it essential to invest in highly-effective security solutions.

The MITRE ATT&CK evaluations measure that effectiveness. In the 2024 evaluation that features 19 vendors, it's challenging to sift through the noise. As you review the results, here are five high-impact metrics to consider: Out-of-the Box Capability, Detection Coverage, Efficiency & Number of Critical and High Alerts, Visibility, and False Positives.

100% OUT-OF-THE BOX CAPABILITY

ZERO Configuration Changes Required to detect every Windows, Linux, and macOS based threat.

100% DETECTIONS

Cybereason achieved **100% threat detection across all 79 attack steps** by Clop, LockBit, and the DPRK.

100% VISIBILITY

Exposed ALL attack behaviors evaluated for Windows, Linux, and macOS environments.

100% ACCURARCY

Cybereason had **ZERO false positive detections** throughout the entire evaluation.

100% SOC EFFICIENCY

Cybereason demonstrated the Best SOC Efficiency with creating **ONLY 18 Critical Alerts** while detecting ALL 79 Attack steps.

Why Does MITRE ATT&CK Matter?

ATT&CK is a standardized framework that maps adversarial tools, tactics and procedures (TTP's) and is the gold standard for both Endpoint Security vendors and security practitioners. This catalog of TTP's creates structure and organization for detection and response where it previously did not exist through a digestible framework. ATT&CK is always expanding to incorporate new threats.

ATT&CK emulations test detection and response efficacy on a yearly basis. MITRE is extremely reputable and is the most qualified organization to conduct these attack emulations. Their mission is to help global users better understand adversary behaviors. Most importantly, vendors can't pay more for better results. MITRE evaluations of Endpoint Security solutions are unbiased and transparent.

The Enterprise Evaluation 2024 examined common behaviors that are prevalent across prolific ransomware campaigns (Clop and LockBit). This evaluation features an introduction into macOS, delving into adversary behavior inspired by the Democratic People's Republic of Korea's (DPRK) targeting of macOS. This evaluation also incorporates multiple smaller emulations, introducing a more nuanced and targeted evaluation of defensive capabilities.

The **MITRE ATT&CK** evaluations are a Meritocracy. It's an equal playing field where every vendor submits their best endpoint security solution and all go through the same evaluation process. Today, these yearly rounds are the gold standard in technical testing across attack prevention and detection.

2024 EVALUATION RESULTS

100% COMPLETE DETECTION

Cybereason achieved 100% threat detection across **ALL 79 attack steps** exhibited by Clop, LockBit, and the DPRK. Every Cybereason detection occurred with Zero-False Positives.

100% OUT-THE-BOX COVERAGE

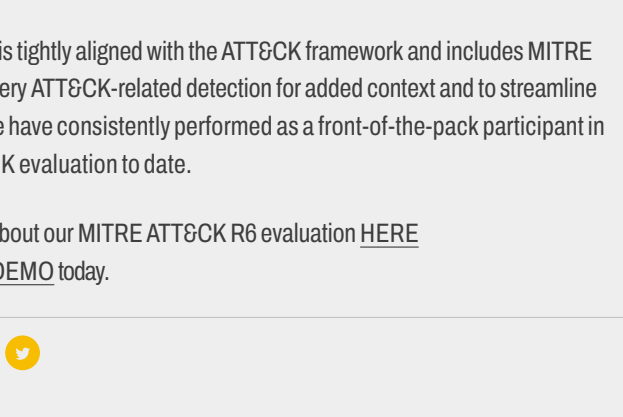
Cybereason understands security teams do not get a do-over when experiencing a real world cyberattack. The SOC needs a solution that works right out-of-the-box. Cybereason was one of the few vendors that delivered this in MITRE 2024 Evaluation.

100% VISIBILITY

Cybereason is mapped tightly to the overall ATT&CK framework, with 100% visibility into ATT&CK TTP's included in the Enterprise Evaluation 2024. The MalOp Detection Engine is the core of how Cybereason provides this level of visibility to our customers, and in this round we demonstrate the complete picture of the threat.

100% ANALYTIC COVERAGE

Analytic detections are deeper detections that are constructed from subtle signals and indicators. Analytic detections are built from a broader data set and are a combination of technique + tactic detections. This produces a nuanced view of what took place for enriched detections.

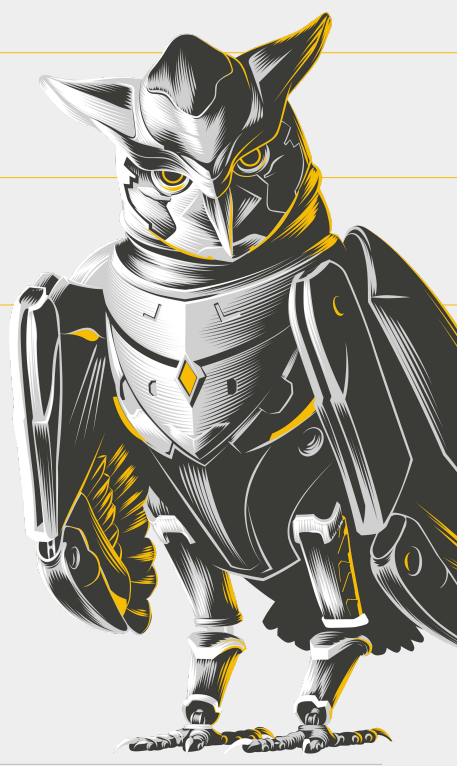


100% Efficiency on Alerts

Cybereason had the most efficient score on the number of total alerts raised vs. which were deemed critical or high. Cybereason had one of the lowest number of alerts vs. other vendors at 18. **ALL 18** were critical or high alerts, whereas other vendors had hundreds or thousands of alerts, many of them still deemed critical or high.

Why Cybereason

Results When It Matters	Cybereason security solutions are reliable and perform in the field against the most sophisticated adversaries.
Ransomware Ready	Cybereason is undefeated in the fight against ransomware and our defenses are predictive and multi-layered.
Immediate visibility	See threats in real time and react without delays to minimize impact and reduce risk.
Bulletproof Prevention	Defenders can rely on our technology to act competently to block and prevent in lieu of manual investigation and response.
Actionable Detections	The MalOp™ is highly actionable and contains scope, timeline, tools used by the attacker and all telemetry that led to a conviction in a single UI view.
One Click Response	Immediately restore trust to all impacted systems and users across the enterprise with a single click.



Cybereason is tightly aligned with the ATT&CK framework and includes MITRE tagging on every ATT&CK-related detection for added context and to streamline response. We have consistently performed as a front-of-the-pack participant in every ATT&CK evaluation to date.

Learn more about our MITRE ATT&CK R6 evaluation HERE or request a DEMO today.