HOW TO USE

MITRE ATT&CK™

MARK DUFRESNE

Protections Team Lead, Elastic Security

"So...are we good?"

That is the final question of many meetings on cybersecurity between C-level executives and their cybersecurity teams. Whether the meeting resulted from a board-level panic at the latest breach headline, a proactive strategy to secure proprietary data and critical systems, a regulatory mandate, or something else, the core question remains the same: "Are we good?"

ARE WE GOOD?

This question should give a security team pause. Where do they begin to explain the complexities and nuances of the risks posed by cyber threats? What does "good" mean to an analyst, SOC manager, or CISO? The executive often only wants a yes or no. She may not have the time to pick apart anything more complicated.

The same question hovers around proof of concept evaluations for new cybersecurity solutions. As independent antivirus vendor testing often reports results with mere tenths of a percent separating the top solutions by only testing a fraction of the possible attack surface (exploits, malware, and not much more), finding a material difference to justify a purchase decision becomes a challenge. Will the new solution bring a "yes" to the question: "Are we good?" Teams cannot afford to wait for a real-world deployment to get the answer.

Many are turning to MITRE ATT&CK™ to better understand threats in their unique environments to know how "good" their existing security infrastructure may be.

SO WHAT IS ATT&CK™?

ATT&CK began more than six years ago as an internal project at MITRE that has since expanded into a large open project with hundreds of detailed entries on discrete attacker techniques. It is based on real research and observations of intrusion activity and helps provide a common language to describe the techniques adversaries use. ATT&CK is routinely updated as our collective understanding of the threat landscape evolves.

There are only so many ways in which an adversary can achieve a particular objective on a system. ATT&CK is the language we can use to describe these methods. Unlike previous attempts at frameworks like this, ATT&CK does not deal in generalizations. Every framework needs to be simplified on some level, but when reduced too much it provides no actionable information.

ATT&CK is detailed enough for cyber defenders to turn a high-level goal such as: "I should find post-compromise activity on my network," into an itemized system of achievable checkpoints. For example, an analyst's goal

MITRE ATT&CK™ MATRIX

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITS Jobs	Cloud Instance Metadata API	Cloud Service Dashboard	Component Object Model and Distributed COM	Data from Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Bypass User Account Control	Credential Dumping	Cloud Service Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command History	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compile After Delivery	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data Staged	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Email Collection	Fallback Channels	Transfer Data to Cloud Account	Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Firmware	Hooking	Password Policy Discovery	Remote File Copy	Input Capture	Multi-hop Proxy		Resource Hijacking

See full matrix here

may be: “Gather data and analytics that allow me to find unusual scheduled tasks on my Windows endpoints.” Each enumerated cell in the corresponding topic’s ATT&CK matrix provides an identified threat type, tactic, or technique that the analyst can then reference against his unique security infrastructure to ensure his Windows endpoints are secure.

ATT&CK matrices exist for the following security domains:

- **Enterprise: Techniques threat actors use to access and operate on Windows, Mac, and Linux systems**
- **Cloud: Tactics and techniques used on cloud platforms, including AWS, GCP, Azure, Office 365, Azure AD, and SaaS**
- **Mobile: Techniques used on iOS and Android devices**
- **Pre-ATT&CK: Activities threat groups may undertake during targeting, technical development, and attack staging activities**
- **ICS: Techniques that may be used in operations targeting industrial control systems**

SOMETHING FOR EVERYONE

ATT&CK is first and foremost a knowledge base, albeit one that can be overwhelming at first. Even individuals following the latest cybersecurity trends may find themselves intimidated by the large wall of techniques in ATT&CK.

The references and explanations provided by MITRE are a big help, but it does take a rather deep well of security knowledge to understand each technique in full detail. The key to success for using ATT&CK is in understanding what you can get out of it. If used properly, it can help frontline security practitioners, managers, vendors, and security teams of all sizes and maturity levels.

Today’s products need to assume that breaches will indeed occur, and that defenses must provide detection and visibility beyond the traditional areas of malware and exploit protection to account for this reality. Vendors can reference

WHO USES ATT&CK™?

01 MATURE (SOC) TEAMS

Experienced cybersecurity teams can use it to coarsely measure their ability to see and respond to techniques used by attackers. Understanding coverage — or lack thereof — can help provide teams with a list of items to consider when seeking to improve detections.

02 RISING SECURITY TEAMS

Teams that are just developing their security policies and establishing themselves within an organization’s IT infrastructure can use ATT&CK as a place to start. Rather than trying to tackle all of ATT&CK at once, it is advisable to pick a few key techniques to gain visibility into and defend against. There are also many open source software options available to automate basic Red Team actions based on ATT&CK.

03 MANAGERS AND BUSINESS LEADERS

While comprehension of the nuances of security may vary amongst management, managers are now increasingly responsible for ensuring the protection of critical systems. ATT&CK can help with the difficult tasks of measuring security investments and highlighting cyber risk areas. Understanding ATT&CK will help decision makers understand the qualitative importance of security initiatives and improvements to visibility. Using ATT&CK as a quantitative measuring stick for defenses and investment can have pitfalls — more on that later.

04 SECURITY VENDORS

Lately, the cybersecurity industry has had a hard time demonstrating to customers the difference between products. Marketing all starts to sound alike, with vendors using the same ‘next-gen, AI-powered, 99% effective’ language to describe products. ATT&CK presents an opportunity to help educate customers during the evaluation process and beyond.

ATT&CK mappings to more effectively describe specifically how their products enable protection across the adversary lifecycle — and further educate and enable users through integrations with ATT&CK.

POTENTIAL PITFALLS

For all its benefits, ATT&CK is not all-powerful. Organizations that treat it as such could end up with a false sense of security and misallocation of resources. Every framework has limitations because, as previously mentioned, frameworks are all simplifications of the real world. Organizations that hope to use ATT&CK to improve their security postures must be aware of, and prepared to address, items that fall outside those limits.

The first thing to consider is that ATT&CK is an ever-expanding database that is by no means complete. While it is the most comprehensive taxonomy of hacker techniques currently available, it will not cover everything — in part because of the boundless nature of cybersecurity. Hackers, whether white or black hat, are developing new techniques and strategies so quickly that it is impossible for something like ATT&CK to keep up in real time. Even with MITRE's clear top positioning as the go-to framework and its collaborative approach to gathering and incorporating techniques observed by the security community, it takes time for MITRE to add new cells or update existing ones in response to the discovery of new techniques.

ATT&CK also does not provide a comprehensive account of every possible variation of a given technique. For example, there are several different ways adversaries can achieve a technique like process injection. Adding visibility and monitoring for a single process injection technique does not mean you can answer "Are we good?" with a firm "Yes." MITRE is in the process of addressing this well-known drawback through the introduction of sub-techniques to its matrices. This makes things more granular in some respects, but practitioners will still be behind the cutting edge of adversary tradecraft; adding further details to existing techniques could lead to an overwhelming and counterproductive ATT&CK matrix. MITRE has a difficult balance to strike between completeness and usability.

We should note that ATT&CK coverage is not the place to start when rolling out an effective security program. Even if it was absolutely complete and usable, it does not replace a foundational cybersecurity strategy. The very first step begins before even looking at ATT&CK. Organizations in the early stages of building up their security processes first need to ensure they have good hygiene. Some questions you should consider internally are:

- **Do we have a strong password management system in place?**
- **Are we regularly applying patches to our systems?**
- **Can we see and stop common malware?**
- **Do we have sufficient data sources to succeed with ATT&CK?**

Only once a strong foundation for security is in place does it make sense to reference ATT&CK, as sophistication is necessary in taking actions based on its matrices. As we've mentioned a couple times, ATT&CK is largely intended as a knowledge base of adversarial techniques, and must be treated as such. The resources required to extend low false positive rate coverage across every cell are enormous, and efforts to do so will come with diminishing returns.

In reality, if a security team were to be alerted every time a technique in ATT&CK was detected on an endpoint or on the network, they would be flooded with alerts every time a user compressed a file or every time an admin ran Powershell on an endpoint. After all, there is significant overlap between attacker techniques, operating system functionality, and normal IT operations. Extensive tuning and detection engineering is needed to get to high confidence, low noise detections. Many techniques should rarely, if ever, alert. They should instead be used as contextual indicators towards higher confidence alerts. Teams need to understand what is right for alerting in their environment. They should understand which ATT&CK matrix cells are more about visibility into techniques to ensure the ability to hunt proactively and further enrich other security alerts.

We'll dive deeper into this later.

Even once a team has come up with a good detection, there are issues with what type of coverage exists. Much of ATT&CK can be dealt with via command line monitoring: See a process execute with certain arguments and alert. But what if the attacker renames the tool you are monitoring for? Suddenly your analytic may fail if *wscript.exe* becomes *nothingtoseehere.exe*. Or, what if PowerShell can be used to do the exact same thing? What if native APIs can be called and you lack visibility? There tend to be numerous holes in analytics created by teams new to ATT&CK. Holes are nearly unavoidable — even for advanced teams — because analytics are based on data, and most teams are stuck with insufficient data visibility.

A summary point based on the last few ideas we've covered is that there isn't yet an agreed-upon methodology for using ATT&CK as a measuring stick. Matrix cells have varying levels of granularity and many undefined subtechniques, so blind spots do exist. Alerting is appropriate in some networks but not others depending on the normal benign baseline. Good research and discussion on this is taking place and progress will be made, but we still have a general question of "What is good coverage?"

ATTRIBUTION

One of the more compelling features of ATT&CK is its listing of known adversaries and hacking groups cross-referenced with techniques they've used in the past. It may be tempting to use ATT&CK as a shortcut for attribution or a way to reliably find threat groups you believe are targeting your systems, but the truth is that cyber attack attribution is far too complex to be solved so simply — especially with adversaries actively changing behaviors and tooling to avoid detection. It is helpful to see what attack chains have been used in the past, but publicly available information on past attacks is fragmentary at best. Even if it were perfectly accurate, past information is neither a reliable way to predict what an adversary will do in the future, nor a good way of attributing a series of observed actions to a specific group.

If organizations cannot use ATT&CK as a checklist for their security programs, by the same token they should avoid relying on it as a compliance standard for security. ATT&CK should not solely drive any product purchase decision or other security investment. Users of ATT&CK must be prepared to have nuanced conversations about how to use its matrices to drive both visibility and detection initiatives with the understanding that quantifying subsequent results may land somewhere between inconsistent and misleading. Users must also look to ATT&CK as a resource to better understand and contextualize observed behavior, rather than as a way to catch all bad activity.

DEVELOPING A PLAN

Once you understand the challenges and possible missteps one can make in using MITRE ATT&CK, it's time to start thinking about what to do with it. Its primary utilities are based in understanding the taxonomy of adversary techniques and then building up corresponding detection programs designed to discover when those techniques are being used in your environment through a combination of alerting and hunting. Easy, right?

A key concept when operationalizing ATT&CK is visibility. Visibility is a word we hear commonly in security, and for good reason. You can't stop an adversary that you don't know is there. Visibility is about ensuring security teams can see into systems and collecting the right information they need to prevent, detect, and respond to threats. This sounds straightforward in concept, but the practice is much more complicated given the millions or even billions of events happening on endpoints and on the network in a given day. You need to worry about what data to gather, how to gather it, and where to put it.

Organizations that will benefit most from ATT&CK are ones that already have some level of maturity in their cybersecurity processes. Yet early-stage security teams can benefit from using ATT&CK to help them decide where to begin building in monitoring and protections — most often starting with a data availability assessment. For these teams, iterative improvements are the way to go — incrementally

expanding visibility and, where appropriate, detections.

Users just getting started need not be intimidated by the hundreds of entries in the matrix, but rather pick a few key techniques on which to focus. A good place to start is somewhere between five and ten techniques associated with relevant threats to the organization. Collect the data, get the data to a place where it can be worked with, ensure that the data can be queried, and potentially generate alerts based on the data. We usually recommend starting with simple techniques wherein significant progress can be made with only command line logging — for example, a subset of the 'Discovery' techniques. Taking a look at results, teams can start asking questions like:

- **Where are there gaps in my visibility?**
- **How often does this occur in my environment?**
- **Can I associate this with a legitimate business process?**
- **What is the relative normalcy of the associated user or host?**

Not every technique should generate an alert. This is so important that it merits mentioning again. Don't produce a scorecard of alerting coverage across ATT&CK and assume that maximum coverage is best. This issue arises because some techniques in ATT&CK are based on abuse of legitimate features — features that may be entirely normal and commonly leveraged in your enterprise. Periodic hunts will be far more appropriate in these cases where there's significant overlap between the technique and your normal baseline.

Knowledge is key in security, and ATT&CK is the best knowledge base we have about adversary actions. Security personnel at all stages of their career development can use the matrix as a training tool to learn more about attacker tradecraft and why it is important. Improving knowledge of techniques in the adversarial arsenal will help analysts studying the matrix to be better at their job and better prepared to identify and respond to a technique when it shows up in their environment.

ATT&CK can also be a useful tool for security evaluations. It cannot replace a penetration test or a dedicated Red Team, but it can help teams with some quick-and-dirty assessments. Several software projects, including Caldera from MITRE and Atomic Red Team from Red Canary, can generate real data on endpoints corresponding to ATT&CK techniques. These automation frameworks can be effective ways of making sure that a new logging feature or security tool has the visibility the organization needs, or that data streams are properly calibrated to alert security teams when they occur. ATT&CK can also be useful in driving collaborative "Purple Team" exercises, where the Red and Blue Teams work together to more dynamically test defenses. Purple Team exercises can be oriented to a narrowed set of ATT&CK techniques.

And finally, ATT&CK can help guide security teams to have specific and intelligent conversations with business leaders about the state of the organization's cybersecurity posture. ATT&CK is a common language that organizational leadership can use to improve their ability to communicate with budget and risk owners about changes in people, process, and technology that are necessary to reduce risk and exposure to adversaries. The matrix provides a concrete framework to show where the organization has good visibility protections, where there is a gap in coverage, and how investments can lead to improvements in those problem areas.

ELASTIC TOOLS AND ANALYTICS FOR MITRE ATT&CK

Open source Elastic Logstash and Beats are two pre-built solutions that provide a wide variety of ingestion types. Logstash is a server-side data processing pipeline that can ingest from a multitude of sources simultaneously. Beats is a collection of lightweight, single-purpose data shippers that can send data from thousands of machines and systems. Both ingestors ship to Elasticsearch for additional data normalization and powerful search functionality for security functions ranging from threat hunting to SIEM. With this

technology, a security team can achieve extensive visibility without the need for an expensive traditional vendor solution.

Analysts need to be able to search their security data. Elasticsearch is well-known in the security community for its speed, scalability, vast applications (security and otherwise), and vibrant open source community. Elasticsearch also works well towards the visibility goal we have in mind. Elastic Common Schema (ECS) is a specification that provides a consistent and customizable way to structure your data in Elasticsearch, facilitating the analysis of data from diverse sources. Whether your team needs to perform interactive analysis (e.g., search, drill-down and pivoting, visualization) or automated analysis (e.g., alerting, machine learning-driven anomaly detection), it needs to be able to uniformly examine the data. To streamline and strengthen the practitioner experience, Elastic SIEM can process data normalized through ECS to provide an interactive workspace for event triage and investigations.

Further visibility and capability can be achieved with the Elastic Endpoint Protection product. This product features the deepest visibility into security data, full EQL capabilities (more on that shortly) and the ability for users to turn ATT&CK queries into real-time preventions on the endpoint via Reflex™.

Good coverage comes from unified data analysis, simplified analyst workflows, and ready communication and collaboration between different members of the security team. The Event Query Language (EQL) is an extensible language built in-house at Elastic to express relationships between security-relevant events. Advantages of EQL include schema independence, an OS-agnostic framework, support for multi-event behaviors through sequences, and threat hunting readiness through data stack pipes built into the language. EQL powers the ATT&CK-oriented search and detection experience in the Elastic Endpoint Security product and will soon come as a core feature in the Elastic stack. To learn more about the language and updates, please visit the EQL documentation or visit the accompanying EQL Analytics Library.

EQL enables practitioners to reinforce their defensive posture, in part because it affords them a robust approach to detecting attacker behaviors (i.e. using sequences to associate different event types). For instance, malware droppers will create files and immediately execute, so analysts should primitively look for a creation file event and process execution (they could also further investigate that file being subsequently deleted). Or, even more simply, perhaps they'll want to look for suspicious events generated from an inbound email.

EQL also allows users to share hunt queries seamlessly with one another. For instance, with the abundance of "living-off-the-land" techniques, wherein attackers use native OS tools to conduct their operations, practitioners are hunting for anomalous usage of these applications like Microsoft PowerShell. Using EQL, threat hunters can easily look for all unique PowerShell commands in one simple command using data pipes.

IN CONCLUSION

The cybersecurity world is moving at a rapid pace and adversaries are always coming up with new tactics to achieve their goals. Frameworks like MITRE ATT&CK — while not catch-all guidelines for previously mentioned reasons — are essential to developing stronger cybersecurity programs. As breach headlines continue to cross business leaders' desks, the C-level will continue to turn to their security teams and ask: "Are we good?" With proper consideration and utilization of ATT&CK, security team leaders will be able to provide more insight into the strengths and weaknesses of their security program to ideally be able to respond: **"For now."**

If you'd like to learn more about the prevention, collection, detection, and response capabilities of Elastic Security, visit: elastic.co/security.

