cynet

THE PRACTICAL GUIDE TO THE MITRE ATT&CK EVALUATION

2023 TURLA EDITION

Once again, security technology buyers rely on the latest MITRE ATT&CK Evaluation results to help them better understand the capabilities of leading endpoint detection and response (EDR) providers. While no test can fully simulate a real world threat, the MITRE ATT&CK Evaluation comes closest by emulating portions of a real-world cyberattack and measuring how well the tested solutions detect and address the threats.

MITRE's testing methodology objectively evaluates endpoint security solutions based on the highly regarded MITRE ATT&CK framework. The evaluation tests the endpoint protection solutions against simulated attack techniques based on the real-life approaches of well-known Advanced Persistent Threat (APT) groups. The 2023 MITRE ATT&CK evaluation emulates attack techniques used by Turla, a sophisticated Russian-based threat group that has infected victims in dozens of countries.

As in the past, MITRE does not rank or score vendor results. Instead, the raw test data is published along with some basic online comparison tools. Buyers can use the data to evaluate the vendors as they see fit, based on their company's unique priorities and needs.

This guide provides advice and considerations for how to use the MITRE ATT&CK results as one component of your selection criteria as you determine which vendor will meet your specific needs.

MITRE ATT&CK Evaluation – Approach

MITRE's uses simulated attacks in a controlled lab environment to evaluate how vendor solutions behave against the exact same threats introduced in the exact same manner. Along with the myriad benefits of this approach, it's important to note that many important solution capabilities and characteristics are not included in the evaluation.

What It Is

Let's take it from the top – the MITRE ATT&CK evaluation uses an open, transparent, and unbiased testing process. MITRE provides a level playing field in a controlled environment so that all vendor solutions are tested consistently, without external, extraneous factors influencing the results as is the case in a real-world deployment.

MITRE does not simulate an end-to-end actual attack simulation. Every step and substep is presented regardless of previous detections and the attack techniques are not presented in the order that would be taken in an actual attack. This approach does evaluate how effectively a solution can detect an abundance of discrete steps that might be used by a certain threat group to carry out an attack. Because MITRE uses the techniques of real threat groups, each technique presented represents what is likely to happen in a real-world scenario.

The evaluation allows vendors to demonstrate how each threat is (or isn't) detected, the data sources used, and how they correlate with each other to determine a detection. This "under the hood" view contextualizes each capability, in addition to establishing that a detection occurred.

What It Isn't

Importantly, MITRE does not include any type of scoring or ranking of results. Any vendor claims of "victory" are based on the vendor's own interpretation of the results and are certainly not endorsed by MITRE.

For buyers, this means all vendor claims must be taken with a grain of salt. Buyers should read through all results to determine which measures best suit their particular needs and weigh these results alongside other factors necessary to vendor evaluation.

The MITRE ATT&CK evaluation also does not necessarily test a vendor's full range of threat protection capabilities. As the evaluation focuses on endpoint protection, it doesn't adequately test for other important telemetries that may be included in the vendor solution, such as network traffic, user behaviors, or deception. Nor does it adequately test how a real-world breach protection stack or an XDR solution would perform in detecting and preventing a real-world attack scenario. But, endpoint protection is critical — and the MITRE ATT&CK evaluation remains the best methodology for that component.

While the evaluation includes vendor platform screenshots and other useful measures, it does not evaluate platform usability or implementation and maintenance requirements. It doesn't evaluate false positive rates or breadth and depth of response features and capabilities, or whether individual threats are correlated into incidents.

As the go-to source for unbiased endpoint protection solution testing, the MITRE ATT&CK evaluation should be an important factor in any buyer's vendor evaluation process — but never the only factor, nor, in many cases, the primary factor.

Methodology

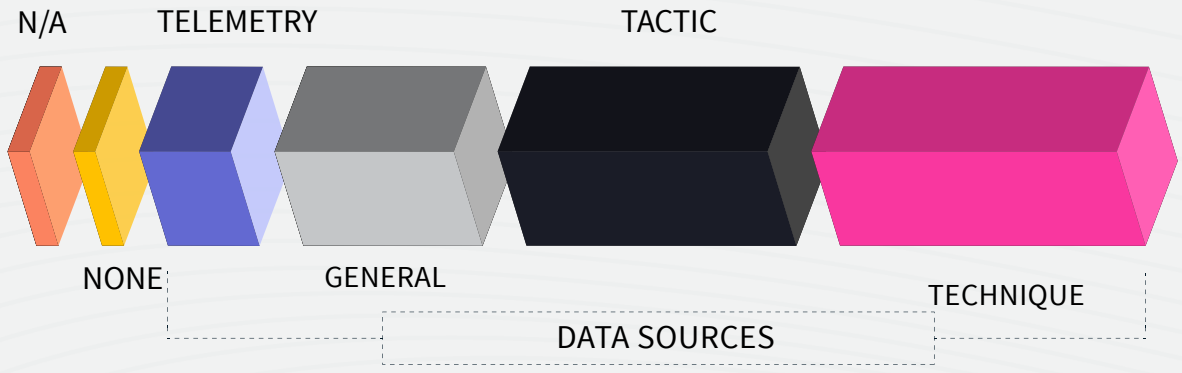
The 2023 MITRE ATT&CK Evaluation emulated attack techniques employed by the Turla hacking group. Turla, often claimed to be part of FSB's Center 16 group, is known for innovative stealthy approaches and post-exploitation persistence. The group is associated with the infamous Snake implant, which the US government considers the most sophisticated cyber-espionage tool in the world. For over 25 years, the Turla group has continually evolved by introducing novel techniques which are enumerated in a lengthy listing on the MITRE website.

Beyond Snake, some of the tools associated with Turla include ComRAT, KopiLuwak, Kazuar, and Carbon. While Turla primarily targets government entities, embassies and military organizations, it has also targeted private sector companies in pharmaceuticals, retail, education and high tech across most of the world. Turla is attributed with hacking the notorious Iranian hacking group APT34 and uniquely hijacking satellite communications to steal victims' data.

Turla Threat Detection on Windows

Day one testing focused on a multi-layer campaign targeting both Windows and Linux infrastructure with malware known to be used by Turla. Day two focused on kernel and Microsoft Exchange exploitation, again using malware associated with Turla. A total of 143 unique attack techniques were tested to determine the level of detection for each technique on a scale ranging from no detection through identifying the specific technique that was employed.

The detection categories indicate increasing levels of context provided to an analyst for each detection, with the best detection outcome being the identification of the specific MITRE ATT&CK technique or sub-technique.



MITRE ATT&CK evaluation detection categories

Turla Threat Detection on Linux

Similar to previous years' evaluations, MITRE included a separate evaluation of vendor solutions on Linux devices. The Linux evaluation included 27 of the 30 vendors. The expansion to Linux devices confirms the importance of providing protection across the hybrid operating system environments present (and growing) throughout the vast majority of companies. Today, Linux is often used for file servers and domain controllers, both of which are targeted for APT attacks.

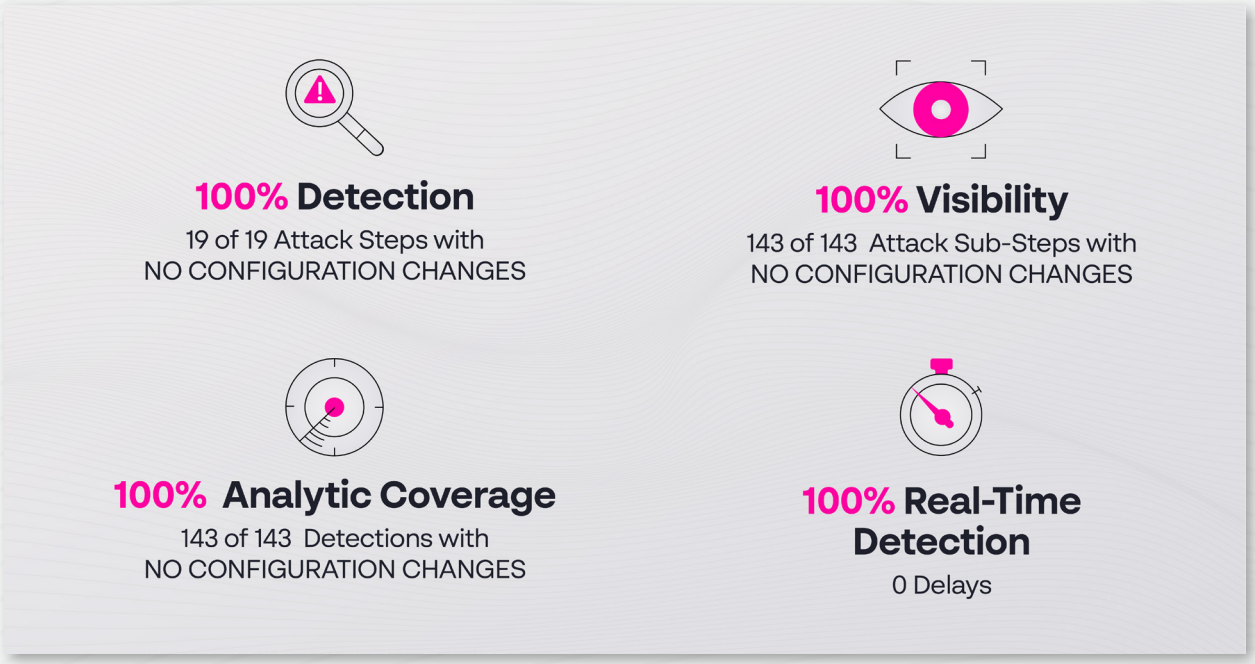
Using MITRE to Evaluate Endpoint Protection Solutions

The MITRE ATT&CK results can be a useful element when choosing the best threat protection tool for your organization. As part of any vendor selection exercise, each company will weigh components of the test differently, according to their needs and priorities. Several key measures from the MITRE evaluation will likely be relevant to most organizations at some level, including:

- Overall detection across the entire MITRE ATT&CK sequence
- Quality of detection that provides the detection category achieved for each sub-step
- Speed of detection to ensure that threat response is not delayed
- Evaluating the detection capabilities BEFORE the vendor was allowed to make configuration changes

Cynet Results

Cynet's 2023 ATT&CK evaluation results were exceptional by any measure. Cynet excelled in every category, even outperforming our previous strong ATT&CK evaluation results. Cynet's results demonstrate the unmatched effectiveness of our platform for protecting your organization using an intuitive, cost-effective solution.



Cynet is a Leader in Overall Visibility and Detection Quality

Charting Visibility with Analytic Coverage illustrates how well a solution does in detecting threats and providing the context necessary to make the detections actionable. These two metrics are clear indicators of a solution's ability to uncover dangerous attacks across the MITRE ATT&CK framework.

This is the first year in MITRE ATT&CK Enterprise Evaluation testing that a vendor delivered BOTH 100% Visibility and 100% Analytic Coverage with no configuration changes! We couldn't be prouder of this performance milestone. The following chart helps visualize how participants stacked up on these two important measurements. We'll get into more detail the measurements in the following sections.

The following table provides the numerical results depicted in the chart above

		Visibility	Analytic Coverage	Overall Detection Rate
1	cynet	**100%**	**100%**	**100%**
2	paloalto NETWORKS	100%	100%	100%
3	cybereason	100.00%	99.30%	99.65%
4	CROWDSTRIKE	97.90%	95.80%	96.85%
5	FORTINET	88.11%	83.92%	86.01%
6	SentinelOne	88.11%	83.92%	86.01%
7	SOPHOS	83.22%	81.12%	82.17%
8	Microsoft	85.31%	78.32%	81.82%
9	Uptycs	81.12%	78.32%	79.72%
10	TREND MICRO	83.92%	72.03%	77.97%
11	deep instinct	75.76%	75.76%	75.76%
12	WatchGuard	78.79%	69.70%	74.24%
13	Bitdefender	73.43%	71.33%	72.38%
14	CHECK POINT	78.32%	65.73%	72.03%
15	Symantec	75.52%	65.04%	70.28%

		Visibility	Analytic Coverage	Overall Detection Rate
16	Trellix	76.92%	61.54%	69.23%
17	HarfangLab	76.92%	60.14%	68.53%
18	IBM Security	72.03%	62.94%	67.48%
19	BlackBerry	78.32%	55.94%	67.13%
20	elastic	79.02%	55.24%	67.13%
21	AhnLab	66.67%	64.39%	65.53%
22	eset	76.92%	51.75%	64.34%
23	vmware Carbon Black	67.83%	48.95%	58.39%
24	TEHTRIS	65.73%	50.35%	58.04%
25	Secureworks	75.52%	37.76%	56.64%
26	Malwarebytes	58.04%	44.06%	51.05%
27	RAPID7	67.83%	26.57%	47.20%
28	WITH secure	65.73%	26.57%	46.15%
29		58.74%	33.57%	46.15%
30	Qualys.	35.66%	23.78%	29.72%

Cynet analysis of 2023 MITRE ATT&CK results

Overall Detection Rate = average of Visibility and Analytic Coverage

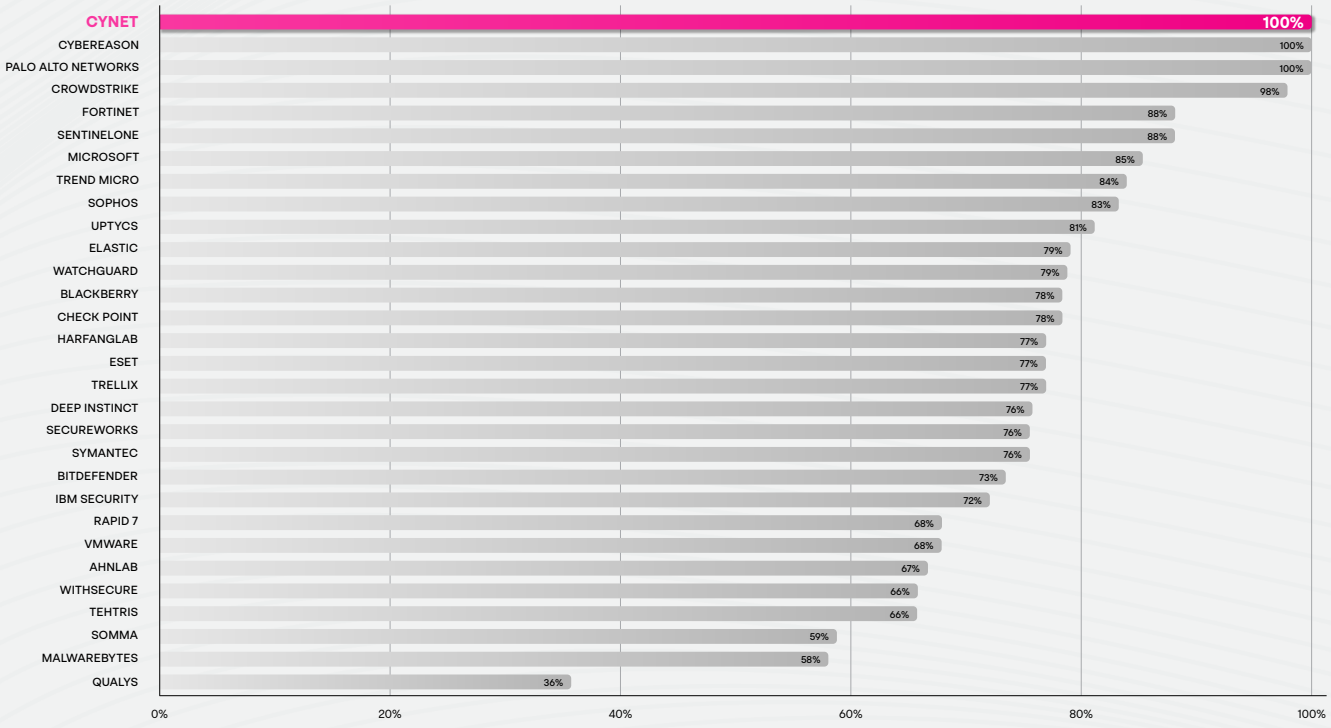
Results shown are before configuration changes

Cynet Delivered 100% Visibility and Perfectly Detected Every One of the 143 Attack Steps *using no configuration changes*

The ability to detect threats is the fundamental measure of an endpoint protection solution. Detecting attack steps across the MITRE ATT&CK sequence is critical for protecting the organization. Missing any step can allow the attack to expand and ultimately lead to a breach or other catastrophic outcomes.

The Turla attack sequence was executed over 19 steps, which were broken out into 143 sub-steps. This year, Cynet detected all of the 143 substeps that made up the attack. Cynet had ZERO misses in this year's MITRE testing and detected 100% of attack steps over Windows devices as well as Linux servers.

As importantly, every one of the 143 detections was done without the need for configuration changes. It's important to note that MITRE allows vendors to reconfigure their systems to attempt to detect threats that they missed. In the real world we don't have the luxury of knowing detections are missed and then reconfigure our systems, so the more realistic measure is detections without the configuration change modifier. As you review other the MITRE ATT&CK Evaluation outcomes for other vendors, make sure their detections were not after they were allowed to make configuration changes.



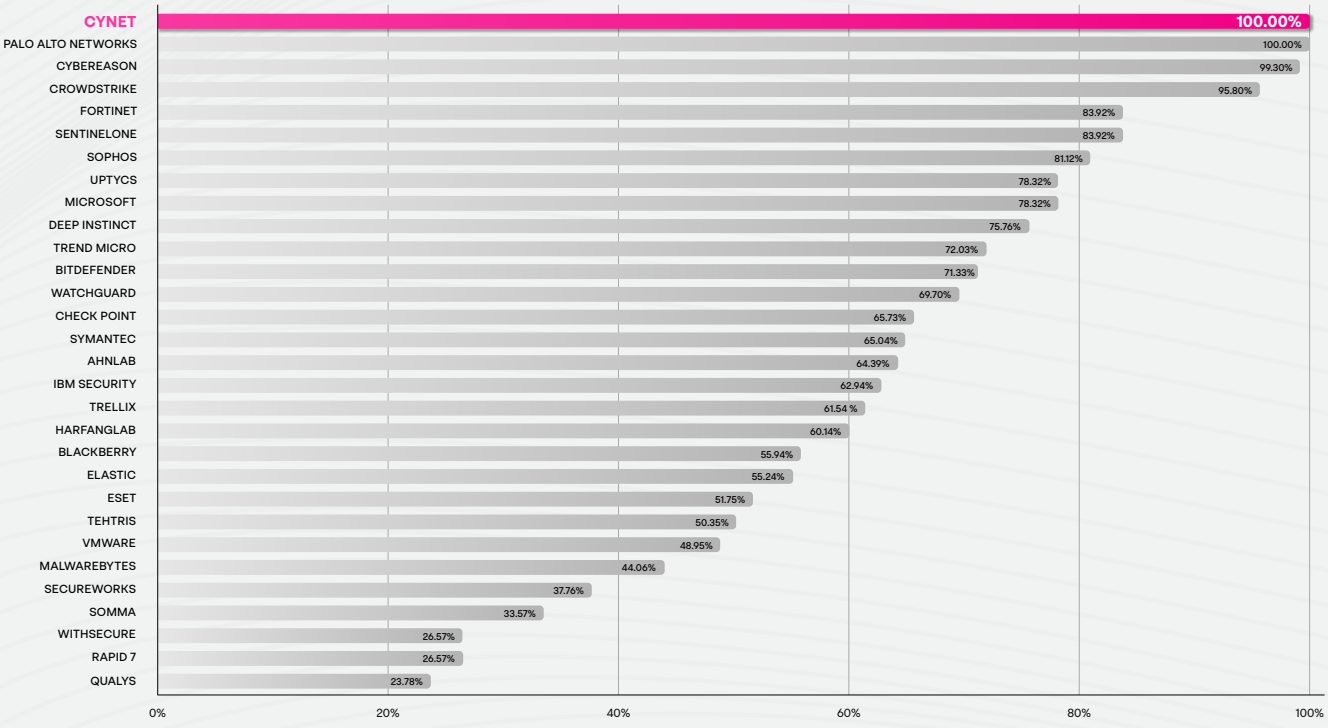
Total Visibility before Configuration Changes - 2023 MITRE ATT&CK Enterprise Evaluation

Cynet Provided Analytic Coverage for 100% of the 143 Attack Steps *using no configuration changes*

Analytic detections are those that identify generally that malicious/abnormal event(s) occurred, the tactic (why an activity may be happening) or technique (both why and how the technique is happening). These details are not only very helpful for security analysts when investigating an alert, but are also indicative of real threats vs false positive alerts.

Cynet provided analytic information (general, tactic, or technique) for every one of the 143 steps deployed in the Turla attack sequence. Again, it's important to note that vendors were allowed to reconfigure their systems to improve their analytic coverage results for each step. All analytic information was provided without the need for any configuration changes.

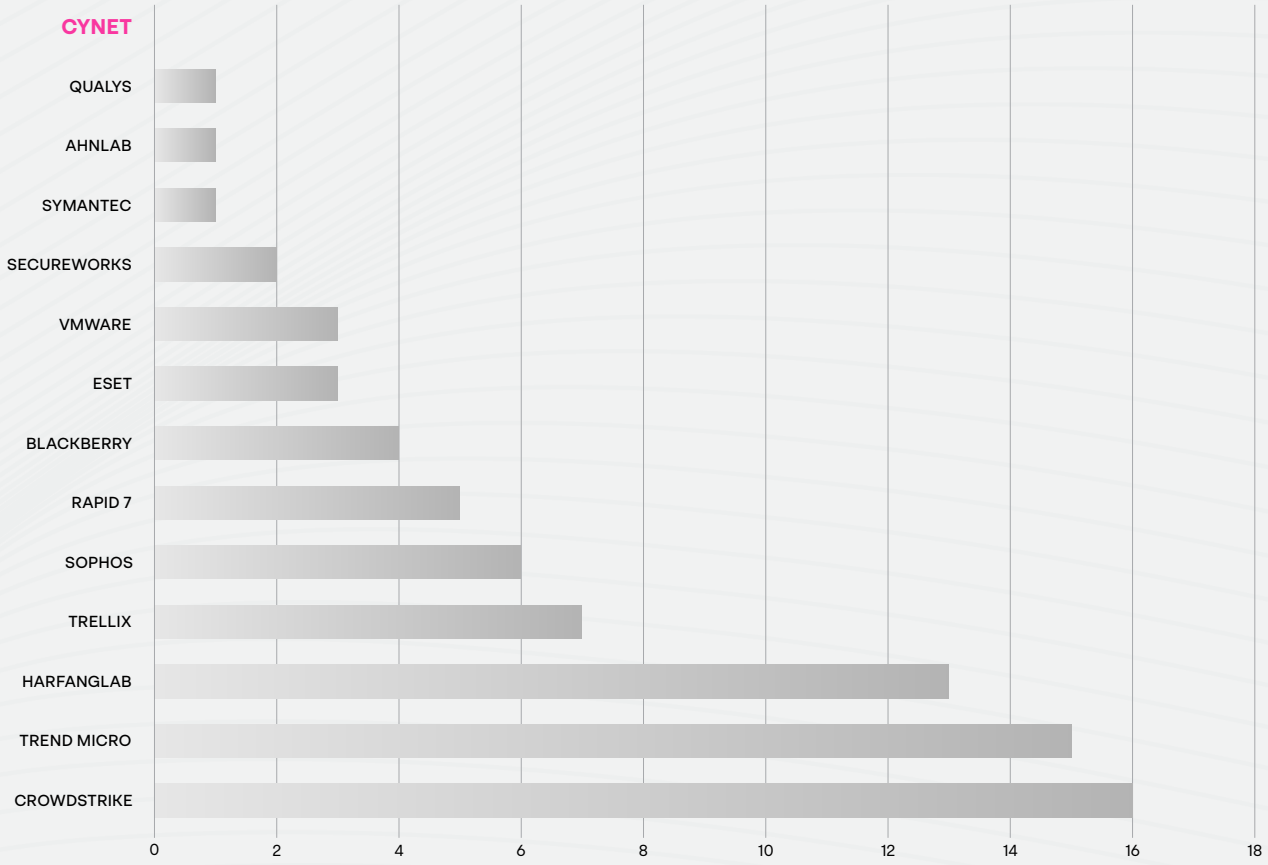
The Cynet platform provides full detection details for every alert, including information on the file, host, network, and user associated with the alert. Moreover, the platform launches an automatic investigation to uncover the root cause and scope of the potential attack to reduce your manual response efforts.



Analytic Coverage before Configuration Changes - 2023 MITRE ATT&CK Enterprise Evaluation

Cynet Delivered 100% Real-time Detections, Experiencing Zero Delays

In addition to Threat Visibility and Detection Quality, Detection Speed is a crucial measure when evaluating cybersecurity solutions. Detection delays during the evaluation often means that human intervention was required to evaluate the suspicious activity. Cybersecurity is all about speed, so any detection delays only allow the attacker that much more time to cause harm. Cynet detected every threat automatically, without delay. This is exactly what you want.



Number of Detection Delays - 2023 MITRE ATT&CK Enterprise Evaluation

Beyond MITRE With Cynet

As important as MITRE testing is to evaluate threat protection solutions, many other factors are equally or more important to the solution selection process. Although Cynet clearly demonstrated industry-leading detection and protection capabilities in the MITRE ATT&CK evaluation, several highly differentiating factors are critical to consider.

End-to-End, Highly Accurate Threat Visibility

The MITRE ATT&CK evaluation is primarily used to test the capabilities of endpoint detection and response (EDR) platforms. The rise of extended detection and response (XDR) capabilities expands telemetry beyond the endpoint, to additional critical elements of the environment. For example, Cynet XDR includes user-based telemetry analysis to detect behavioral anomalies that are indicative of cyberattacks. Cynet XDR includes several other important protection components that are not tested in the MITRE ATT&CK evaluation, including Network Detection and Response (NDR), Deception technology, and both SaaS and Cloud Security Posture Management (SSPM and CSPM).

Combining additional telemetry signals with endpoint telemetry signals adds context for more accurate results. Seemingly benign signals can signal dangerous attacks. Conversely, seemingly high-risk signals may be legitimate operations when viewed in full context. Adding telemetry, when done right, provides the rich information necessary to detect threats far more accurately than when analyzed alone or separately.

A tool that fires off alerts with too little or too much data isn't very helpful, even if it detects something that should be investigated. Cynet leverages telemetry from endpoint, network, user, and deception technology to ensure highly accurate alerts while minimizing false positives.

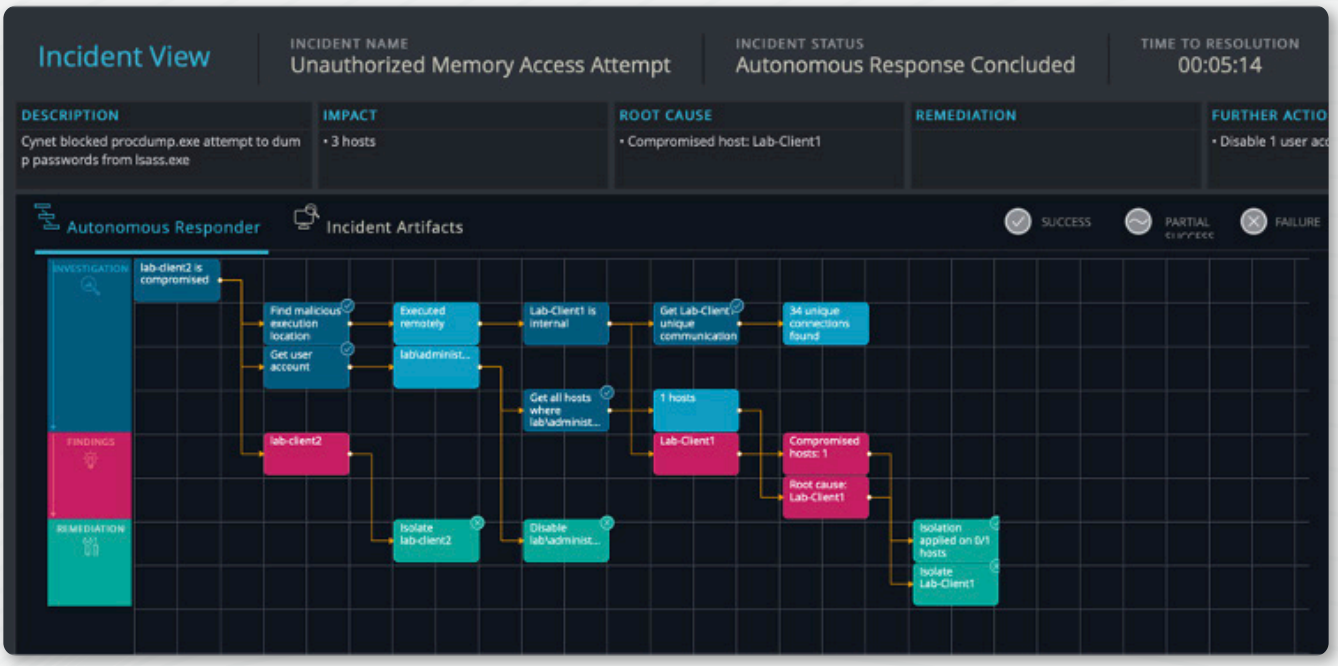
Ease of Use

While the tested vendors supply detection screenshots that can be viewed on the MITRE ATT&CK evaluation site, the solution's efficacy and ease of use was not evaluated. While it's important to select a provider that scored among the top of the MITRE evaluation measures, it's also important to select a user-friendly, intuitive product. Security analysts spend significant time interacting with vendor technology, so ensuring the platform is intuitive and easy to use should be an important component of your evaluation criteria.

This advice holds especially true for smaller security teams with limited budgets and skills. A tool that typically requires a small army of cybersecurity experts may work for a large, well funded security team, but will end up being mostly ignored without the necessary internal support resources. Cynet is purpose-built for lean security teams that don't have the bandwidth to work through overly complex interfaces designed for large security teams at large organizations.

Automated Incident Investigation and Response

Cynet goes beyond traditional alerts, to generate an automated incident response to ensure all alerts are investigated and all response actions are performed thoroughly and accurately. Cynet's built-in security orchestration, automation, and response (SOAR) automates threat investigation and response, moving beyond responding to the single threat at hand to helping determine if the detected threat is a single part of a larger attack, and if so, uncovering and responding to related attack components.



When a threat is detected, Cynet's Response Automation can launch an automated investigation to uncover the root cause of the threat. Was it downloaded from a specific site, embedded in a document, or attached to an email? Was it spawned by a yet undetected malicious process or planted from an RDP connection? Automated root cause analysis peels back these layers to ensure all elements of the attack are exposed, and ultimately uncovering the so-called "patient 0" — the origin of the attack.

Once additional components of a threat are uncovered, the entire environment is searched to expose the full scope of the attack. This includes taking appropriate remediation actions across the environment to eradicate all attack components automatically or manually, depending on your preference. You cannot be assured of safety until the attack is fully rooted out.

Manually performing these investigation steps takes time and skills and effort. Every alert becomes a lot of work. Unfortunately, many security teams do not have the bandwidth, and many smaller security teams lack the skills, to perform the necessary investigative steps. Automating this workflow, at a minimum, provides security teams with a considerable head start on incident response. And, in many cases, it eliminates the need for manual intervention.

Moreover, Cynet's automated response playbooks can be fully customized to consider company and environment-specific needs and preferences. An intuitive, drag-and-drop response playbook editor allows you to modify pre-built response workflows or completely build customized response playbooks from scratch.

Extended Platform Capabilities

Many large enterprises operate an extensive array of highly specialized IT security technologies that are integrated into a comprehensive security stack. Significant expertise and resources are required to design, build, integrate, operate, and maintain such a stack. Most companies, however, do not have the budget or bandwidth to take this approach.

It behooves resource-constrained companies to adopt security solutions that provide multiple capabilities. This way, organizations can obtain protections that might otherwise be unobtainable due to budget and/or resource constraints. Modern XDR tools that include multiple sources of telemetry, for example, help companies avoid the expense and burden of acquiring and integrating multiple third-party technologies to expand threat visibility across their environments. So-called "open XDR" solutions, conversely, still require companies to purchase multiple detection technologies that are integrated into the open XDR solution.

The Cynet 360 AutoXDR platform includes telemetry from endpoint, network, users and deception technologies. The solution is fully integrated out of the box, making it highly effective yet highly affordable.

Moreover, the Cynet platform offers additional security technologies, including SaaS Security Posture Management (SSPM), Cloud Security Posture Management (CSPM) for Azure, and Centralized Log Management (CLM). These options allow clients to easily obtain such important capabilities with the flip of a switch, fully integrated into the Cynet platform.

MDR Services

Some vendors offer in-house MDR services for an optional fee, others outsource to a third party, and some offer neither of these options. Because many organizations rely on MDR services, ensure the vendor's offering and price point are in line with your budget and expectations. Using the platform providers in-house or outsourced MDR team ensures familiarity with the platform, maximizing effectiveness and efficiency. It's also a boon to resource-constrained teams that rely on outside help to protect their organization.

Cynet Elite and Ultimate packages include comprehensive MDR services at no additional cost. This includes 24x7 monitoring to ensure that no dangerous threats are missed and 24x7 on-demand expert advice and guidance.

Final Thoughts

The MITRE ATT&CK evaluation is a valuable resource that can be used to inform your decision when selecting a security vendor. A top-performing MITRE ATT&CK evaluation indicates a vendor whose solution will perform well in detecting real world threats.

The Cynet 360 AutoXDR platform was a top performer in the 2023 MITRE ATT&CK evaluation. The key is knowing how to get the most out of these resources. We hope you found this guide helpful. If you have any questions or want to learn more about Cynet, let us know. We'd love to chat.

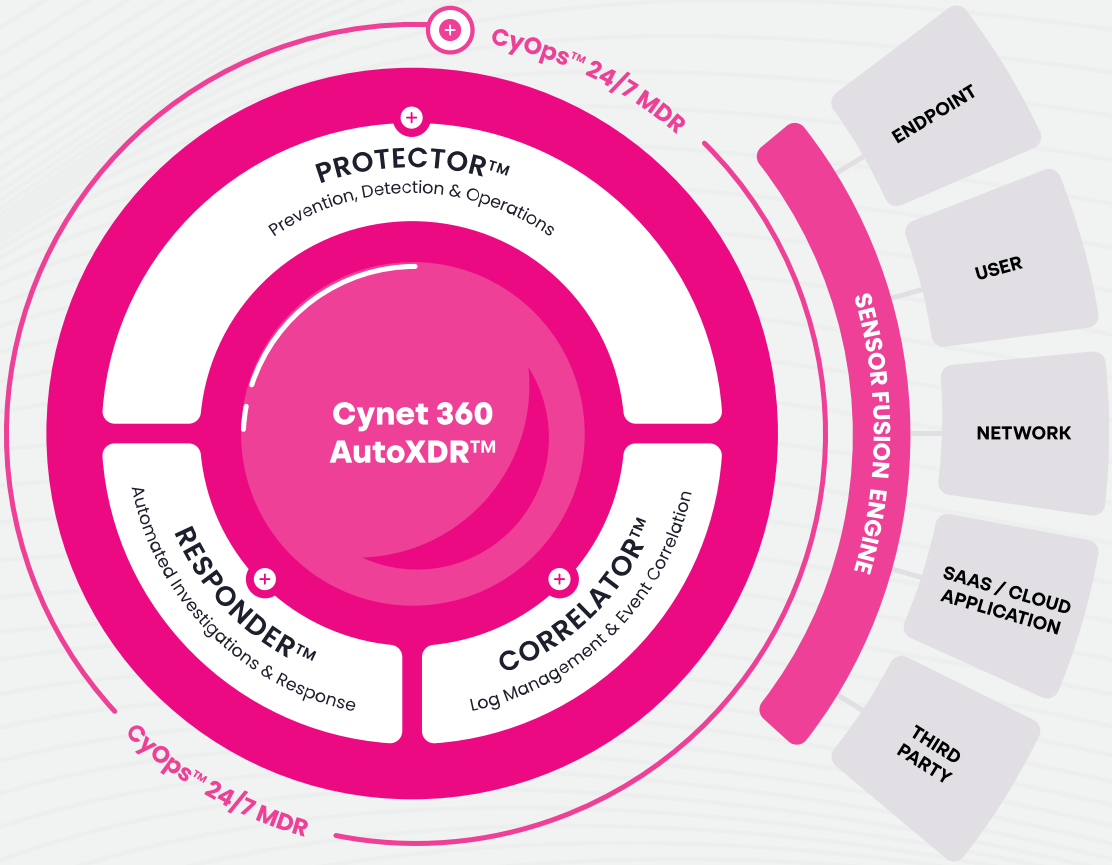
About Cynet

Cynet's end-to-end, natively automated XDR platform, backed by a 24/7 MDR service was purpose-built to enable lean IT security teams to achieve comprehensive and effective protection regardless of their resources, team size or skills.

Cynet delivers the prevention and detection capabilities of EPP, EDR, NDR, Deception, UBA rules and CSPM, together with alert and activity correlation and extensive response automation capabilities.

Our vision is to enable security teams to put their cybersecurity on autopilot and focus their limited resources on managing security rather than operating it.

Bring sanity back to cybersecurity with a fresh approach that makes protecting your organization easy and stress-less.



Learn more

*The views and opinions expressed herein are those of Cynet and do not necessarily reflect the views or positions of any entities they represent. Calculations herein have not been verified by MITRE Engenuity.