Organizing the Hunt for Cyber Threats with MITRE ATT&CK

MITRE's framework helps security teams uncover gaps and map defenses against known attack behaviors, tactics, and techniques by providing insight into attacker behaviors.

Keeping track of and defending against the evolving nature of cyber threats is a challenge for security teams large and small. For many organizations, the strategy has shifted from trying to bar all cyber interlopers outside the network perimeter to—assuming that bad actors will find ways to infiltrate networks—instead having security teams focus on detection and mitigation. That's easier said than done, of course; in many cases, organizations rely on multiple security tools that can result in defensive gaps.

Responding to a high volume of alarms and addressing high-priority Indicators of Compromise (IOCs) can leave little time left for strategy and improving the overall security environment. And a lack of resources and growing specialization within security organizations may hinder sharing and understanding of threat intelligence and how it can be applied to testing defenses and mitigating attacks. A more strategic approach is to uncover potential threats by better understanding attacker behaviors, tactics, and techniques. This understanding can then be used to build stronger defenses and identify gaps that attackers may try to exploit.

UNDERSTANDING ATTACKER BEHAVIORS

Many organizations are targets of threat actors—sometimes individuals, but increasingly malicious groups and criminal gangs comprising highly skilled professional cyber attackers. Larger organizations, such as military contractors and financial services companies, are often subject to Advanced Persistent Threats (APTs) that are aligned with or under the direction of nation-states or commercial entities.

Analysis of known attacker behavior can be instrumental in determining the source of a threat, mitigating attacks in progress, and identifying gaps in cyber defenses. Behavior patterns that have been identified as preceding attacks elsewhere can provide an early warning that an attack is likely.

Threat actors use various means for gaining access to networks, including social engineering such as spear phishing, propagating stolen and valid credentials, exploiting vulnerabilities in public-facing applications, and compromising supply chain and partner networks.

Once in the network, attackers can take advantage of multiple techniques and switch among them at different stages or navigate around newly erected defenses. They will try to evade defenders, escalate privileges to gain access to critical assets, execute code that exfiltrates data or conducts other actions, move laterally through the network, harvest for credentials, or take command and control of key assets.

Sophisticated threat actors, such as APT groups or other skilled threat groups aiming to harvest information or exploit financial systems, typically attempt to hide their malicious activity if their objective is data theft. Thus, the longer they are hidden, the more they will be able to steal. While the APT is active, the threat actor may be spying on activity, stealing classified or proprietary files, reading emails, or even co-opting the target network to perpetuate surreptitious Distributed Denial-of-Service (DDoS) attacks against other entities.

Other threat actors may not necessarily care about staying hidden over a longer term because their goal is extortion, as was the case with the WannaCry and NotPetya ransomware attacks, or because they seek to maximize the visibility of the disruptions they create.

Understanding the Tactics, Techniques, and Procedures (TTPs) of attacks may reveal the identity of an actual or potential threat actor. That is key to understanding the motivation and goals of particular attackers. The MITRE ATT&CK framework, developed by MITRE Corporation, a not-for-profit organization that operates federally funded research-and-development centers, aids security teams in understanding adversarial behaviors by categorizing common cyberattack strategies and tactics.

ATT&CK (an acronym for Adversarial Tactics, Techniques, and Common Knowledge) structures comprehensive information on attacker tactics and techniques in a manner that can provide better insights into threat intelligence, reveal gaps and weaknesses in security, and develop better detection and mitigation controls. Organizations can leverage that growing knowledge base to emulate adversary attacks and investigate intrusion detection preparedness.

HARNESSING INFORMATION ON THREATS

The growing number of threat actors and the increasing volume and evolution of indicators present a significant challenge for Security Operations Centers (SOCs), analysts, and network administrators. As cyberattacks have proliferated, organizations have become inundated with data and information on incidents and threats. In addition to using information generated by Security Information and Event Management Systems (SIEMs), many organizations try to absorb external intelligence information, with the goal of keeping up to date on threat activity.

However, the amount of information available can be overwhelming, making it difficult to operationalize. Constantly responding to false-positive IOCs leads to fatigue, increasing the likelihood that teams will miss an actual attack event. Growing specialization and the lack of standard shared terminology can result in gaps in understanding the nature and seriousness of looming threats.

MITRE ATT&CK adds structure to intelligence information by mapping the data on tactics and techniques of known and unknown threat actors. Standardizing the description of adversarial activity increases understanding of adversarial behaviors and methods across organizations as well as specializations.

ATT&CK was initially developed by MITRE to systematically categorize adversarial behavior in its Fort Meade Experiment (FMX) research environment. It is now available as a globally accessible

knowledge base organized around a set of three matrices. SOCs and analysts can utilize the framework to analyze threats and attacks, and to organize "red team" attack simulations and "blue team" defense exercises.

Actors can be tracked through associations to techniques in ATT&CK that they have been known to utilize. This gives defenders a potential roadmap to potentially determine the strengths and weaknesses of their defenses. Some threat actors target particular industries, and ATT&CK provides information that can be instrumental in anticipating potential future attacks.

WHAT ATT&CK BRINGS TO THE CYBER BATTLE

Cyber threat analysts are often fully occupied by analyzing and reporting on the latest in threat intelligence and reacting to the volumes of organizational data on potential malicious activity indicators. ATT&CK helps shift analysts' perspective from low-level indicators to overarching attacker behaviors. With empirically documented threat activity, security teams can gain insight into the motives and norms behind attacker behaviors, anticipate potential attacks, and possibly identify actual attackers.

MITRE ATT&CK tracks more than 70 threat groups and the tactics and techniques that each has been publicly identified as using. Three matrices provide a visualization of the techniques and tactics that attackers use when interacting with target systems, providing an easy way for analysts to drill down to the relevant information in the ATT&CK knowledge base:

- **The ATT&CK Enterprise matrix applies to Windows, Linux, and/or macOS systems**
- **ATT&CK Mobile applies to mobile-specific domains**
- **PRE-ATT&CK relates to what attackers do before they try to exploit a particular target network or system**

PRE-ATT&CK and ATT&CK Enterprise combine to form a full list of tactics that roughly align with the Cyber Kill Chain, Lockheed Martin's methodology that defines the steps used by cyber attackers: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. PRE-ATT&CK aligns mostly with the reconnaissance, weaponization, and delivery phases, whereas ATT&CK Enterprise aligns well with the final four phases.

"The framework helps to very quickly identify gaps in defenses and figure out what other security solutions may be needed to fill those gaps," says Nicholas Hayden, Senior Director, Threat Intelligence, at Anomali. "The gap analysis really helps to understand where you can get the most return on investment and make decisions based on how existing or potential security solutions overlay the framework."

Information in the matrices is structured in columns that cover attacker tactics—what they are trying to achieve—mapped to cells in the matrix that describe the individual techniques they may use to accomplish those steps or goals.

ATT&CK provides SOCs with a common language for describing malicious behavior. According to MITRE, ATT&CK takes on the perspective of an adversary in its terminology and descriptions, providing context that makes it easier to understand actions and potential countermeasures. Organizations can utilize the framework to:

- ✔ **Align controls with techniques**
- ✔ **Catalog defensive controls**
- ✔ **Categorize defenses**
- ✔ **Develop better detection and prevention**
- ✔ **Identify defense gaps to provide insight into spending needs**

OPERATIONALIZING ATT&CK

Studies indicate that the average length of time between a breach and its detection is about 200 days (according to 2016 data); during that time, SIEM log data could generate millions of IOCs—many of them false-positives—representing an amount of data few organizations could analyze in a timely manner. The challenge for most organizations is to identify IOCs that are relevant to current attack behaviors so that a SOC staff can respond by mitigating attacks in progress or bolstering defenses against attacks that other organizations may be experiencing.

ATT&CK provides the structure to prioritize threats and create a foundation for more effective penetration testing and detection. With the common terminology and matrix structure of ATT&CK, Red Team penetration testers and Blue Team defenders can constantly test against a full range of real-world tactics and techniques and improve understanding of gaps and limitations in existing defenses.

Hayden recommends that organizations start with ATT&CK Enterprise. "As their use matures, they can implement PRE-ATT&CK, which is really threat intelligence, to identify emerging threats before they happen," he says. "If they have a bring your own device (BYOD) environment they will want to start considering ATT&CK Mobile."

CONCLUSION

MITRE ATT&CK is quickly gaining support and generating excitement in the threat intelligence community. ATT&CK can be utilized to map defenses and understand gaps in protection. Attackers can be tracked through associations with techniques and tactics known to ATT&CK that they have been known to utilize. This gives defenders a roadmap to apply against their operational controls to see where they have weaknesses that make them vulnerable to certain actors and where they have strengths.

ATT&CK also provides a way to describe new techniques as they develop so that organizations can stay informed, update controls, and continually simulate, hunt for, and detect threats based on the latest information. In an era when quickly multiplying and evolving threats can overwhelm both the proactive and reactive capabilities of an organization, ATT&CK helps strengthen defenses by anticipating how attacks will unfold so you can strategize your response.

To learn more about how your organization can implement the framework, go to What Is MITRE ATT&CK and How Is It Useful.

LEARNING MORE ABOUT ATT&CK

ATT&CK, initially developed in 2010, was released publicly in 2013. MITRE periodically updates the matrices, drawing on community insight and feedback, and new information on tactics and techniques. Over the past few years, many best practices, open source tools, and other resources have become available.

BEST PRACTICES:

Everyone gains by sharing information on threat intelligence, new and modified attack tactics and techniques, and how best to utilize and improve existing tools to better mitigate and improve defenses against attacks:

- Follow and internalize external research on detection and mitigation
- Share discovered methods with the larger community
- Leverage ATT&CK in existing tools where possible
- Encourage vendors and service providers to add support for ATT&CK in their tools and services

RESOURCES:

- MITRE ATT&CK blog on Medium
- Presentations made at the ATT&CKcon conference
- Anomali Weekly Threat Briefing

TOOLS:

- MITRE ATT&CK Navigator, a simple-to-use open source web application that provides basic navigation and annotation of the three ATT&CK matrices to visualize defensive coverage and likely attacks
- Caldera, MITRE's automated adversary emulation system for testing endpoint security solutions and assessing network security posture
- Metta, an open source tool from Uber for basic adversarial simulation
- Red Team Automation (RTA), a framework of scripts from Endgame designed to enable blue teams to test their detection capabilities
- Atomic Red Team, a testing framework from Red Canary enabling defenders to simulate specific attack behaviors