cybereason

MITRE ATT&CK EVALUATIONS

2023 ENTERPRISE RESULTS

Outclass a sophisticated adversary

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 2023 evaluation that features 30 vendors, it's challenging to sift through the noise. As you review the results, here are five high-impact metrics to consider: Protection Coverage, Detection Coverage, Visibility, Real-Time Detections, and Out-of-the-Box Coverage.

100% PROTECTION COVERAGE

Cybereason uncovered and prevented all 13 of the attack sequences across Windows and Linux systems.

100% DETECTION COVERAGE

Cybereason detected **all 19 of the attack steps** that are commonly executed by the Turla threat actor.

100% VISIBILITY

Cybereason exposed **all 143 attack behaviors** with zero missed detections across Windows and Linux systems.

100% REAL-TIME DETECTION

Every Cybereason detection occurred in real time, providing teams with the fastest response times possible.

100% OUT-OF-THE-BOX COVERAGE

Cybereason delivered **complete out-of-the-box performance**, with no configuration changes required.

Why Does MITRE ATT&CK Matter?

The MITRE ATT&CK evaluations are a Meritocracy. It's an equal playing field where every vendor submits their best 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.

ATT&CK is a standardized framework that maps adversarial tools, tactics and procedures (TTP's) and is the gold standard for 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 security solutions are unbiased and transparent.

The 2023 Enterprise Evaluation was based on Turla, a highly sophisticated threat group known to carry out surveillance on targets to exfiltrate sensitive information. 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.

EVALUATION RESULTS

Turla

100% PROTECTION

A security solution that can't put up a good fight against attackers ultimately sets off a chain reaction of chaos for your security team. The more threats that are prevented, the less security teams must investigate and respond. Cybereason boasts a 100% protection score in the 2023 Enterprise Evaluation.

100% VISIBILITY

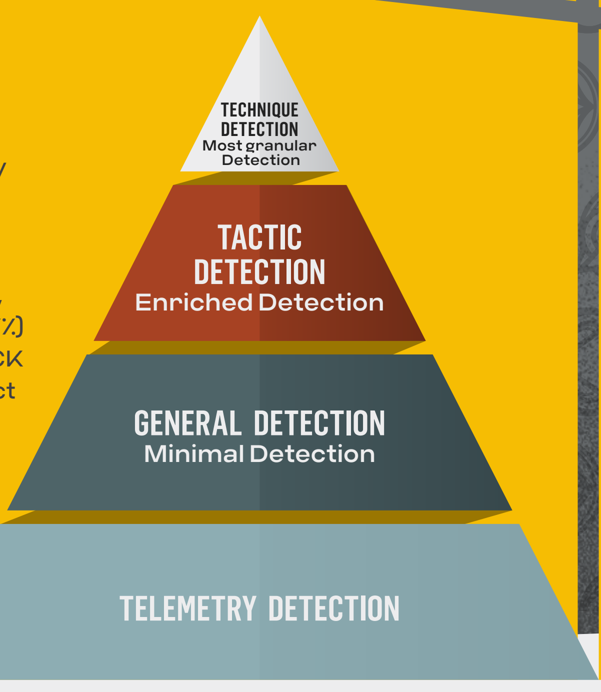
It can be a real challenge for defenders to spot and stop sophisticated attacks, which is why it is crucial to evaluate a solution's ability to see the complete picture - where it started, what was impacted, and the complete attack timeline. Cybereason is mapped to the MITRE ATT&CK framework and exposed 100% of the 143 attack behaviors evaluated in the 2023 Enterprise Evaluation.

100% REAL TIME

Delayed detections are ones that are not caught immediately, and instead require additional time and context to identify and catch. When it comes to defending against sophisticated threats such as Turla, the single most important factor is time. In the 2023 Enterprise Evaluation, Cybereason provided immediate visibility with 100% real-time detections and with zero delays.

100% DETECTION

To keep attackers from hiding amongst the noise, you need security tools that can instantly spot attacker behavior. Cybereason achieved 100% threat detection across all 19 attack steps exhibited by Turla, with nearly every detection (97%) mapped back to the key ATT&CK techniques that reveal the exact actions that attackers take.



100% OUT-OF-THE-BOX COVERAGE

When a security solution misses a simulated attack on the first try, you can adjust configurations for another shot at stopping the attack. But in the real world, businesses don't get a do-over. Out-of-the-box capabilities allow teams to focus on critical response actions rather than spend time fiddling with security systems. In the 2023 evaluation, Cybereason delivered complete out-of-the-box performance, requiring no configuration changes.

Why Cybereason

Results When It Matters	Cybereason security solutions are highly effective and perform in the field against the most sophisticated adversaries.
Ransomware Ready	Cybereason is undefeated in the fight against ransomware, with predictive and multi-layered defenses.
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 block and prevent in lieu of manual investigation and response.
Actionable Detections	The MalOp$^{\text{tm}}$ is highly actionable and contains scope, timeline, tools used by the attacker, and all telemetry that led to a conviction - presented in a single 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 evaluation HERE or request a DEMO today.

The views and opinions expressed in this are those of Cybereason and do not necessarily reflect the views or positions of any entities they represent.

LEARN MORE AT CYBEREASON.COM