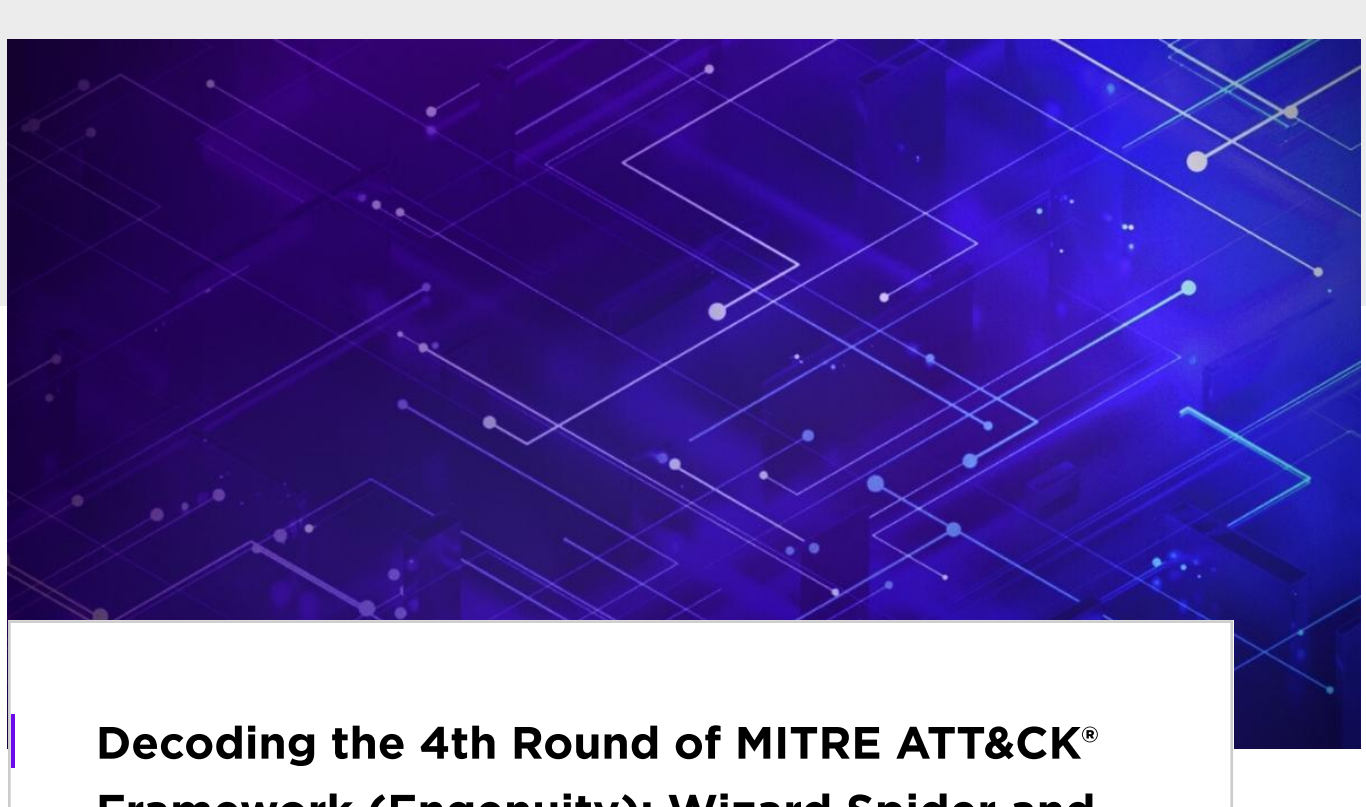
SentinelOne blog

GET A DEMO



Decoding the 4th Round of MITRE ATT&CK® Framework (Engenuity): Wizard Spider and Sandworm Enterprise Evaluations

March 22, 2022
by Resha Chheda

The next round of MITRE Engenuity ATT&CK evaluation results is around the corner, and the participating vendors everywhere are starting to ramp up the marketing machine to create a noise about it. MITRE Engenuity is clear that they don't declare a "winner" and do not assign overall scores, rankings, or ratings to the vendors or their cybersecurity technology. Instead, they're very transparent assessments of all the detections a given security solution has produced for different stages of a specific adversary's attacks and present the evaluation results based on four separate but related categories of visibility and detection.

Coinciding with the published results is a barrage of various vendor positioning blogs and PR that claim the "win", making the results hard to navigate and understand. All the positioning among vendors does not help security teams get what they really need: information on leveraging the results to advance their security objectives.

In this post, we explain what you need to know about the latest MITRE Engenuity ATT&CK evaluation, what that evaluation means to your business, and how you can implement it to better understand and use the security tools at your disposal.

The ATT&CK Framework

MITRE has become the common language of EDR and is the *de facto* way to evaluate a product's ability to provide actionable information to the SOC. For three years now, MITRE Engenuity has conducted independent evaluations of cybersecurity products to help the industry and government institutions make better decisions to combat security threats and improve their threat detection capabilities. Leveraging the ATT&CK framework, evaluations assess various vendors on their ability to automatically detect and respond to real-life cyberattacks within the context of the ATT&CK framework.

MITRE Engenuity ATT&CK Enterprise 4 Testing

The latest round of evaluations is called 'Enterprise 4' evaluations. Through the lens of the MITRE ATT&CK ®knowledge base, MITRE Engenuity focused on two threat actors, Wizard Spider and Sandworm, for this Enterprise 4 Evaluation. These two threat actors were chosen based on their complexity, relevancy to the market, and how well MITRE Engenuity's staff can fittingly emulate the adversary.

- Wizard Spider is a financially motivated criminal group that has been conducting ransomware campaigns since August 2018 against a variety of organizations, ranging from major corporations to hospitals.
- Sandworm is a destructive Russian threat group that is known for carrying out notable attacks such as the 2015 and 2016 targeting of Ukrainian electrical companies and 2017's NotPetya attacks.

The Evals team chose to emulate two threat groups that abuse the Data Encrypted For Impact (T1486) technique. In Wizard Spider's case, they have leveraged data encryption for ransomware, including the widely known Ryuk malware (S0446). Sandworm, on the other hand, leveraged encryption for the destruction of data, perhaps most notably with their NotPetya malware (S0368) that disguised itself as ransomware. While the common thread to this year's evaluations is "Data Encrypted for Impact," both groups have substantial reporting on a broad range of post-exploitation tradecraft.

Technique Scope for Enterprise 4 Evaluations

Learn More: Technique Scope

Starting with the Wizard Spider and Sandworm evaluations, each substep will have a single detection category that represents the highest level of context provided to the analyst across all detections for that substep. If a vendor is awarded 'technique', which is the highest context within the Detection category, they will not be able to also claim 'tactic', 'general', or any other detections. This helps deobfuscate and simplify vendor assertions of the 'number detections' they received.

This round of evaluations also has Protection evaluation, which was introduced in the last evaluation to determine a vendor's ability to block key techniques and tactics rather than just identifying and logging them. The ability to detect malicious activity is important but blocking is often preferred, given the sophistication of today's cyber threats and recognition that 100% prevention over an extended period of time is unsustainable.

Implementing MITRE Engenuity ATT&CK Evaluations to Advance Your Organization's Security Objectives

The ATT&CK framework brings a common lexicon to stakeholders, cyber defenders, and vendors, helping us to apply intelligence to cybersecurity operations. CISOs and security teams can use the following ATT&CK framework best practices to improve their security posture.

1. Plan a Cyber Security Strategy

Use ATT&CK to plan your cyber security strategy. Build your defenses to counter the techniques known to be used against your type of organization and equip yourself with security monitoring to detect evidence of ATT&CK techniques in your network.

2. Run Adversary Emulation Plans

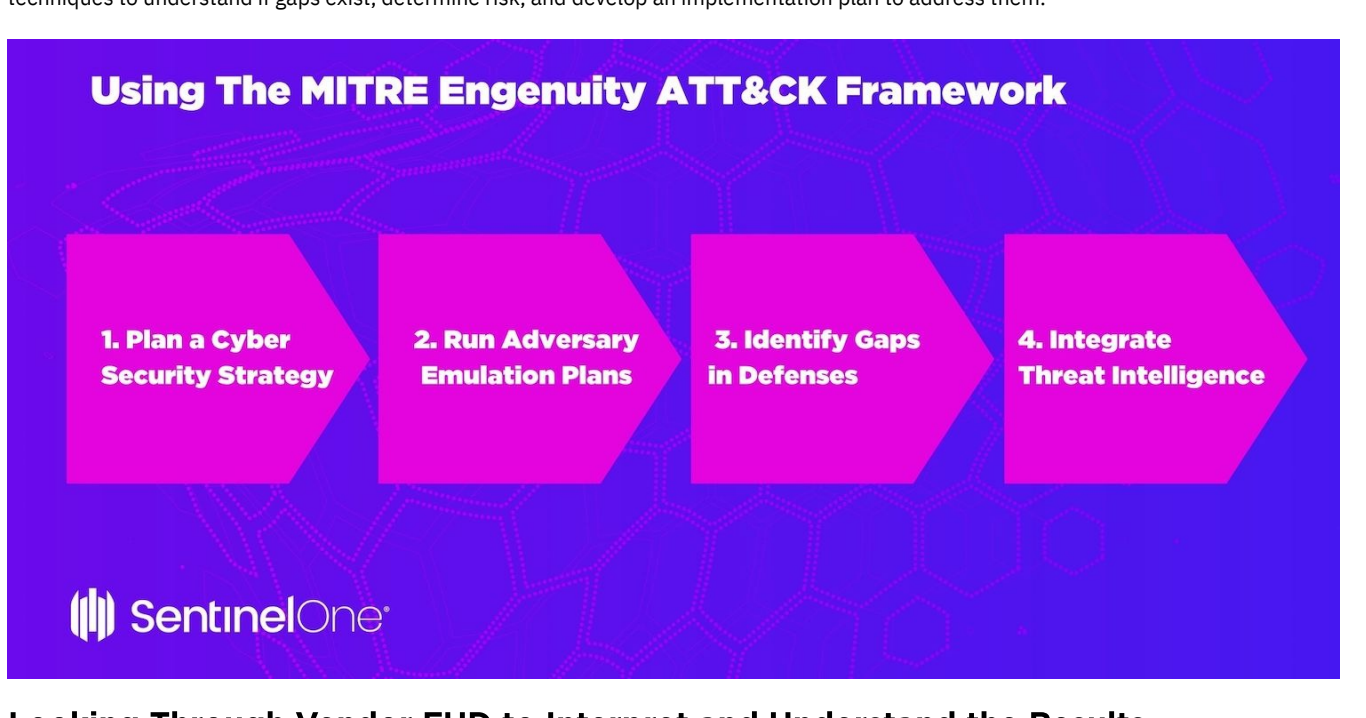
Use ATT&CK for Adversary Emulation Plans to improve Red team performance. Red teams can develop and deploy a consistent and highly organized approach to defining the tactics and techniques of specific threats, then logically assess their environment to see if the defenses work as expected.

3. Identify Gaps in Defenses

ATT&CK matrices can help Blue teams better understand the components of a potential or ongoing cyber attack to identify gaps in defenses and implement solutions for those gaps. ATT&CK documents suggested remediations and compensating controls for the techniques to which you are more prone.

4. Integrate Threat Intelligence

ATT&CK can effectively integrate your threat intelligence into cyber defense operations. Threats can be mapped to the specific attacker techniques to understand if gaps exist, determine risk, and develop an implementation plan to address them.



Looking Through Vendor FUD to Interpret and Understand the Results

A pragmatic approach to the data will help you cut through the hype and make informed decisions about your organization's security. MITRE Engenuity is clear that they don't declare a "winner" and do not assign overall scores, rankings, or ratings to the vendors or their cybersecurity technology. Instead, they're very transparent and present the evaluation results based on four separate but related, categories of visibility and detection so other organizations may provide their analysis and interpretation. This is preferable over heavily creative statistics derived from the data in an effort to present vendor products in a favorable light. We've seen some interesting claims being made relative to the ATT&CK Evals that are dubious, at best. Rather than focus on them, here's our perspective on some of the solution capabilities you should focus on.

- **Visibility Is The Foundation To Any Superior EDR & XDR Solutions**

  The foundation of an outstanding EDR & XDR solution lies in its ability to consume and correlate data at scale in an economic way by harnessing the power of the cloud. Every piece of pertinent data should be captured—with few to no misses—to provide the breadth of visibility for the SecOps team. Data, specifically capturing all events, is the building block of EDR and should be considered table stakes and a key MITRE Engenuity metric.

- **Automated Context and Correlation is Critical in Understanding the Compete Attack Story**

  Correlation is the process of building relationships among atomic data points. Preferably, correlation is performed by the machine and at machine speed, so an analyst doesn't have to manually stitch data together and waste precious time. Furthermore, this correlation should be accessible in its original context for long periods of time in case it's needed.

- **Alert Consolidation Is Critical in Helping Unburden the SOC Teams**

  More signal, less noise is a challenge for the SOC and modern IR teams who face information overload. Rather than getting alerted on every piece of telemetry within an incident and fatiguing the already-burdened SOC team, ensure that the solution automatically groups data points into consolidated alerts. Ideally, a solution can correlate related activity into unified alerts to provide campaign-level insight. This reduces the amount of manual effort needed, helps with alert fatigue, and significantly lowers the skillset barrier of responding to alerts. All of this leads to better outcomes for the SOC in the form of shorter containment times and an overall reduction in response times.

- **Delays in Detecting Alerts Can Prove Deadly Allowing Adversaries to Maximize Material Damage**

  Time is a critical factor whether you're detecting an attack or neutralizing it. You need to ask yourself how much of your data can be exfiltrated in an hour? A delayed detection during the evaluation often means that an EDR solution requires a human analyst to manually confirm suspicious activity due to the inability of the solution to do so on its own. The solution typically needs to send data to the analyst team or third-party services such as sandboxes, which in turn analyzes the data and alerts the customer, if required. However, many critical parts of this process are done manually, resulting in a window of opportunity for the adversary to do real damage. Adversaries operating at high speed must be countered with machine speed automation that's not subject to the inherent slowness of humans.

Looking Ahead

At SentinelOne, we continue to be enthusiastic supporters for the work MITRE Engenuity is doing to painstakingly define and continually expand a common cybersecurity language that describes how adversaries operate. This matters to you because ATT&CK Evaluations is a unifier and a force multiplier for the people on security's front line who work tirelessly defending their infrastructure and assets from unscrupulous adversaries looking to turn a quick buck, wreak havoc, or steal a life's work.

We are excited to announce the details of SentinelOne's participation in the Fourth Round of MITRE Engenuity ATT&CK® Enterprise Evaluations, and we will be posting the results when available. In the meantime, if you'd like to learn more about how the SentinelOne Singularity platform can help your organization achieve these goals, contact us for more information, request a free demo or register for the MITRE Evaluations webinar below.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Best-of-Breed Identity Threat Detection and Response Meets Best-of-Breed XDR
- SentinelOne's Cybersecurity Predictions 2023 | What's Next?
- Dealing with Cyberattacks | A Survival Guide for C-Levels & IT Owners
- Apple's macOS Ventura | 7 New Security Changes to Be Aware Of
- Bringing Identity to the Era of XDR
- SentinelOne Debuts at the Top of MITRE Engenuity ATT&CK® Deception Evaluation. See Why.