WHITE PAPER

From Endpoint Detection and Response to Proactive Cyber Defense with XDR

Using MITRE ATT&CK to Evaluate Security
## Table of Contents

Abstract..........................................................................................................................................3

What is the MITRE ATT&CK Framework.......................................................................................3

MITRE ATT&CK evaluation for Carbanak+FIN7................................................................................3

What Are The Results....................................................................................................................4

Operational Flow............................................................................................................................4

How can decision makers use the MITRE ATT&CK framework?.....................................4

Understanding the evaluation and its limitations........................................................................5

Considerations Beyond the MITRE Evaluation............................................................................5

Response........................................................................................................................................5

Detections beyond EDR................................................................................................................7

Assessing your security posture prior to an incident.................................................................8

Introducing Active XDR................................................................................................................9

Summary.......................................................................................................................................10

References.....................................................................................................................................10
Abstract

Every year, MITRE Engenuity™ publishes an independent evaluation of enterprise cybersecurity products to show how each solution approaches threat detection. The MITRE Engenuity ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Evaluations are focused on each product’s technical ability to address known adversary behavior. The 2020 testing evaluated products against the Carbanak and FIN7 cyber-crime threats. The results are intended to provide a common base that government and industry can use to assess which products will best fit their needs to improve threat detection capabilities to combat modern security threats. These evaluations serve as an important first step in building a secure IT environment. This report will provide an overview of how to use and interpret these results, why they are important, and what else needs to be considered. We will also cover how Fidelis Endpoint®, part of the Fidelis Elevate® Active XDR platform, is ideally suited to help organizations protect themselves from modern threat actors.

What Is the MITRE ATT&CK Framework

The MITRE Engenuity ATT&CK framework is a well-known, widely used knowledge base of cyber adversary tactics, techniques, and procedures (TTPs) based on observations on real world attacks. Referring to the table below, TTPs are:

- **Tactics** (in columns), or stages of an attack, represent the “why” or the short-term tactical goals an adversary is trying to accomplish (e.g., Reconnaissance, Initial Access, Discovery, Lateral Propagation, Exfiltration, and more.)
- **Techniques** (individual cells) represent the means by which the threat actor achieves a tactical objective. These cells provide the details a security defender must detect in order to discover an attack in progress.
- **Procedures** are the detailed information included in the framework on how an adversary would implement the technique to perform a specific tactic to achieve an objective. It includes examples of procedures based on past and known attacks.

MITRE ATT&CK evaluation for Carbanak+FIN7

MITRE Engenuity regularly conducts independent evaluations of enterprise cybersecurity products. The MITRE Engenuity ATT&CK Evaluations use the above framework to evaluate multiple vendors ability to detect known adversary behavior.

In its 2020 testing, MITRE Engenuity evaluated 29 products’ ability to detect the TTPs leveraged by the Carbanak and FIN7 threat group because these financially motivated attacks can impact a wide range of vertical industries.

This framework defines an industry standard lexicon to characterize and categorize the behaviors attackers use throughout the different stages of a cyberattack—from infiltrating the network through exfiltrating data. As such, this framework can be used to map attack techniques and behaviors, discover the root cause of an attack, and minimize dwell time. It also can help determine prevention and remediation options before and after an attack and across endpoints, network, and cloud.

Click here to enlarge and view the interactive website version.
What Are The Results?

By design, there is no “winner” in MITRE Engenuity evaluations. The organization does not provide scores, rankings, or ratings. Instead, it performs a suite of tests to ascertain how each vendor approaches endpoint threat detection in the context of its ATT&CK framework.

Every detection in the evaluation was categorized (e.g., tactic, technique, telemetry, general) to each attack technique. There were a total of 174 unique techniques and sub-techniques tested.

All participating vendors performed well, which is welcome news with the ever-growing threat of cyber criminals and nation state actors. The results provide a common basis that organizations can use to consistently evaluate which products will best fit their individual needs to combat security threats and improve threat detection capabilities.

In the absence of clear ranking and ratings—every vendor will highlight the facet of results that show where they excelled. Fidelis Endpoint detected activity across every attempted adversary tactic and the vast majority of ATT&CK techniques. Out of 20 discrete adversary steps and 174 adversarial sub-steps in the simulated attacks, Fidelis Endpoint detected an indicator a total of 282 times, across all 20 steps, providing extensive coverage across the adversary attack lifecycle.

It is hard to filter through the noise when each vendor claims “100%” victory. Particularly since no single vendor performed the best across all detection categories under measurement. Equally important, not all detection categories should be weighted equally. For example, detection of tactics and techniques are foundational to achieving actionable alerts. Whereas telemetry requires additional correlations by the analyst to get to a point where it is actionable. If your analyst team is less experienced, your weighting of this consideration in the acquisition process may be very different than a more mature security team.

How can decision makers use the MITRE ATT&CK framework?

Security teams should use the framework techniques to influence security implementation designs and monitoring requirements, since many techniques are prevalent across multiple attacks.
For example, techniques common to both Carbanak and FIN7 threat actors are also frequently used by hacktivists, cyber criminals, cyber terrorists, and nation states. Additionally, security teams can proactively adjust or tune their defensive security posture based on in-depth understanding of the specific threat actor objectives that could be targeting their enterprises. It could also be used by security teams to change the aperture of their detection systems to collect additional data on targets of interests.

In an ideal world, enterprise security solutions would provide coverage across all techniques (and sub-techniques) in the MITRE ATT&CK framework. Modern IT environments require a comprehensive set of detection and response capabilities deployed across network, endpoint, and (multi-)cloud to discover and defeat the full spectrum of sophisticated threats. Defending against all adversary techniques may not be practical or economically feasible.

The MITRE ATT&CK framework provides a tool to consistently measure and assess cyber security investment effectiveness based on product utilization, coverage gaps and overlaps, and more. Gaps in coverage across the framework represent residual risk. Understanding the relationship between gaps and threats can inform acquisition and security stack rationalization decisions to improve efficiencies in both technology solutions and operational processes.

MITRE Engenuity evaluations are important basis for endpoint detection abilities. It is important that results of this assessment be considered within the broader context of an overall enterprise cyber defense strategy to help a security team to understand their full ability to defend threats, reduce duplicity, and close gaps in coverage.

Understanding the evaluation and its limitations
In building a comprehensive cyber defense strategy, organizations must properly identify all known and unknown attacks to neutralize them before they can impact business operations. At the same time, it is impossible for one single test to evaluate a full cyber-security environment including every threat, every TTP, across every threat vector. Understand the scope (and limitations) of each evaluation.

The MITRE Evaluations focus on endpoint detections and the ability to tag detections with the appropriate tactics and techniques for two known attack sequences (FIN7 and Carbanak).

But not every behavior that matches a technique in the framework is malicious. (This may cause false positives in your environment.) For example, “file deletion” is listed as a technique under Defense Evasion. The challenge now lies in how to distinguish normal file deletes from an attacker deleting files to evade detection. In practice, this requires your solution to not only detect an issue, but also to correlate data across multiple techniques to determine whether the behavior is malicious, then to create high confidence alerts to automatically respond or allow the analyst to act with confidence.

Attackers do not follow a precise recipe. Tactics provide the general goal of each step in the attack, but adversaries will not use them all. Instead, they implement the tactics and techniques that help them most quickly accomplish their objective. In reviewing the MITRE ATT&CK Evaluation results, consider:

• Did the vendor detect every major step and every tactic? Where were the gaps?
• Within the detected techniques, which are unique to malicious activities and therefore particularly important to consider?
• If a technique also occurs as part of normal business processes (e.g., file deletion), does a detection lead to an increased workload or does it aid in defense?
• Can you map detections to the MITRE ATT&CK framework to easily identify the sequencing of the attack over many steps and tactics?
• Can you detect and respond early enough to block the attack before damage is done?

Considerations Beyond the MITRE Evaluation
Evaluation results provide a starting point to analyze a security posture; however, that is just the beginning. The framework includes more than one hundred observed attack patterns to consider, including Carbanak and Fin7. Let’s pivot to additional considerations as you define your cyber-defense strategy, including response; detection beyond the endpoint; and assessing your security posture prior to an incident.

Response
Detection and response go hand-in-hand. Without detection, there is no response. Response plays a critical role in stopping threat actors before they achieve their mission. There are many flavors of detection and response – Endpoint (EDR), Network (NDR) and now XDR or eXtended Detection and Response, which extends detection and response more broadly across IT environments.

Early detection and response can stop an attack and prevent damage to your business. Responses can be manual or automated, but any response must be thorough. An improper response may not be effective. Worse, an ineffective response can alert the attacker that their efforts have been detected, forcing them to change techniques that may go undetected. Fidelis considers robust response to be based on several criteria:
Prevention: One form of response is prevention; however, response and prevention should not be confused. Endpoint prevention (or anti-virus software) can block a file from being installed or from running and works best on known malware. A strong prevention technique should prevent 99% of attacks. It is the other 1%, as well as attacks not based on malware, that cause the most significant damage. Response needs to cover the known, unknown, and attacks not driven by malware.

Scope: The system must be able to provide the full scope of the attack as well as historical data to determine the infiltration path and lateral propagation. Data needs to provide all details of the detections, including process behaviors, process owners, and impact. Without this data, a proper response may not be possible. Ask:

- Does the system provide enough data to scope the attack and gain insight into the attacker’s motives?
- Is the attack concentrated on a single person or widespread?
- Is the attack based on malware, phishing, known exploits, or unknown “zero-day” vulnerabilities?

Completeness: Is the response robust enough to cover investigation, correction, and restoration. For instance, Fidelis Endpoint ships with hundreds of script resources for Windows, Linux, and Mac responses to cover these dimensions. Next, does the system allow simple expansion by the import of scripts from the enterprise administrators or user community. Fidelis allows virtually any response.

Automated: SOC teams are over-whelmed. When possible, automate the response. Can you create automated playbooks that allow administrators to craft responses according to prescribed enterprise indecent response procedures? With early-stage detection, it may be necessary to:

- First investigate providing essential data to the detections.
- Isolate the endpoint to cut off lateral propagation.
- Remove files, rewrite registries, rollback the system or one of many other potential responses.

Graphic 1. Fidelis Endpoint live console
Organizations should be prepared for any situation with an incident response plan. Viewing a detection as a stand-alone event creates extra work for the security team.

The MITRE ATT&CK framework can help guide a security team’s decisions based on which stage a response is desired and how early the response should be taken using observed detections. Automated playbooks can greatly improve efficiency by automatically taking those first steps, based on a detection pattern, to let software do the work.

**Manual:** When an automated response is not possible, enable an easy manual response. Whether the correct playbook is not yet in place, or a security team needs a faster response to a real time issue, there are times that require a “live console” that the team can immediately access a system and take the appropriate response—deleting files, killing processes, changing system firewall settings, removing user accounts, uninstalling software, installing, or upgrading systems, and much more.

The Fidelis Endpoint live console (see Graphic 1), for instance, provides a file view, a process view, and a console on the endpoint operating system with privileged access. Response can be done on a live system before or after isolating it from the network. The fastest response sometimes requires live access—as if the system were confiscated—without requiring an action that slows response.

**Flexible:** Detection is not limited to endpoints. Security teams must have flexibility to detect and respond using any system and in any environment. It can help to identify techniques over email, DNS, networks, and decoys, for example. Each of these detections may require a response on the network or endpoint. Playbooks and manual response should be available for any such detection and not be limited to endpoint alone.

**Detections beyond EDR**

When push comes to shove, what we want to do is detect any attack that has made its way through our defenses before it can damage our environment. The endpoint is one detection point. There are other points of detection that should equally be considered and used—either by preference and/or by necessity.

To illustrate this point, let's look at the MITRE ATT&CK tactics and techniques, where detecting an issue prior to the endpoint may make more sense:

**Initial access** includes many techniques to infiltrate an enterprise. The techniques include phishing, spear phishing, drive by malware, and others. Many of these techniques involve tricking the end user to click a link, visit a site, respond to a phish and more. When humans (aka, users) are involved, anything is possible—even with the most robust training regiment, people can make mistakes. It only takes one mistake for an adversary to be effective. If possible, it is better to detect and block these techniques using email and network visibility and coverage against potential threats that may emanate from such angles.

**Lateral movement** includes techniques to move from one infected host to another where more valuable or essential information resides. Lateral propagation techniques can be detected by internal network analysis, blocking the attacker from advancing. When detected by an endpoint, blocking lateral propagation involves detecting a process as it executes, hoping to detect and block early enough to thwart the attack. When the same techniques are detected using an NDR solution, you prevent lateral movement before they execute. This can lead to endpoint quarantine for further analysis and a better overall response.

**Command and Control techniques** are methods for an attacker to communicate from an infected host to their control center. NDR solutions are very successful in detecting and blocking such communications and effectively cutting off an attack in progress. EDR solutions can also be effective, but like lateral propagation, EDR must detect while a process is running, then race time to block communication. Better would be to block with NDR and then trace the connection to its origin or source and determine the cause of the connection attempt.

**Exfiltration** is often the last stage of the threat. The attacker has infiltrated the enterprise, moved laterally to identify the assets to steal, and coordinated the threat through command and control. Exfiltration is often the end game. It is at this point where the cost to the enterprise escalates exponentially because damage has been done. In most cases, exfiltration is performed over the network, and a strong NDR solution can be extremely effective, especially when it incorporates DLP capabilities to block data exfiltration. Fidelis is one of the few NDR solutions that includes DLP.

**Deception** plays a role throughout the ATT&CK framework. When an attacker is blocked, they will search for alternative techniques to achieve their tactic. When you deploy Deception technologies, the attacker will be coerced into carrying on with their techniques, not realizing that they are engaging with a decoy rather than an actual enterprise device. This becomes interesting for two reasons:

- Observe the interactions with a decoy. Typically, there are no interactions with a decoy in a business use cases, which means any activity involving a decoy is an indication of the attacker’s motives. SOC teams can use this information to threat hunt in the enterprise for similar activity on real assets where the activity may be obfuscated within normal daily operations. The security team can also capture the...
tool used by the attacker when they install it on a decoy. Capturing tools plus further analysis also provide sources for threat hunting. Decoys become an excellent source of detections in this sense.

- Deception provides an alternative to blocking a process or network connection. Instead, deception routes the connections to a decoy. Lateral propagation and command and control tactics are two strong examples where a decoy can become an effective response both blocking the attack and enabling teams to observe next steps.

EDR solutions can be effective detection and response solutions. Fidelis Endpoint is a great solution as demonstrated in the most recent MITRE ATT&CK results. As illustrated in the use cases above, there are also use cases where email, NDR, and Deception solutions—like those offered by Fidelis Cybersecurity—may be more efficient and less error prone.

At the same time, there are situations where EDR is not an option whatsoever.

- Legacy systems running an operating system not supported by EDR;
- IoT devices where endpoints cannot be deployed; and
- The proliferation of applications and services where the security team lacks control, such as mobile devices, cloud services, remote workers, BYOD, and more.

In every enterprise, there are unmanaged devices. It would be naive and irresponsible to rely solely on EDR or endpoint detections in most enterprises.

Assessing your security posture prior to an incident

When a threat detection is made, the security team begins its race to identify the threat and respond in adequate time. Often, these security teams are inundated with detections—or suffering from “alert fatigue”. They have so many alerts that they are having trouble staying on top of or triaging alerts to come close to effectively stop threats. This gives an attacker a distinct advantage.

To alleviate that advantage, security solutions must offer a method to understand and assess the full enterprise IT security posture. Solutions should help security teams think like an attacker and constantly assess the posture to identify weaknesses and patch those weaknesses before racing through the threat detection and response cycle. By focusing solely on detection of tactics and techniques, you may miss the need and ability to wholly assess your environment.

Make sure your security solutions allow your team to:

- Fully understand the IT landscape. You cannot defend what you can’t see. You must quickly identify and classify all IT assets and connections—even in dynamic multi-cloud environments—and be able to monitor assets without missing unmanaged systems, shadow IT, and other systems that cannot support an EDR agent.
- Determine communication paths both internal and external to the enterprise. Even a Zero Trust architecture does not replace a security teams’ need to understand and confirm proper configuration and detect unknown communication
paths that attackers can exploit. Make sure to understand:
  - Which devices can reach other devices.
  - Lateral propagation paths. Internal and external communications.

* Evaluate enterprise risk. Risk is not a static situation, but something that changes with every phish, every malware, every exploit attempt, every detection of every tactic and technique. Risk changes with every response to detections. There are several risk factors that require ongoing attention:
  - State of the asset (vulnerabilities, user behavior, anomalies).
  - Coverage of the asset (protection by EDR, NDR, email, deception, etc.).
  - Threat detections (attempts to infiltrate or exploit systems should raise the risk to the organization).
  - Importance of an asset (the asset type and the user can raise or lower importance).

If the security team has a complete understanding of the attack surface and constantly evolving risk, then the response can fortify any discovered weaknesses. Fidelis cyber terrain mapping (see Graphic 2) provides holistic, contextual visibility of the entire IT environment.

The security team does not need to be passive and wait for attack detections which launch a race against the clock to defeat everyone. Instead, they can be proactive, which can create a more efficient team that spends less time triaging alerts and more time fortifying the enterprise.

**Introducing Active XDR**

As discussed previously, the MITRE ATT&CK framework presents a map of known attacker tactics and techniques. This framework is developed from the viewpoint of the attacker and outlines the major steps required to accomplish their goal. To level the playing field with the adversary, MITRE has created a similar framework—MITRE Engage—which lists applicable use cases from the defender’s perspective. MITRE Engage outlines how defenders can take a proactive cyber defense approach, where the security team can engage adversaries early to respond faster.

Fidelis Elevate is aligned with both the MITRE ATT&CK and MITRE Engage frameworks. This Active XDR platform takes XDR a step further by natively integrating deception technologies with classic detection and response for endpoint (EDR), network (NDR), and cloud. Fidelis Elevate has been purpose-built for proactive cyber defense strategies to focus on engaging with and defeating adversaries earlier in the attack lifecycle. It uses telemetry and integrated deception technologies to re-shape the network attack surface, while providing SOC teams the whole picture of where attacks are on the network and how to respond to them.

**When comparing XDR offerings, make sure your solution can:**

- Detect threat activity using multiple means: EDR, NDR, and Deception are the key methods of detection.
- Map all detections to the MITRE ATT&CK tactics and techniques and provide a map of the attacker’s tracks.
- Use correlation across multiple alerts to prioritize alert response. Responses can include either EDR scripts or manual intervention, as well as network packet loss, email quarantining, web page redirection, and diversion of network traffic to decoy networks, among others.
- Include Deception as a key element to enable a proactive cyber defense. Deception allows the security team to place decoys in the environment and automatically change the network to move the decoys.
- Identify all assets and network connections across the environment, including those without endpoint security protection.
- Provide risk assessment that combines assets, vulnerabilities, threat detection, security coverage, and importance.
- Store metadata for all network and endpoint process behaviors. With data, detections can be investigated, threat hunting can occur, and you can leverage new information to ascertain whether past events constitute a threat.
- Within the context of the MITRE ATT&CK evaluations, endpoint detections are the only criteria. However, for more holistic and proactive defense, endpoint is simply one piece of a proactive cyber defense platform.
Summary
Fidelis Elevate includes an EDR solution that has been proven effective by the most recent MITRE Engenuity assessment. This Active XDR solution delivers the critical capabilities described in this paper and helps users engage adversaries earlier in the attack lifecycle. Fidelis Elevate includes:

- **Fidelis Endpoint**, an EDR solution, tested effective in the Carbanak and FIN7 MITRE Engenuity evaluation. The solution detected every tactic and every major step in the attacks. The solution provides response in automated and manual methods, including forensic abilities.

- **Fidelis Deception**, an automated decoy environment. Any IT or OT system can be built as a decoy with capabilities to add decoys in Active Directory and to create breadcrumbs as lures to push attackers to the decoys.

- **Fidelis Network**, an NDR solution, provides threat and DLP detections over network ports and protocols, with specific solutions for email and web traffic. Fidelis Network provides response in the form of packet drops, email quarantine, and web page redirection.

- **Fidelis Sandbox** is used to analyze files and URLs found at endpoints, networks, and decoys.

- **Sophisticated machine learning** to detect threats and anomalies from data derived from any component of the solution.

Learn more about Fidelis Elevate XDR

References

“MITRE ENGENUITY ATT&CK Evaluations”, MITRE, 2020

“MITRE ENGENUITY ATT&CK Evaluations” results.

“An Introduction to Extended Detection and Response”, Fidelis Cybersecurity Blog, March 2021

“Preparing for the Next ‘Big Attack”, Fidelis Cybersecurity Blog, March 2021

“How to Use MITRE ATT&CK for Deception Missions”, Fidelis Cybersecurity Blog, May 2020

About Fidelis Cybersecurity
Fidelis Cybersecurity, the industry innovator in proactive cyber defense solutions, safeguards modern IT environments with unparalleled detection, deception, response, cloud security, and compliance capabilities. We offer full visibility across hybrid environments via deep, dynamic visibility and asset discovery, multi-faceted context and risk assessment. These features help minimize attackable surface areas, automate exposure prevention, threat detection, and incident response, and provide the context, accuracy, speed, and portability security professionals need to find and neutralize adversaries earlier in the attack lifecycle. With Fidelis, organizations emerge stronger and more secure. Fidelis is trusted by many top commercial, enterprise, and government agencies worldwide. For more information, please visit [www.fidelissecurity.com](http://www.fidelissecurity.com).

Copyright © 2021 Fidelis Cybersecurity®. Inc. All rights reserved.