cybereason

FIVE CLEAR STEPS TO ENHANCE SECOPS WITH MITRE ATT&CK_

DANIELLE WOOD
SENIOR DIRECTOR, SECURITY SERVICES
CYBEREASON

ALLIE MELLEN
SECURITY STRATEGIST,
CYBEREASON

TABLE OF CONTENTS

EXECUTIVE SUMMARY

A skyrocketing numbers of alerts, limited security talent, and millions of new malware strains daily has made security a seemingly insurmountable task. Simply buying another security tool doesn't make it easier; adversary groups are constantly evolving, putting pressure on security teams to anticipate adversary advancements in smarter and more human ways. This white paper establishes a process that empowers SecOps to improve iteratively over time by leveraging their existing talent and tools.

KEY TAKEAWAYS

01. Implementing MITRE ATT&CK takes five simple steps that easily integrate with any security strategy:
    - **Step 1: Establish Inputs**
    - **Step 2: Create an Adversary Emulation Plan**
    - **Step 3: Run an Attack Simulation**
    - **Step 4: Alert, Hunt, and Report**
    - **Step 5: Process and Technology Improvement**
02. With these five steps, you can continuously tune your security strategy and leverage the connection between techniques, tactics, and procedures, adversary emulation plans, and real-world adversary groups.
03. Use these steps to align your blue and red teams around a common goal: securing your environment against real adversaries.

RECOMMENDATIONS

01. Use MITRE ATT&CK to emulate adversaries known to target your industry.
02. Refresh your AEPs and run new simulations at least annually. Adversary groups change their techniques and tactics regularly, and your defense should reflect that.
03. Report in detail on the results of your AEPs so your security team can not only improve detection, but also prevention and threat hunting capabilities.

INTRODUCTION

Before the MITRE ATT&CK framework was publicly released in 2015, security teams used multiple frameworks to develop an effective security strategy: ISO-17799, its successor ISO-27000, Cobit, NIST, and others. These frameworks are an analytical approach to defense, lacking the realistic testing and process improvements SecOps has needed for some time.

MITRE ATT&CK fills this gap with a knowledge base of real-life adversaries and their processes. It gives a foundational understanding of adversaries that security teams can leverage to improve their defense against real-world attacks. In this paper, we extend MITRE ATT&CK by outlining five steps you can take to implement MITRE ATT&CK and enhance your defense.

WHAT IS MITRE ATT&CK?

MITRE's Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) is a model and knowledge base of adversary behavior. It catalogs the attack lifecycle of different adversaries and the platforms they choose to target, all based on real-world observations. ATT&CK is not a static framework, and is updated quarterly with new adversaries, tactics, techniques, and other information supplied by security vendors and organizations around the world.

Since its public release, MITRE ATT&CK has become a staple of the endpoint security space. As of this writing, ATT&CK has built a community for sharing techniques, a yearly conference called ATT&CKCon, adversary emulation plans, evaluations for security vendors, and various tools to interface with ATT&CK.

In this paper, we explain how to use two of MITRE ATT&CK's most important components to develop a continuously improving defense: techniques, tactics, and procedures, and adversary emulation plans.

WHAT ARE TACTICS, TECHNIQUES, AND PROCEDURES?

Long before their use in cybersecurity, tactics, techniques, and procedures (TTPs) were used to describe military operations within the United States Department of Defense. Like much military terminology, TTPs are aptly used in cybersecurity, as they describe the processes and profile of a specific adversary.

ATT&CK that allows for tangible, real world improvement in detection capabilities.

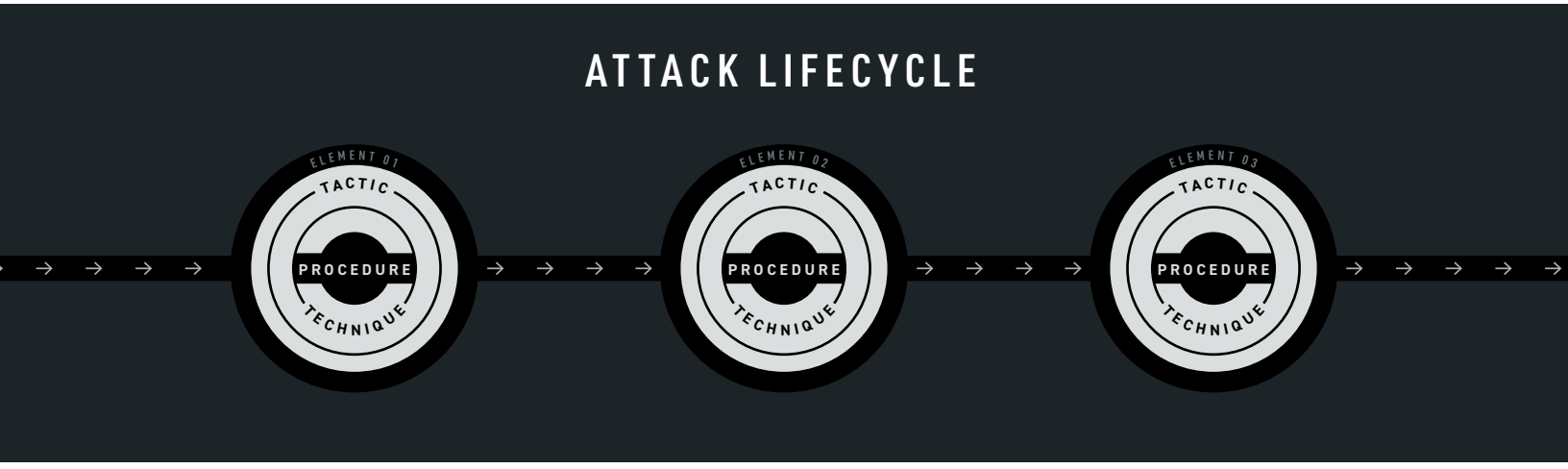


Figure 01: A representation of how techniques, tactics, and procedures can be represented as part of the attack lifecycle.

TACTIC

A tactic is a high-level description of part of the attack lifecycle with limited details on how the adversary explicitly carries out an activity. For example, MITRE ATT&CK lists twelve different enterprise tactics attackers may use across their attack lifecycle, like initial access (TA0001), persistence (TA0003), command and control (TA0011), and exfiltration (TA0010).

TECHNIQUE

A technique is the middle ground between high-level considerations of tactics and specific details of procedures. Within each tactic are a list of techniques that adversaries may use to accomplish the goal of the tactic. For example, some MITRE ATT&CK techniques can be used for initial access (TA0001), including a drive-by compromise (T1189), spearphishing via service (T1194), or a supply chain compromise (T1195).

PROCEDURE

A procedure is the specific details of how an adversary carries out a technique to achieve a tactic. For example, MITRE ATT&CK lists how APT19 (G0073) uses a watering hole attack to perform a drive-by compromise (T1189) and gain initial access (TA0001) of forbes.com in 2014.

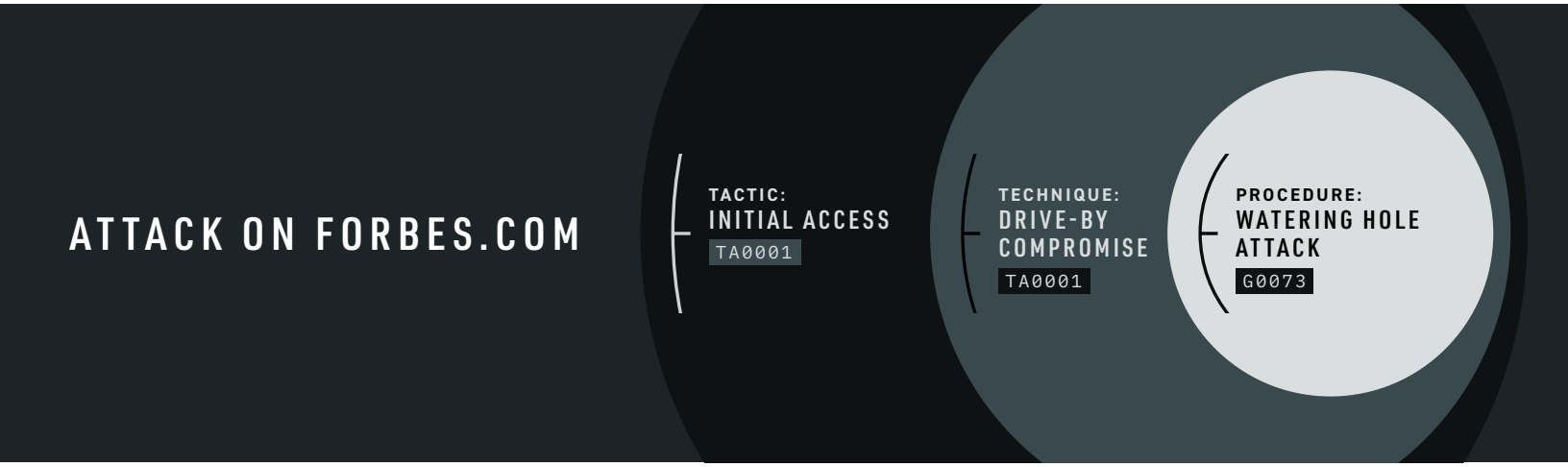


Figure 02: A representation of how techniques, tactics, and procedures for APT19's attack on forbes.com can be represented.

TTPs give vendors, analysts, and everyone in between a common vocabulary around which to consistently communicate methods of an attack.

WHAT ARE ADVERSARY EMULATION PLANS?

Adversary emulation plans (AEPs) are the way to model adversary behavior based on a particular set of TTPs in MITRE ATT&CK. For example, MITRE has created an AEP for APT3 to showcase exactly how APT3 compromises a system and exfiltrates sensitive information. Security teams use AEPs to create attack simulations based on specific adversaries to test their defense.

Though AEPs are especially important when testing and building a strong defense, they are often overlooked for TTPs by security practitioners versed in the "trench warfare" of day-to-day security operations. Though TTPs are useful in their own right, they are much more effective when coupled with AEPs.

In fact, our team finds that AEPs are the most important feature when constructing an effective operational security effort tailored to your business. **While TTPs may change, the general process of bringing TTPs together into a real-world attack simulation whose efficacy can be measured is the real gem.** AEPs bring TTPs into a measurable attack simulation based on a specific, real-world adversary for specific, real-world improvements.

USING AEPS IN THE REAL WORLD: ATTACK SIMULATIONS

Your red team can use AEPs to develop an attack simulation and execute it against your enterprise security infrastructure. These simulations leverage real-world attacks so you can identify and tune gaps in your defense before the actual adversary strikes. They also help reduce your security team load and give them greater visibility into their environment.

For the most significant results, turn this process into a monthly or yearly activity to consistently strengthen and tune your defense over time.

DIVING DEEPER INTO MITRE ATT&CK

CHOOSING THE RIGHT TARGETS

MITRE ATT&CK has threat intelligence on almost eighty different adversaries, from the techniques they use to the industries they target. To get the most out of your AEP, prioritize simulating adversaries you are most likely to face in real life.

For example, a healthcare organization may model an adversary like Deep Panda (MITRE ATT&CK ID G0009), since they are well-known for targeting healthcare companies like Anthem. This same thinking can be applied to all the adversary groups across industries.

ADVERSARY GROUP	INDUSTRY TARGET
APT 19	FINANCE
Deep Panda	HEALTHCARE
menuPass	MANUFACTURING
APT 19	LEGAL
OilRig	OIL AND GAS
Turla	HIGHER EDUCATION
BRONZE BUTLER	GOVERNMENT
Dragonfly 2.0	CRITICAL INFRASTRUCTURE

Table 01: Example adversaries and the industries they target.

To make things easier, you can search for an industry within the MITRE ATT&CK website and immediately see which adversaries are known to target it.

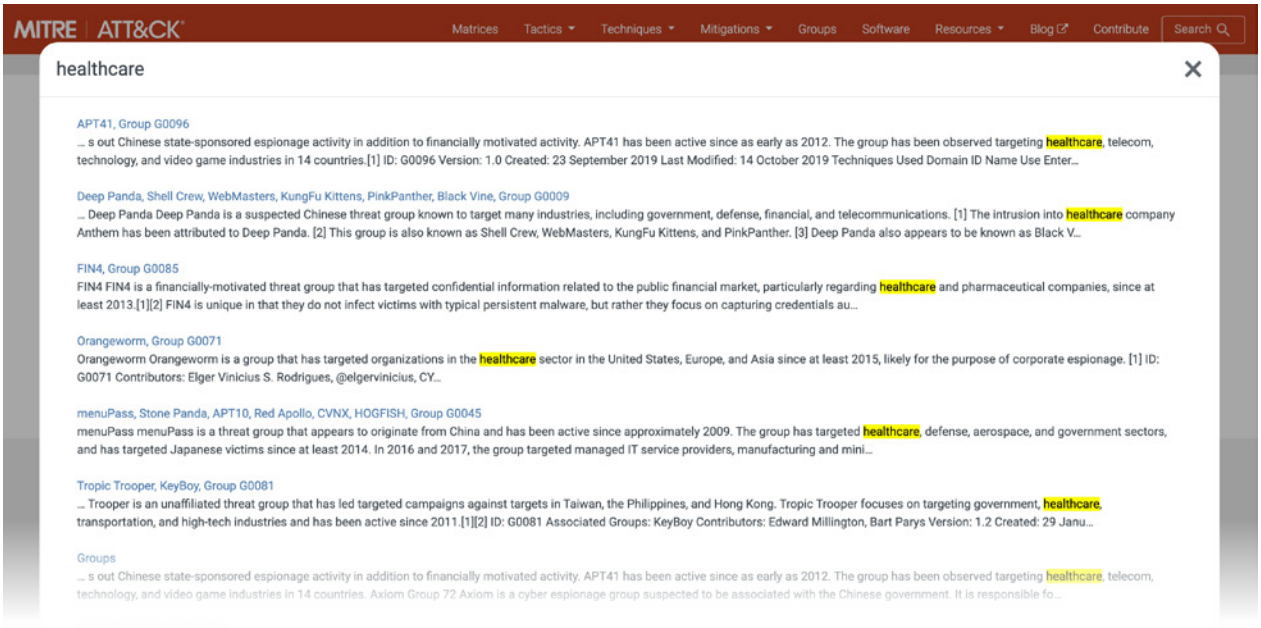


Figure 03: Searching the MITRE ATT&CK website for adversary groups known to target healthcare companies.

WHY NOT DETECT EVERY TTP IN ATT&CK?

You can argue that, if you can detect all the **TTPs** in ATT&CK, you should also be able to defend against all of the **adversaries** in ATT&CK. While technically true, many TTPs are not inherently malicious.

For example, Account Discovery (T1087) could be any of 33 different actions, including ones as benign as running *"net user/domain"*. If you were to alert every time *"net user/domain"* occurred, you'd drown SecOps in false positives. There are many TTPs in ATT&CK that, when used legitimately, are benign.

It's important to strike a balance between alerting on every TTP and maintaining SecOps efficiency. By alerting on every TTP in ATT&CK without context, your team will inevitably suffer from alert fatigue, until they ultimately tune out certain alerts and miss actual attacks.

To address this, low fidelity alerts should be used only in context, such as who ran the process, what its parent process was, whether remote access was involved, and other factors that can be used to identify if a TTP is part of an attack or just benign behavior.

The low fidelity example "alert me when *net user/domain* is run" put in context becomes this higher fidelity alert, "alert me when *net user/domain* is run by a non-shell process or by a domain user under a shell whose parent tree doesn't contain explorer when that user is not a member of domain admins."

> A chain of TTPs that tie malicious activity together is known as an Indicator of Behavior, which we discuss in the Threat Intel section below. This is contrasted by AEPs, which are a full document of the TTPs used by a specific adversary group.

Instead of alerting on every TTP in ATT&CK, a more effective approach is to test your environment against a fully developed attack simulation that takes into account the TTPs of an attack. The attack simulation gives your team actionable feedback on where you may need additional logging or where you should add new policies and technologies.

Now that we are up to speed on MITRE ATT&CK, let's dig into the five steps you should use to consistently improve your defense with MITRE ATT&CK: establish inputs, create an AEP, run an attack simulation, hunt and report on threats, and perform alert maintenance.

FIVE CLEAR STEPS TO IMPLEMENT MITRE ATT&CK

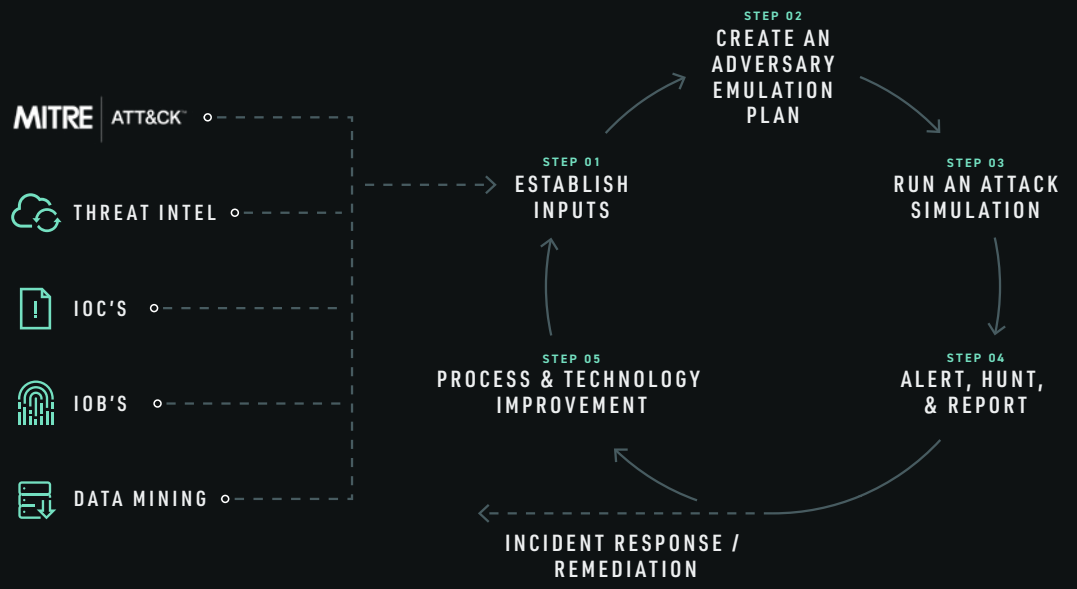


Figure 04: The Process Through Which the Five Steps Continuously Improve Defense

You can use these five steps to leverage MITRE ATT&CK in your security operations and create a simple, repeatable process to tune your enterprise security over time. In fact, this process should be a staple of your security toolkit that is used regularly, as adversary groups change TTPs over time.

Let's break down each of these steps in more detail.

STEP 1: ESTABLISH INPUTS

Before identifying an adversary to target, always start by identifying what inputs you have available. Though MITRE ATT&CK gives a good basis of knowledge and input, it's important to expand your inputs to other areas to give you a more complete and timely perspective. MITRE ATT&CK is highly curated, with eighty different adversary groups available that are only updated once a quarter. We don't want to build in blind spots to our security process by excluding more recent data or adversaries.

Additionally, more traditional feeds will inform your red team and empower your blue team to make more effective defense decisions.

INCORPORATING THREAT INTEL

Incorporating outside threat intelligence into your security process is a best practice with or without these five steps. It helps you keep your defenses up-to-date based on the latest intel from the community, and gives you a basis to validate and classify attacks you are seeing.

For example, you may use outside threat intel to simulate attacks like NotPetya, WannaCry, or many other popular campaigns you want to prevent. Moreover, threat intel can inform your team and help them make connections between attacks they are seeing and popular adversaries.

If you make these connections and attribute a new campaign to a particular adversary, you can contribute to MITRE ATT&CK directly to help the community through ATT&CK Sightings.

INDICATORS OF COMPROMISE

Most threat intelligence is shared as Indicators of Compromise (IOCs), or artifacts on a system or network that signal malicious activity. IOCs are the fingerprints left behind at the crime scene of a cyberattack. They are a static input, and are often identified as file hashes, IP addresses, domain names, or other information in the environment.

AN IOC AS A CONCRETE PIECE OF THREAT INTELLIGENCE LOOKS LIKE THIS:

```
Adversary IP Address: 100.35.197.249
```

IN JULY 2019, the Cybereason Nocturnus team uncovered a new threat group, Operation Soft Cell. This group is a state-sponsored threat group that leverages global telecommunications providers to target high-value individuals. We mapped the multi-year attack to MITRE ATT&CK and contributed our findings to MITRE ATT&CK so others could defend against it in the future.

Antivirus software looks at file attributes such as the file hash, function calls or embedded code sections. If it finds a match, it prevents the associated process from running. IOCs help identify and prevent adversary attacks based on the unique signature of the malware, C2 server, or other tools attackers may be using. For example, you may wish to flag unique hashes associated with a specific adversary group to give greater context to your alerts.

IOCs are valuable when preventing known malware, but over 350,000 new strains of malware are detected every day, and fileless malware attacks are on the rise. IOCs are no longer an innovative or sufficient standalone method for defense.

INDICATORS OF BEHAVIOR

Indicators of Behavior (IOBs), on the other hand, describe the approach an attack takes. IOBs are the witness at a crime scene of a cyberattack. They couldn't necessarily see the adversaries face, but they saw what the adversary did. IOBs are the set of behaviors, independent of tools or artifacts, that describe an attack, and can be very useful when building an AEP and attack simulation.

A HIGH LEVEL IOB LOOKS SOMETHING LIKE THIS:

- **Initial access by phishing attachment with malicious Microsoft Word document attached.**
- **Subsequent payloads downloaded by a malicious macro within the Word document executing commands to leverage PowerShell and create persistence via a scheduled task.**

AN IOB AS A CONCRETE PIECE OF THREAT INTELLIGENCE LOOKS LIKE THIS:

- **T1193 Spear Phishing Attachment (Microsoft Word) -> T1093 Shell Process (PowerShell) -> T1407 External Connection -> T1053 Child Process (Create Scheduled Task)**

IOBs report on malicious behavior, which is a more contextualized approach to describing an attack. Admittedly, IOBs can vary: some will be specific down to a procedural description, while others will be more generic at the technique level.

With the example above, the IOB is generic enough so you can use these techniques with a range of procedures to test your defenses more broadly. For a blue team, this IOB can easily be turned into a search that they execute.

A PLAIN-LANGUAGE SEARCH LOOKS SOMETHING LIKE THIS:

Identify all executions of Microsoft Word where Word spawns a child process of PowerShell that connects to the internet and executes another shell (CMD or PowerShell) or a binary that is unsigned and downloaded from the internet.

Your blue team can use this direction and freedom to creatively hunt for this IOB in their environment.

DATA MINING

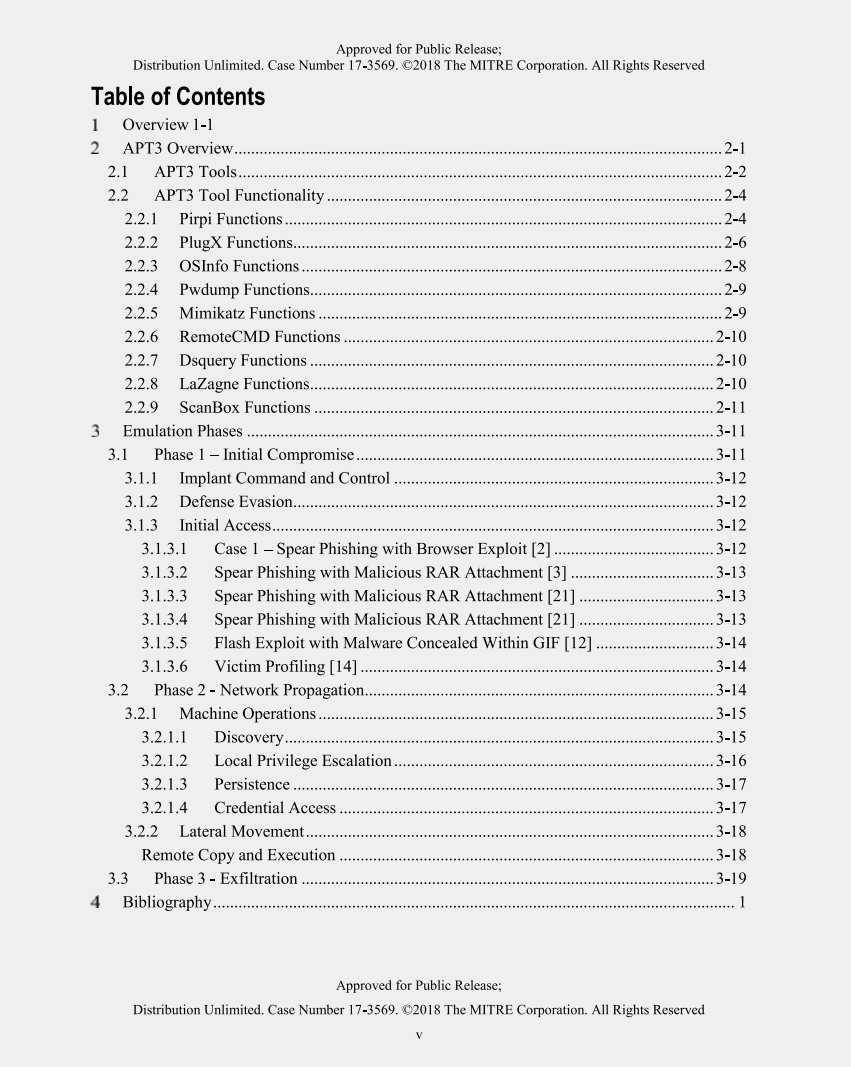
Threat hunters and analysts leverage data mining to identify new attack patterns and previous attack patterns that were missed/remained unidentified. You can data mine using Splunk, Elasticsearch, Hadoop, or other tools to find patterns in the noise of the immense amount of incoming data. While it can be very productive and yield dividends in threat hunting and threat identification efforts, it is difficult and resource-intensive.

It's important to note that most shops do not have the infrastructure to take advantage of data mining, since it is complex and requires extensive expertise and resources. However, if the resources are available, it can be quite valuable.

BY USING TECHNIQUES like retro-matching, you can go back in time and use current threat intel to evaluate your past environment for adversaries you may have missed.

STEP 2: CREATE AN ADVERSARY EMULATION PLAN

AEPs are made up of several sections, including an overview of the plan, an overview of the adversary group, a detailed listing of the emulation phases, and a biography of sources.



Approved for Public Release;
Distribution Unlimited. Case Number 17-3569. ©2018 The MITRE Corporation. All Rights Reserved

Table of Contents

Approved for Public Release;
Distribution Unlimited. Case Number 17-3569. ©2018 The MITRE Corporation. All Rights Reserved
v

Figure 05: The components of a thorough AEP, from the MITRE ATT&CK APT3 example AEP.

You can find a guide for creating an AEP and an example AEP from MITRE ATT&CK. This example AEP is a great template for teams starting their first adversary emulation.

OVERVIEW OF THE APT

The overview of the APT is a detailed description of the adversary group and the tools they are known to use. This is a useful section to reference later in the emulation phases, when the red team is outlining how to emulate the adversary group.

When constructing an adversary emulation plan, it's best to start with known adversary groups that target your organization or industry, as explained in *Choosing the Right Targets* section above.

BUILDING EACH PHASE OF THE ADVERSARY EMULATION

One of the most critical components of a detailed AEP is the section on Emulation Phases. The *Emulation Phases* section is a specific, detailed breakdown of the tactics of the adversary group.

In order to construct the *Emulation Phases*, your red team must identify the tactics the adversary group uses for an attack, along with the particular techniques and procedures for each tactic. Much of this information is available in MITRE ATT&CK.

To detail an emulation phase in the AEP, your red team must note the tools they will use to emulate the particular TTP. This information is available as part of the MITRE ATT&CK description of the adversary group, and more detailed information can be found through a simple Google search of the vulnerability exploited or attack methodology. The more detailed your red team is able to make the phase, the better. Ideally, they will also include the detection step in the AEP.

> The Cybereason Nocturnus team regularly releases detailed research so red teamers and others in the community can learn the exact processes of the most popular adversary groups.

Each emulation phase should be constructed individually and compiled together in the AEP.

EXAMPLE: AN EMULATION PHASE FOR APT28

To understand how to construct an emulation phase, let's look at an example with data from the MITRE ATT&CK framework.

Adversary Group APT28 (G0007) is known to exploit CVE-2015-1701 to perform Access Token Manipulation (T1134). CVE-2015-1701 is an older Windows vulnerability that allows adversaries to co-opt the win32k.sys driver to download and execute arbitrary code.

ENTERPRISE	T1134	Access Token Manipulation	APT28 has used CVE-2015-1701 to access the SYSTEM token and copy it into the current process as part of privilege escalation.

Table 02: A description of how APT28 performs Access Token Manipulation, as seen on the MITRE ATT&CK website.

A simple google search shows there are several tools available on GitHub that can exploit this particular vulnerability and several guides on how to execute it through a watering hole or phishing attack. When red teaming with this TTP, we recommend the hfiref0x tool on GitHub.

Your red team should outline the steps needed to execute the TTP in the emulation phase. They should also note the detection step for that phase.

In this instance, there should be exploit protection at the workstation. However, if this is not the case, the blue team must search process execution logs for unsigned binaries executed with system privileges. This can be done through EDR or SYSMON process execution logs sent to a SIEM.

If there is no execution logging at the targeted workstation, your blue team must note this in their final report and address it as part of their remediation and maintenance activities. Other detection techniques, like identifying IOCs, may be helpful, but are not as reliable as execution logging.

> A detailed and complete AEP is a good resource that newer L1 analysts can use to learn about specific attacks and the security tools they will be working with.

TRACKING THE PROGRESS OF AN AEP

Organize the status of your AEPs through a simple AEP Planning Status table. Each TTP should have an associated planning status based on your team's progress.

PLANNING STATUS CAN TAKE ANY OF THE FOLLOWING FORMS:

01. **DOCUMENTED:** The TTP has been properly documented for the adversary group.
02. **CODED:** The TTP has been coded into the actual simulation for your red team.
03. **EXECUTED:** The coded TTP was successfully executed by your red team.
04. **SUCCESSFUL/NON-SUCCESSFUL:** The TTP execution did or did not complete its goal.
05. **DETECTED/NOT DETECTED:** The TTP execution was successful and it was either detected or not detected.

On the following page, you'll find an example AEP Planning Status table. As your AEP evolves, we recommend adding context like a timeline, hierarchy, TTP type, notes, and more details that will help your team with future emulations.

EXAMPLE AEP PLANNING STATUS TABLE: DEEP PANDA			
ID	NAME	PLANNING STATUS	TIME RATIONALE
T1015	Accessibility Features	Deep Panda has used the sticky-keys technique to bypass the RDP login screen on remote systems during intrusions. For example, use the above technique on your internet-facing servers.	Documented
T1066	Indicator Removal from Tools	Deep Panda has updated and modified its malware, resulting in different hash values that evade detection.	Documented, Coded
T1086	PowerShell	Deep Panda has used PowerShell scripts to download and execute programs in memory, without writing to disk.	Documented, Coded
T1057	Process Discovery	Deep Panda uses the Microsoft Tasklist utility to list processes running on systems.	Documented, Coded
T1117	Regsvr32	Deep Panda has used regsvr32.exe to execute a server variant of Derusbi in victim networks.	Documented
T1018	Remote System Discovery	Deep Panda has used ping to identify other machines of interest.	Documented
T1064	Scripting	Deep Panda has used PowerShell scripts to download and execute programs in memory, without writing to disk.	Documented
T1100	Web Shell	Deep Panda uses Web shells on publicly accessible Web servers to access victim networks.	Documented
T1077	Windows Admin Shares	Deep Panda uses net.exe to connect to network shares using net use commands with compromised credentials.	Documented, Coded
T1047	Windows Management Instrumentation	The Deep Panda group is known to utilize WMI for lateral movement.	Documented, Coded

Table 03: An example AEP Planning Status table for Deep Panda.

In this table, you can quickly see all techniques for this AEP and how much progress has been made in their execution.

TRACKING MULTIPLE AEPS AT ONCE

In order to keep track of all current and past AEPs, we recommend organizing their status in an *AEP Tracking table*. This table gives your team an easily referenceable view of all AEPs they have created and their progress. This also helps larger, cross-functional teams stay aligned on the progress of different, simultaneous AEPs.

Below is an example AEP Tracking table. This table lists the priority and status of all AEPs your team has created along with the progress of their attack simulation.

GROUP	PRIORITY	THREAT	AEP STATUS	ATTACK SCENARIO CONSTRUCTION	DUE	OWNER
DEEP PANDA	High	High	Completed	In Progress	1/12/19	John Smith
APT3	High	High	Completed	Completed	12/28/18	John Smith
MENUPASS	High	Medium	Not Started	Not Started	None	None
ORANGEWORM	High	High	Not Started	Not Started	None	None

Table 04: An example AEP Tracking table with relevant attack groups and their associated priorities and statuses

STEP 3: RUN THE ATTACK SIMULATION

When running the actual attack simulation, your red team must ensure their exercises simulate the actual attack resources the adversary uses. This includes resources and activities like an external command and control server, the proper infiltration and exploitation techniques, and the completion of data exfiltration. If your team skips or fails to execute certain steps, you will inevitably miss important activities that take place in an actual attack.

Follow the emulation plans in both technology and process as closely as possible. Automated adversary emulation tools, like MITRE's CALDERA, are complementary to your red and blue team efforts, and will emulate post-compromise adversarial behavior. Using automated adversary emulation tools gives your red team the freedom to automate parts of the test and focus their manpower on the more important tasks.

> MITRE's CALDERA leverages the ATT&CK model to identify and replicate adversary behaviors as if a real intrusion is occurring. Tools like this are especially useful for teams with limited staff.

STEP 4: ALERT, HUNT, & REPORT

At a minimum, your red team should use adversary emulation plans and TTPs for execution and should actively report on the success of their activities. Be sure to document all resources your red team uses and maintain constant communication with them throughout the simulation. It's critical that real attack executions don't get lost in the noise generated by red team activity. Document any successful detections and alerts for evaluation at the end of the attack simulation.

AEPs also provide a roadmap for automating the identification of attacks with a high degree of fidelity. **This is all only possible if your organization has the capability to detect the right TTPs.** If you are unable to detect the TTPs, this is an opportunity to look into new tooling or data collection methods.

If the red team is not detected at any point, your security operations team should evaluate immediately to determine the cause. There are many reasons this could happen, from too much alerting noise to a lack of data, or simply human error.

HUNTING

If your existing tooling is unable to detect parts of the attack simulation, you should let your team threat hunt and find more aspects of the attack. This will not only give your team more experience threat hunting in their environment, but can also serve as a basis for threat hunting operations in the future. They inform your hunt operations so your team can look for techniques in the real world on a day-to-day basis.

REPORTING

Your evaluation **should inevitably** result in tooling or process improvements. It's important to emphasize that reporting on red team aspects should be **faultless and rankless**. Following these principles will lead to better results from reporting and a more collaborative spirit in process improvement. Following this table should give you a good basis for important data to collect and report on after a simulation.

ATTACK SIMULATION PLAN EXAMPLE: AEP 20190107 (DEEP PANDA)

ID	NAME	TECHNIQUE RESULT	DETECTION TYPE	REMEDIATION RECOMMENDATION	PRIORITY
TT1015	Sticky Keys Replacement	Replaced SetHC. exe with cmd.exe	File Write seen by SIEM; Detected as malop when replacement was executed via powershell.	None Needed	None
TT1066	Unique Binary Malware	Execution via Powershell	File Write in Telemetry from SIEM; No Detection	Add unsigned binary execution from temp to malop ruleset	Medium

Table 05: The minimum reporting for a successful attack simulation

YOUR FINAL REPORT SHOULD HAVE SEVERAL COMPONENTS COMPILED BY THE BLUE TEAM IN CONSULTATION WITH THE RED TEAM, INCLUDING:

- **Technique ID and Name**
- **Technique Result**
- **Detection Type**
- **Remediation Recommendation**
- **Priority**

TECHNIQUE NAME & ID

Technique Name and ID are the name and MITRE ATT&CK ID for the techniques used during the simulation.

TECHNIQUE RESULT

The technique result is what happens when the technique is run during the simulation. This field can be as verbose or succinct as needed to give your team enough context about the technique.

DETECTION TYPE

Within your report, all TTPs need to be categorized according to the way you were able to detect them: **detected**, **telemetry**, or **missed**.

DETECTED

TTPs that are successfully detected and alerted on are classified as detected.

TELEMETRY

TTPs that are not alerted on but some telemetry is available are classified as telemetry.

MISSED

TTPs that are not detected are classified as missed.

Bear in mind that some TTPs can be nullified at your discretion if reliable, high-fidelity detection is not possible or other detections mitigate the issue.

Each simulation needs to be quantitatively scored in your report. Scoring can be as simple or as complex as you want. A simple scheme for scoring (and a good place to start) is by listing the number of TTPs used against the number of TTPs detected. You can also gamify the scoring system to give your team further incentive to succeed during the simulation.

REMEDIATION RECOMMENDATIONS

Remediation recommendations should include technical details and, more importantly, context. Identifying individual TTPs effectively may not be possible, so you may need to gather additional information from the execution. For example, running an unsigned binary in a large enterprise would likely result in false positives if alerted on individually. However, when coupled and correlated with other details such as the execution chain, network activity, etc., the alert becomes much more effective.

Wherever possible, include potential methods of prevention in your remediation recommendations. This can lead to much more impactful alert improvements.

PRIORITY

Rank your recommendations based on priority level so your team can quickly remediate key gaps uncovered in the simulation. We recommend a priority level that is a combination of the likelihood of exploitation and the potential damage of the exploit.

STEP 5: PROCESS & TECHNOLOGY IMPROVEMENT

Develop a process and technology improvement plan based on the results of the attack simulation and the final report. Incorporate the results of several different adversary group simulations, as changes per simulation can significantly influence technology decisions.

Meaningful improvement of your alerts is directly proportional to the quality of your reporting. Give as much context as possible in your reporting. Otherwise, you may end up giving recommendations that become custom catch-all rules and just increase the number of false positives.

Remediation efforts should be tracked as a project including information on the system to be modified, the status of modifications, and their owner. It's important to note that, when looking to add more tools to cover security defense gaps, a much more thorough evaluation may be necessary. This might include additional red team testing, budgeting, PoCs, and more.

A FINAL NOTE ON USING MITRE ATT&CK FOR SUBSTANTIAL SECURITY ADVANCEMENT

While these five steps give your team the basis for a continuously improving security process, you still need a dedicated team and the right security tools to defend effectively. Trying to use these steps without security advancements like visibility into your environment or behavioral detections will dramatically limit the security improvements you are able to make.

Security has no silver bullet solution, but by leveraging a combination of the right people, processes, and tools, your security team can reduce risk while maintaining efficiency. These steps are a piece of the puzzle that is a successful security practice.

If you're looking to use this method in your environment and have questions, get in touch with our team

cybereason

ABOUT CYBEREASON

Cybereason gives the advantage back to the defender through a completely new approach to cybersecurity: the Cybereason Defense Platform. Cybereason offers managed, as-a-service, and on-premise prevention, detection and response solutions. Cybereason technology delivers multi-layer endpoint prevention by leveraging signature and signatureless techniques to prevent known and unknown threats in conjunction with behavioral and deception techniques to prevent ransomware and fileless attacks. Cybereason is privately held and is headquartered in Boston, Massachusetts, with offices around the globe.

Visit our website to learn more

CLICK HERE →

FOLLOW US