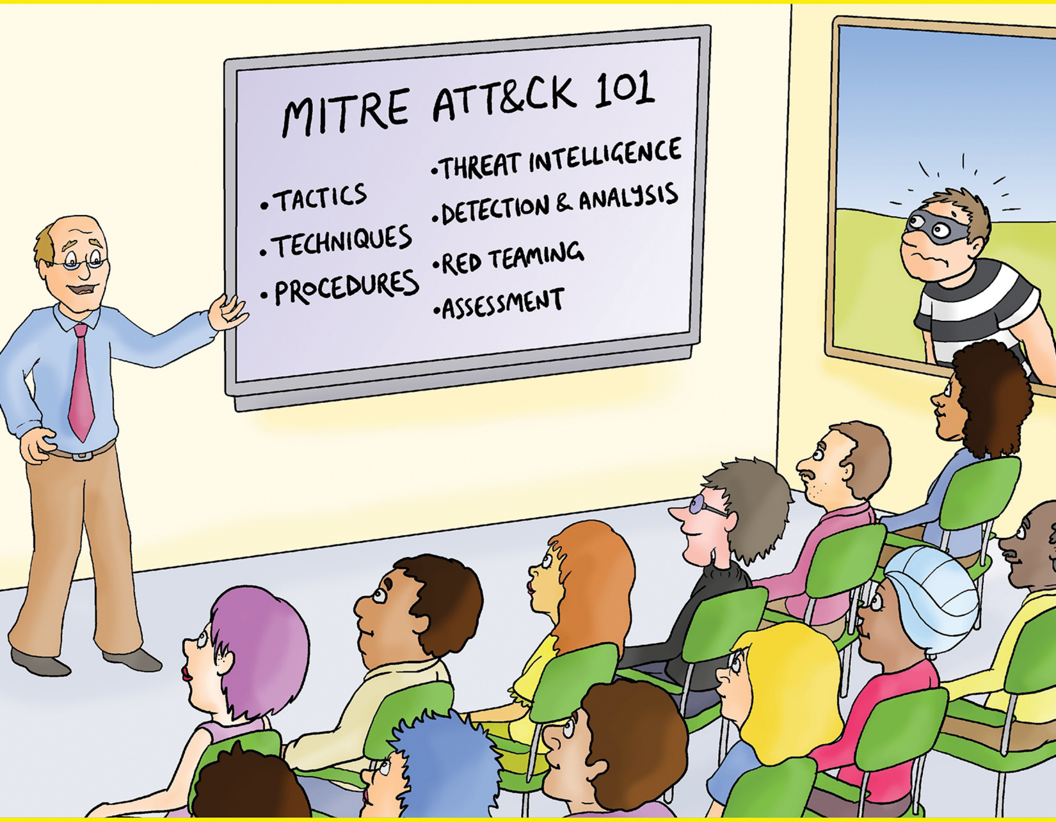
ConversationalGeek®

# Conversational MITRE ATT&CK Framework

By Derek A. Smith (CCISO, CISSP)



**In this book, you will learn:**

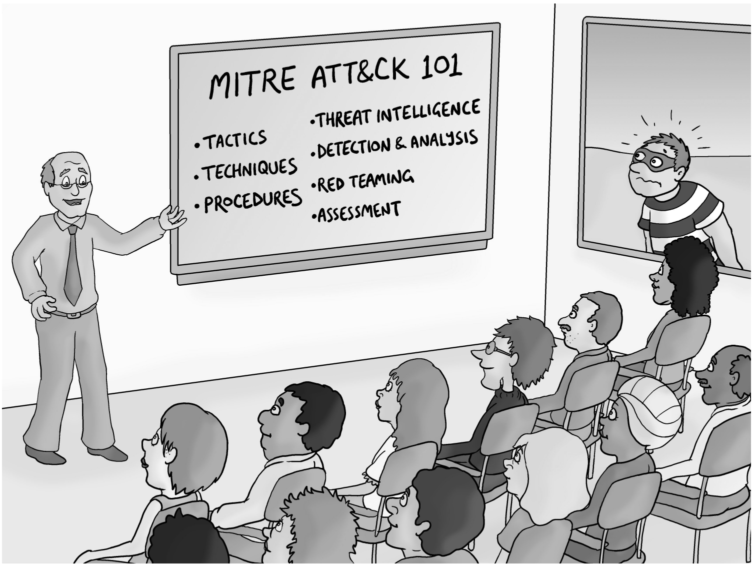
- What the Framework is and how it organizes threat actions
- How the Framework can be used to strengthen your cybersecurity efforts
- How mapping security solutions to the Framework helps to better understand their value

*Sponsored by*

Delinea

# Conversational MITRE ATT&CK Framework

By Derek Smith, CISSP



ConversationalGeek®

## Conversational MITRE ATT&CK Framework
Published by Conversational Geek® Inc.

www.conversationalgeek.com

## Trademarks

## Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or programs accompanying it.

## Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

## Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

| | |
|---|---|
| Author: | Derek Smith |
| Project/Copy Editor: | Nick Cavalancia |
| Content Reviewer(s): | Hope Crocker |

# Note from the Author

Hello and welcome. On behalf of the entire Conversational Geek family, I would like to personally thank you for picking up a copy of the Conversational MITRE ATT&CK Framework ebook. The publication aims to help you understand and use the MITRE ATT&CK framework.

There is a lot of information floating around the internet about the ATT&CK framework, and it can sometimes be overwhelming to figure out how best to use it. This ebook condenses much of that information into concise bits of knowledge that you can easily use when adopting and adapting the ATT&CK framework in your organization.

Derek A. Smith, CISSP

## The "Conversational" Method

We have two objectives when we create a "Conversational" book: First, to make sure it's written in a conversational tone so that it's fun and easy to read. Second, ensure you, the reader, can immediately take what you read and include it in your own conversations (personal or business-focused) with confidence.

These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend, and even the know-it-all Best Buy geek on a level playing field.

## "Geek in the Mirror" Boxes

We infuse humor into our books through both cartoons and light banter from the author. When you see one of these boxes, it's the author stepping outside the dialog to speak directly to you. It might be an anecdote, it might be a personal experience or gut reaction and analysis, it might just be a sarcastic quip, but these "geek in the mirror" boxes are not to be skipped.

Greetings. Within these boxes I can share just about anything on the subject at hand.

Read 'em!

# Introduction

Even as technology and security continue to advance, data breaches are still commonplace, and all business and government agencies can be targets. Security practitioners must fully grasp the difference between threat actors and their motivations if they are to successfully defend themselves against attacks.

Cyber threat actors come in many forms and have various intentions for victimizing you. For instance, cybercriminals are motivated by financial gain. In contrast, insiders may be motivated by discontent with their organization for whatever reason. As varied are the type of threat actors, so are the types of businesses, government agencies, organizations, and individuals who fall victim to their attacks. These threat actors love to capitalize on the interest and fear related to disruptive situations, like the recent COVID-19 pandemic. They forge techniques to lure users into clicking on malicious links and attachments. Events surrounding COVID-19 emboldened threat actors to adopt more sophisticated and discreet tactics.

Microsoft's digital defense report gathered observations from thousands of security experts across 77 countries worldwide. Their study detailed threat actors' methods to harvest data and information from unsuspecting victims. The report offered insight into threat actors' relentless efforts to take advantage of remote working situations caused by the pandemic.

Attack surfaces are massive and significantly different from the past. Cybersecurity used to be easier and relatively straightforward, like defending a building. But instead of a single building, today's organizations are like sprawling cities with expanding neighborhoods, unmapped alleyways, and ever-changing borders. However, defenders still defend this new, broader attack surface as they did over a decade ago. This is not good because today's enterprise attack surface has far more available for threat actors to target than in the past. Additionally, the less aware an organization is of its attack surface, the slower its response will be to attacks when they occur.

Organizations are vulnerable to a host of attacks, from sophisticated phishing attacks to ransomware to missed misconfigurations during rapid deployments. The attack surface was already difficult to manage, but the move to remote work during the pandemic made it even more so almost overnight.

This new reality means defenders must take an operationalized approach to security intelligence, not just to respond to an attack but also to understand precisely what type of defense to deploy, how to defend themselves, and who their specific threat actors are.

The shifting technological landscape has fundamentally altered when and how adversaries decide to attack. Therefore, an organization's cyber defense approaches must address this decision calculus if it hopes to create effective defenses.

To combat cyberattacks and protect against urgent threats, some companies like Microsoft are amassing billions of signals to garner a holistic view of the security ecosystem. This provides relevant, contextual threat intelligence to detect, investigate, and respond to threats by providing broad threat visibility faster. Given the billions of signals, defenders can easily get lost in a sea of noise. They must have the context to understand which signals are the highest priority, why, and what actions they must take to deal with the threat.

To defend against the most capable cyber threats, defenders must focus on the actors with the greatest capability and intent to attack. Typically, those will be large, adversarial nation-states, cybercriminals, hacktivists, and others. When defenders adopt an adversary-focused approach to cyber defense, the same approach can be used on various actors. The combination of enforcement actions and messaging can push criminal decision-making in a positive direction.

But the bottom line is to effectively counter today's threats, defenders must be able to shift the decision of attackers, keeping them below the threshold of deciding to attack. To do this, defenders must understand the criteria adversaries use to justify an offensive cyber operation. One way these defenders can better understand adversary behaviors is to follow a more organized way of approaching threats. Thus, the need for the MITRE ATT&CK Framework. This guide will examine the MITRE ATT&CK framework's approach to security, explore various components of the ATT&CK framework and discuss how you can start applying the framework in your organization.

The easiest way to learn about the ATT&CK framework  and see the depth of information it provides is to dive right in. So off we go!

# What is The MITRE ATT&CK Framework?

*I don’t know how they’re getting in!*

The MITRE Corporation, a non-profit organization that works with government agencies, industry, and academic institutions, created its ATT&CK framework in 2013. The framework is a globally accessible knowledge base that comprehensively represents attack behaviors. It is defined as MITRE Adversarial Tactics, Techniques, and Common Knowledge (abbreviated as, and herein referenced as *ATT&*CK) and is a repository of cyberattack behaviors based on real-world observations of adversaries' behaviors categorized by tactics and techniques.

You can see and interact with MITRE's ATT&CK Framework by visiting

**https://attack.mitre.org**

ATT&CK documents common tactics, techniques, and procedures (TTP) that cyber criminals use when attacking targets. The framework outlines adversarial behaviors specific to Windows, Linux, Mac, cloud-based, and mobile environments. Defenders regularly rely on this knowledge base to devise offensive and defensive measures to strengthen their security posture.

The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

Cyber defenders can use ATT&CK to better classify attacks, understand adversary behavior and assess their organization's risk. They can also use the framework to gain insight into how adversaries might operate against them in various scenarios so they can create informed strategies to detect and prevent those behaviors from affecting their organization's security.

ATT&CK's unique ability to provide insights into adversaries' behaviors and a standardized, easily accessible global language has led to its growing popularity for defenders looking to share threat intelligence and strengthen their security posture.

MITRE organizes its observations about attack behaviors into tables called Matrices. Each Matrix addresses a different target, like enterprise operating systems and cloud platforms, mobile devices, or industrial control systems. There are three different ATT&CK matrices: *Enterprise*, *Mobile*, and *ICS*. Each individual matrix filters down the list of all documented possible techniques and tactics:

- The *Enterprise* matrix consists of all the tactics and techniques within the framework specific to Linux, Windows, macOS, cloud, Network, and containers (with sub-matrices for each). When any one of these operating systems or environments is penetrated, the Enterprise matrix helps identify the nature of the threat and outlines the information that can be used to defend against it in the future.

- The *Mobile* matrix has the same objective as Enterprise, but it applies specifically to those actions taken against Android and iOS mobile devices (again, with sub-matrices for each).

- The *ICS* matrix focuses on attackers' techniques and tactics used when attacking industrial control systems.

## Breaking Down ATT&CK

ATT&CK functions using a hierarchy that helps to organize all the threat actions that can be taken during an attack.  The hierarchy is as follows:

- **Tactics** - Each tactic is essentially a goal of the attacker (e.g., move laterally within your network) at certain stages of a cyber attack. If cybercriminals can accomplish each of these individual goals, they are one step closer to their objective. In some cases, the attack will not seek to realize every tactic because some may go beyond what the attacker aims to do. For example, an attacker may not want their attack to perform lateral movement if they simply want to steal information from a specific computer.

- **Techniques** – Within a given Tactic, each technique represents the high-level action (e.g., phishing) taken to achieves a tactical goal.

- **Procedures** – Within each technique lies procedural examples (e.g., the use of a specific malicious tool) to demonstrate how the technique has been reportedly accomplished in an actual attack.

Additionally, for a given technique, ATT&CK – when possible – also may provide detection and mitigation suggestions.

The hierarchy exists to organize each of the adversary behaviors. An actual cyberattack would be made up of a larger number of tactics, techniques, and procedures (TTPs) that, in sum total make up the actions necessary to accomplish the adversary’s malicious goal. And not every attack uses every TTP.

So, if an adversary simply wants to to be an Initial Access Broker who sells of stolen credentials, they may only perform those TTPs involved in phishing a target organization’s users and harvesting their credentials using, say, a spoofed Microsoft 365 logon page.

Conversely, if an adversary is intent on gaining access to an organization’s network, needs to laterally move within it, gain elevated privileges along the way, destroys backups, and encrypts data and systems as part of a ransomware attack, many, many TTPs will be involved in the single attack.

Let’s continue breaking down the hierarchy.

## Tactics

As of version 12 of the matrix (which was released in October of 2022), there are fourteen different tactics in the matrix for an Enterprise ATT&CK that describe how an attacker could operate within an enterprise network:

1. **Reconnaissance** – Gather information that can be used to plan future attacks

2. **Resource Development** – Establish resources that can be used to support an attack

3. **Initial Access** – Establish a foothold on the target system or within the target network

4. **Execution** – Start malware or other malicious code running on the target system

5. **Persistence** – Implement protections to make it more difficult for an attacker's access to be removed from the target system

6. **Privilege Escalation** – Elevate the current account's access or gain access to additional privileged accounts to achieve the permissions necessary to achieve objectives

7. **Defense Evasion** – Prevent detection and removal of the attacker's access by automated defense systems (e.g., antivirus)

8. **Credential Access** – Gain access to user accounts by guessing passwords or authentication information

9. **Discovery** – Explore the target environment to identify targets of interest and so on

10. **Lateral Movement** – Move throughout the target environment

11. **Collection** – Collect data that moves the attacker toward their objective

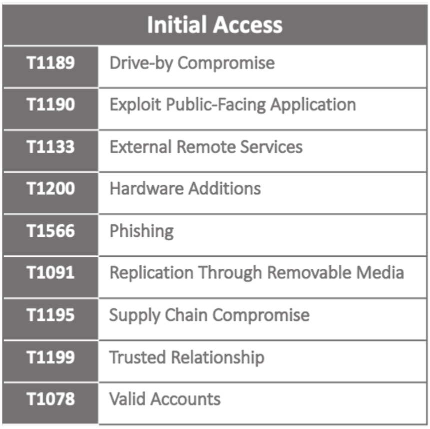
12. **Command and Control** – Communications between the attacker and systems they control on the target network

13. **Exfiltration** – Removal of stolen data from the target environment

14. **Impact** – Attempt to manipulate, interrupt or destroy target systems or data

## Techniques

Within each tactic is a list over every documented action taken to accomplish the tactical goal.  Take the example below of the tactic *Initial Access*; the techniques listed below it represent the possible ways a threat actor could achieve the goal:



| Initial Access | |
|---|---|
| T1189 | Drive-by Compromise |
| T1190 | Exploit Public-Facing Application |
| T1133 | External Remote Services |
| T1200 | Hardware Additions |
| T1566 | Phishing |
| T1091 | Replication Through Removable Media |
| T1195 | Supply Chain Compromise |
| T1199 | Trusted Relationship |
| T1078 | Valid Accounts |

Note the “T####” next to each technique; MITRE assigns a unique identifier to every tactic, technique, data source, mitigation, and threat group referenced within the framework.

Techniques may also have sub-techniques that further break out the threat actions taken. For example, *Phishing* has three sub-techniques: *Spearphishing Attachment*, *Spearphishing Link*, and *Spearphishing via Service*, with each having it’s own detail, procedural examples, mitigations and detections.

## Benefits of the MITRE ATT&CK Framework

ATT&CK brings a common vocabulary that enables stakeholders, cyber defenders, and vendors to clearly communicate the exact nature of a threat and the objective assessment of the cyber defense plan that can defeat it.

There are two significant benefits of using ATT&CK:

1. **ATT&CK will help defenders understand their adversaries and how they operate.** It outlines their steps to penetrate your network and achieve their end goal. Defenders must understand how the offense works, how the adversary works, how they think, and what they need to do to accomplish their goals.

2. **Help overcome some cyber skills training issues that defenders currently face.** If defenders can effectively leverage ATT&CK, junior security analysts with little experience can gain the knowledge base they need and a research database to examine to determine what is occurring in the industry, what to look for, and how to defend against it. ATT&CK provides a system that can be used to consistently address threats. MITRE formalized the process of categorizing attacks and allows for a common language when different security teams must communicate with each other.

These benefits ensure that defenders:

- Gain insight into the adversary's game plan in terms of combinations of tactics and techniques.

- Clearly communicate the exact nature of a threat and respond faster with greater insight.

- Proactively design defenses to thwart adversaries.

# Focus Areas of ATT&CK

Defenders such as red teams, blue teams, incident responders, cyber investigators, penetration testers, and cyber threat analysts can use ATT&CK to develop use cases for shoring up their cyber defenses.

ATT&CK can serve as a unifying taxonomy for these groups to share information, work together and build the necessary detection and response procedures. The following are the focus areas of the framework broken down, as needed based on the sophistication of your cybersecurity teams.

## 1. Threat Intelligence

A critical aspect of ATT&CK is how it integrates cyber threat intelligence (CTI). Unlike previous methods of digesting CTI used primarily for indicators, ATT&CK documents adversary group behavior profiles based on publicly available reporting to demonstrate which groups use which techniques.

Usually, individual reports are used to document a particular incident or group, but it is difficult to compare what happened across incidents or groups and conclude on what types of defenses were most effective. Defenders might want to start with techniques with the highest group usage when deciding how to focus defensive resources. With ATT&CK, defenders can view across groups of activity by focusing on the technique.

Examples of how particular adversaries use techniques are documented on MITRE's ATT&CK page, representing that group's procedure for using the technique. The procedure is a specific instance of use. It can be beneficial for understanding exactly how the technique is used, replicating an incident with adversary emulation, and specifics on detecting that instance in use.

## 2. Detection and Analytics

Once you understand the methods adversaries use to attack you and how to use that knowledge to prioritize your defensive strategy, you must understand how to build detections for those behaviors.

Detection can be broken up into levels based on how sophisticated your team is and what resources you have access to:

- Level 1 is for beginners who may not have many resources,
- Level 2 is for mid-level teams starting to mature, and
- Level 3 is for more advanced cybersecurity teams and resources.

Building analytics to detect ATT&CK techniques might be different than how you're used to doing detection. Rather than identifying behaviors that are known to be bad and blocking them, ATT&CK-based analytics involves collecting log and event data about the behaviors on your systems and using that to identify the suspicious behaviors described in ATT&CK.

### Level 1

The first step is understanding your data and search capabilities. To find suspicious behaviors, you must see what's occurring on your systems. One way to do this is to examine the Data Sources listed for each ATT&CK technique. Those data sources describe the data types that could give you visibility into the given technique. They provide a good starting point for what to collect.

Once you've collected the data in your SIEM, you can analyze the data. One excellent starting point is to look at analytics created by others and run them against your data. There are several analytic repositories available for this.

Once you have the basic search returning data and understand the results, you can filter out your false positives, so you are not overwhelmed. Examine each result to determine whether it's malicious. Your goal is to reduce false positives as much as possible while still ensuring you'll catch the malicious behavior. Once the analytic has a low false-positive rate, you can automate creating a ticket in your SOC each time the analytic fires or adding it to a library of analytics to use for manual threat hunting.

### Level 2

You can expand coverage by writing your own analytics using other people's analytics. This is a more complicated process that requires understanding how the attacks work and how they are reflected in the data. Once you know how adversaries use the technique, determine how to run it yourself to view in your own logs. An easy way to accomplish this is by using the Atomic Red Team, an open-source project led by Red Canary that provides red team content aligned to ATT&CK that can be used to test analytics.

A general pattern to follow is to write the search to detect malicious behavior, revise it to filter out false positives, make sure it still detects the malicious behavior, and then repeat this process to reduce other typed of false positives.

### Level 3

Once you are confident that you're producing quality analytics to detect attacks from Atomic Red Team, test your confidence and improve your defenses by doing some purple teaming.

In reality, adversaries don't just carry out cookie-cutter copy/pasted attacks. They adapt and try to evade your defenses, including your analytics. The best way to ensure your analytics are robust against evasion is to work directly with a red teamer. Your blue team will be responsible for creating analytics. The red team will be responsible for emulating your adversary, trying to evade your analytics by executing attacks and evasions that adversaries use in the real world. They'll act like real adversaries to help you understand how your analytics will fare against real adversaries.

## 3. Adversary Emulation and Red Teaming

Continuing the previous theme, this section is broken up into the same three levels based on your team's level of sophistication and what resources you have access to:

- Level 1 is for beginners who may not have many resources,
- Level 2 is for mid-level teams starting to mature, and
- Level 3 is for more advanced cybersecurity teams and resources.

If you are not familiar with adversary emulation. It is a type of red team engagement that mimics a known threat to an organization by using threat intelligence to define what actions and behaviors the red team uses. This distinguishes adversary emulation from penetration testing and other forms of red teaming. Adversary emulators construct a scenario to test certain aspects of an adversary's tactics, techniques, and procedures (TTPs). The red team then follows the scenario while operating on a target network to test how defenses might fare against the emulated adversary.

Since ATT&CK is an extensive knowledge base of real-world adversary behaviors, it doesn't take much imagination to draw a connection between adversary or red team behaviors and ATT&CK. Let's explore how security teams can utilize ATT&CK for adversary emulation to help improve their defenses.

### Level 1

Small teams and those mainly focused on defense can benefit tremendously from adversary emulation even without access to a red team. Many resources are available to help jump-start testing your defenses with techniques that align with ATT&CK. I mentioned Atomic Red Team before. They have a collection of scripts that you can use to test how you might detect specific techniques and procedures mapped to ATT&CK techniques. The Atomic Red Team repository has many atomic tests, each with a directory dedicated to the ATT&CK technique that is tested.

### Level 2

For defenders who already have red team capabilities, you can benefit by integrating ATT&CK with your existing engagements. Mapping the techniques used in a red team engagement to ATT&CK provides a common framework when writing reports and discussing mitigations.

Mitigations explain how to defend against attacker TTPs. A single Mitigation can apply to multiple TTPs; for instance, multi-factor authentication addresses account manipulation, brute force, external remote services, and many others.

To begin, you can take one of your existing planned operations or tools and map it to ATT&CK. Mapping red team procedures to ATT&CK is like mapping threat intelligence to ATT&CK. Sometimes mapping techniques can be as simple as searching the command used on the ATT&CK website.

Another helpful resource to map red team procedures to ATT&CK is the APT3 Adversary Emulation Field Manual, which breaks out command-by-command actions that APT3 has used, all mapped to ATT&CK.

Some red teams have their tried-and-true toolkits and methods of operation. They know what works because it works all the time. But they don't always know how much their tried-and-true TTPs overlap, or don't overlap, with known threats that may target your organization. That leads to a gap in understanding how well your defenses stack up to what you're actually trying to defend against, the adversaries targeting your environment and not necessarily the red team themselves. You want to ensure you're not just doing the techniques because your tool can perform them. You want to emulate a real adversary you care about to provide more value.

While there are benefits to mapping to ATT&CK as you plan your red team operations, you also benefit once you've executed your operation as you communicate with your blue team. Suppose they are mapping analytics, detections, and controls back to ATT&CK. In that case, you can easily communicate with them in a common language about what you did and what they were successful at.

### Level 3

By now, your red team is integrating ATT&CK into operations and finding value in communicating back to the blue team. To advance your team's impact, you can collaborate with your organization's CTI team to tailor engagements toward a specific adversary using data they collect by creating your own adversary emulation plan.

Creating your own adversary emulation plan draws on the greatest strength of combining red teaming with your own threat intelligence: the behaviors are seen from real-world adversaries targeting you! The red team can turn that intel into effective tests for showing what defenses work well and what improvements are needed. When security testing exposes visibility and control gaps, there is a much higher level of impact because you can demonstrate a high likelihood that they have been leveraged by a known adversary. Linking your own CTI to adversary emulation efforts will increase both the effectiveness of testing and the outputs to senior leadership to enact change.

We recommend a five-step process to create an adversary emulation plan, execute the operation, and drive defensive improvements.

1. **Gather threat intel** — Select an adversary based on the threats to your organization and work with the CTI team to analyze intelligence about what the adversary has done. Combine what your organization knows with publicly available intel to document the adversary behaviors, what they seek, and how they operate, fast or slow.
2. **Extract techniques** — In the same way you mapped your red team operations to ATT&CK techniques, map the intel you have to specific techniques in conjunction with your intel team.
3. **Analyze & organize** — With your collected intel about your adversary and how they operate, diagram that information into their operational flow in a way that's easy to create specific plans.
4. **Develop tools and procedures** — Now that you know what you want the red team to accomplish, determine how to implement the behavior using these considerations:
    - How did the threat group use this technique?
    - Did the group vary which technique was used based on the environmental context?
    - What tools can we use to replicate these TTPs?

5. **Emulate the adversary** — With a plan in place, the red team can now execute and perform an emulation engagement. The red team should work closely with the blue team to understand where gaps are in the blue team's visibility and why they exist.

Once this process is completed, the red and blue teams can work with the CTI team to determine the next threat to repeat the process, creating a continuous activity that tests defenses against real-world behaviors.

## 4. Assessments and Engineering

Every defense needs to be measured to ensure they function as desired and for continuous improvement. Here I discuss how you can use ATT&CK to measure your defenses and enable that improvement. I will again use the 3-level process based on sophistication and resource availability.

ATT&CK assessments are part of a more extensive process to provide valuable data to security engineers and architects justifying threat-based security improvements. They are used to:

- Assess how your defenses work against techniques and adversaries in ATT&CK,
- Identify the highest priority gaps in your current coverage, and
- Modify your defenses to address those gaps.

The levels for assessments and engineering are cumulative and build on each other. Even if you consider yourself advanced at cybersecurity, I recommend you start at Level 1 and walk through the process.

## Level 1

If your team is small and doesn't have access to lots of resources, and you want to do a full assessment, don't. Doing so will leave you burnt out on ATT&CK rather than excited to use it. Instead, start small by selecting a single technique to focus on, determine your coverage for that technique, and then make the appropriate engineering enhancements to start detecting it. Beginning this, you can practice running a more extensive assessment.

Once you have selected a technique, you must figure out your coverage of that technique. I suggest starting with the following categories of coverage:

- Your existing analytics will likely detect the technique.
- Your analytics won't detect the technique, but you're pulling in suitable data sources to detect it; or
- You're not currently pulling in relevant data sources to detect the technique.

A great way to get started on measuring coverage is to look for analytics that might already cover a technique. Many SOCs already have rules and analytics that might map back to ATT&CK. Often you'll need to bring in other information about the technique, which you can get from the technique's ATT&CK page.

If your analytics are already picking up the technique, great! Record your coverage for that technique, pick a new one, and start the process again. But, if you're not covering it, look at the data sources listed on the technique's ATT&CK page and determine if you might be already pulling in the correct data to build a new analytic. If you are, then it's just a question of building one out.

However, if you're not pulling in suitable data sources, examine the data sources listed on the technique's ATT&CK page as a potential starting point and try to gauge the difficulty of collecting each of them versus the effectiveness of how you'd be able to use them.

Don't stop at one technique. Run through this process several times, picking a new technique (or two) across each tactic for each run. Keep track of your results using the ATT&CK Navigator, which generates heatmaps of ATT&CK coverage. Once you feel comfortable with the process, perform a data source analysis and develop a heatmap of which techniques you could detect, given the data sources you're pulling in.

## Level 2

Once you're familiar with this process and have access to more resources, expand your analysis to span a reasonably large subset of the ATT&CK Matrix. Also, use a more advanced coverage scheme to account for the fidelity of detection.

This expanded scope makes analyzing analytics slightly more complex. Each analytic now can potentially map to many different techniques, as opposed to just the one technique from before. Additionally, if a technique is covered by an analytic, you'll also want to tease out the analytic's fidelity.

In addition to looking at your analytics, you should also analyze your tools. To do this, I recommend iterating through each tool, creating a separate heatmap for each, and asking the following questions:

- Where does the tool run? Depending on where a tool is running, e.g., at the perimeter or on each endpoint, it may perform better or worse with specific tactics.

- How does the tool detect? Is it using a static set of "known bad" indicators? Or is it doing something behavioral?
- What data sources does the tool monitor? Knowing the data sources a tool monitors lets you infer which techniques it might detect.

Try not to spend too much time getting bogged down with the specifics. Instead, gather information on general coverage patterns.

To create a final heatmap of coverage, aggregate all the heatmaps for your tools and analytics, recording the highest coverage over each technique. Once you have this, you'll want to turn towards improvement. As a first step, I recommend you do the following:

- Create a list of high-priority techniques you want to focus on in the short term.
- Ensure you're pulling in the correct data to start writing analytics for the techniques you're focusing on.
- Start building analytics and updating your coverage chart.
- Start with your current coverage, add analytics, and update your coverage accordingly.

You may also want to start upgrading your tools. As you're analyzing documentation, keep track of any optional modules that you might be able to use to increase your coverage. If you come across any, investigate what it would take to enable it on your network and balance this with the coverage it offers. If you can't find any additional modules for your tools, you can also try to use them as alternative data sources.

Once you implement some of these changes and improve your coverage, the next step is introducing adversary emulation, particularly atomic testing. Each time you prototype a new analytic, run a matching atomic test and see if you caught it. If you did, great! See what you missed and refine your analytic accordingly if you didn't.

## Level 3

If your security team is more advanced, a great way to improve your assessment is to include mitigations. This helps you examine what your tools and analytics are detecting and evaluate your SOC as a whole.
An excellent way to identify how you're mitigating techniques is to examine each of your SOC's policies, preventative tools, and security controls and map them to the ATT&CK technique(s) they may impact. Then add those techniques to your heatmap of coverage.

Another way to extend your assessment is to talk to SOC employees to help you better understand how your tools are used and highlight gaps and strengths you might want to consider. Some example questions you can ask include:

- What tools do you use most frequently? What are their strengths and weaknesses?
- What data sources are you unable to see that you wish you could see?
- Where are your biggest detection strengths and weaknesses?

As you talk to your colleagues, look at the tool heatmaps you had previously created. If you're still unsatisfied with the coverage your tools provide, it may be necessary to evaluate new ones. Come up with a heatmap of coverage for each prospective new tool and see how adding it helps enhance your coverage.

Finally, implementing more mitigations can help decrease your reliance on tools and analytics. Examine mitigations in ATT&CK to gauge if you can practically implement them. Consult your detection heatmap as part of this process.

Assessing your defenses and guiding your engineering can be a great way to get started with ATT&CK: running an assessment provides you with an understanding of your current coverage, which you can augment with threat intelligence to prioritize gaps and then use to tune your existing defenses by writing analytics.

You shouldn't need to run an assessment every week or month. Instead, it would be best to keep a running tab on your last assessment, update it when you get new information, and periodically run adversary emulation exercises to spot-check your results. Eventually, by leveraging ATT&CK to show how your defenses stack up to real threats, you'll be able to better understand your defensive posture and prioritize your improvements.

# Practical Ways to Apply ATT&CK

MITRE ATT&CK provides six sample use cases for the focus areas just mentioned to obtain a wealth of information about your cyber defenses. I've added a seventh, as there is an additional use case not mentioned by MITRE.

## 1. Adversary Emulation

Cyber defenders can use ATT&CK to test the organization's resiliency against realistic cyber threats when performing a penetration test. They can realistically simulate the operations of a particular threat. Additionally, they can test whether they have defenses in place against the most commonly-used tactics of cybercriminals and other threat actors. Defenders can verify that their organization's defenses provide adequate protection against real-world threats.

## 2. Red Teaming

Cyber defender red teams can use ATT&CK to identify potential weaknesses in an organization's defenses, for a variety of purposes, including:

- **Comprehensive Coverage:** to ensure that nothing is accidentally overlooked.
- **Clearer Communications:** standardize cybersecurity terminology and the potential attack vectors helpful in communicating results to the client.
- **Avoiding Certain Attack Vectors:** identify attack vectors that may be out of scope for an assessment.
- **Identifying Opportunities:** outlines different methods for achieving specific goals to identify ways to bypass defenses.

## 3. Behavioral Analytics Development

Cyber threat actors can easily modify their malware and tools that render indicators of compromise (IoCs) and malware signatures obsolete.  As a result, only about half of malware is caught by signature AV. ATT&CK Techniques describe "how" a particular goal can be achieved without specifying a specific tool. Defenders can identify attacks based on this tool and can potentially perform attribution based on the list of threat actors known to use that particular technique.

## 4. Defensive Gap Assessment

Cyber defenders can use a defensive gap assessment designed to identify holes in cyber defenses. Using  ATT&CK as a framework for the defensive gap assessment, they can check if each potential attack vector applies to their organization and if solutions exist to detect and/or protect against it. ATT&CK provides a listing of methods an attacker could use to achieve their objectives at each stage of the cyberattack lifecycle.

## 5. SOC Maturity Assessment

An organization's security operations center (SOC) is responsible for detecting and responding to cyberattacks against the organization.  If the SOC cannot detect and react appropriately to a specific type of attack, then the organization is vulnerable to this particular technique.

ATT&CK can be used to measure the maturity and effectiveness of an organization's SOC.  Cyber defenders then prepare their SOC to defend against the cyber threats it is likely to face.

## 6. Cyber Threat Intelligence Enrichment

Cyber threat intelligence, discussed in the previous section, is essential to an organization's ability to protect itself against modern threats. ATT&CK can help defenders make their threat intelligence actionable. Using the information provided within the framework, defenders can identify behaviors common to particular threat actors and determine whether their existing defenses are capable of detecting and responding to attacks by these adversaries.

## Mapping the ATT&CK to Security Solutions

I previously covered the six use cases MITRE provides to practically apply the ATT&CK framework. But I'd like to discuss a seventh use case not mentioned by MITRE – *the mapping of security solutions to ATT&CK*.

This is likely the most important use case of them all. ATT&CK can be used to map out the security solutions you employ to gain a clear assessment of what aspects of cyberattacks you are protected against ,and to determine which threat actions spotlight gaps in your defenses that still present risks to your organization. You must be able to assess the viability of your security solutions against real-world threat actions.

By understanding where your security gaps are, it's possible to identify needed solutions or compensating controls that will address the realized areas of risk in your security strategy.

In the next chapter, I'll provide detail of how the solutions from this eBook's sponsor map to MITRE, helping you to understand which parts of cyberattacks are mitigated by using their solutions.

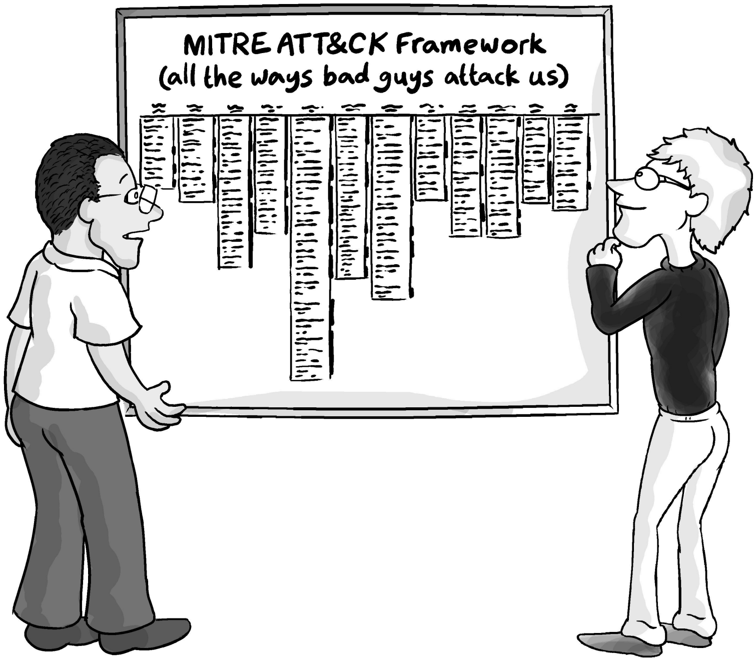
# The Big Takeaways

The MITRE ATT&CK Framework is like an encyclopedia of what adversaries can do using real-world examples as its basis. Therefore, it can seem like a monumental task to defend a constantly expanding attack surface continuously monitored and probed by bad actors. However, ATT&CK's value to security analysts can't be overstated. Leveraging the information already out there, creating a solid foundation of monitoring and execution in your organization, and understanding how the enemy attacks can help you build up your defenses and keep your organization safe.

Cyber defenders who want to operationalize ATT&CK while improving security efficacy, operational efficiency, and ROI on security investment should use the knowledge gained from ATT&CK to see how their security operations aligns with security requirements, objectives, and strategies. ATT&CK can help because it is one of the most complete and definitive resources of hacker techniques available today. Cyber defenders increasingly discuss cyberattack techniques in ATT&CK terms and are building defenses and choosing software based on the MITRE ATT&CK models.

The wealth of information ATT&CK provides is difficult to grasp by description alone. You can best understand the depth of its value by setting aside an hour or two to explore it on your own. You won't be sorry you did.

# Sponsor Chapter: Mapping Delinea PAM to the MITRE ATT&CK Framework



*And which of these are we protected against?*

MITRE's ATT&CK Framework (again, herein simply referred to as *ATT&CK*) not only defines the actions taken by threat actors to achieve aspects of their overall attack; it also helps to define where your security solutions provide coverage and, therefore, where the gaps are. This chapter seeks to provide an overview of the specific TTPs either partially or completely mitigated by Delinea's Privilege Access Management (PAM) solutions.

In general, PAM solutions operate as a subset of your Identity & Access Management initiatives, putting privileged access controls in place for all identities (human and machine). Given that nearly every kind of cyberattack requires privileged access, PAM plays a significant role in stopping any and all TTPs that require elevated credentials as a prerequisite.

The remainder of this chapter focuses on which MITRE TTPs are addressed by implementing *Delinea's solutions below* (herein referred to as *Delinea PAM*):

- Secret Server – Discovers privileged credentials and secures them within a vault, managing their accessibility, password rotation, and use through controlled remote sessions.

- Server PAM – Eliminates the use of unmanaged local administrative accounts on Windows, Linux, and UNIX servers, and prevents lateral movement through just-in-time (JIT) and just-enough (JE) privileged access with multi-factor authentication (MFA) enforcement.

- Privilege Manager – Controls privileged access to applications on workstations to restrict unsanctioned privileged account use and controls privileged group membership.

- Privileged Behavior Analytics – Detects anomalies in privileged account use across the enterprise using machine learning.

- DevOps Secret Vault – Similar to Secret Server, but for DevOps. Manages credentials for applications, databases, CI/CD tools, and services used by DevOps without causing friction in the development process. Also replaces hard-coded credentials with API calls and, optionally, ephemeral tokens.

- **Account Lifecycle Manager** – Manages the entire lifecycle of service/application accounts from discovery and provisioning through decommissioning.

The premise of the use of these solutions in total helps to reduce the risk of successful cyberattacks by:

- **Removing standing privileges** to reduce the attack surface by eliminating local privileged accounts or vaulting those that can't be eliminated - for emergency break-glass access only.

- **Enforcing least privilege** whereby end users (on workstations) & admins (on servers) use their individual enterprise account that has limited rights. This mitigates the risk of damaging mistakes and reduces the blast radius if their account is compromised.

- **Managing privileged accounts** including their passwords, who has access, and where that access can be used.

- **Enforcing MFA at login** to the PAM vault, workstations, and servers, upon vaulted secret access, and application execution or elevation of privileges. This additional identity assurance is to confirm there's a human at the keyboard (blocking malware, bots, and ransomware) and that the human is the legitimate owner of the credential.

- **Utilizing a *Just-in-Time* access request model**, providing users with self-service workflows to request additional access that, if approved, provides elevated permissions provisioned for a limited period.

- **Analyzing privileged behavior** to identify when anomalous activities are taking place using a privileged account, triggering an alert to security teams, denying access, or requiring MFA.

- **Monitoring, reporting, and session recording**, for auditors and incident response teams, to answer questions like "who has access to what" and "who did what."

In general, *Delinea* PAM’s application to ATT&CK is to ensure least privilege is implemented and enforced such that privileged access is either unavailable or limited in scope to the threat actor anytime it’s required to complete a malicious action, across the entire attack chain.

## How to Use this Chapter

For each tactic within ATT&CK where Delinea PAM has an applicable mitigation, the tactic (example shown below) will be listed with a high-level definition of the tactic’s goal, a visual showing only those techniques Delinea PAM helps to mitigate, and a brief description of how the solution mitigates either specific or multiple techniques.

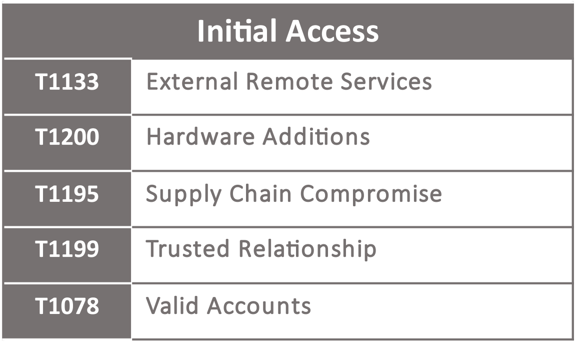
The remainder of this chapter will discuss which ATT&CK TTPs are prevented/stopped/mitigated/etc. using Delinea PAM. Because no solution protects against the entirety of ATT&CK, this chapter will focus only on those ATT&CK tactics Delinea PAM applies to.

# Initial Access

## Goal

To gain an initial foothold within a network.

## Techniques Delinea PAM Helps to Mitigate



| Initial Access | |
|---|---|
| T1133 | External Remote Services |
| T1200 | Hardware Additions |
| T1195 | Supply Chain Compromise |
| T1199 | Trusted Relationship |
| T1078 | Valid Accounts |

## How Delinea PAM Helps

There are five specific techniques that Delinea PAM helps to stop. Typically, the use of insecure externally facing remote access solutions (e.g., RDP and VPN sessions) falls under *External Remote Services*. Delinea PAM provides an alternative for secure remote access that is browser-based, with access to privileged credentials and IT infrastructure remaining protected.

The other four techniques involve the use of accounts that provide access to add maliciously intended hardware on endpoints, to manipulate third-party products in the supply chain, to abuse trusted relationships, or as the initial means itself to launch an attack. All of these actions leverage some form of account privilege which can be restricted by Delinea PAM, thereby eliminating the ability for threat actors to utilize these techniques.

# Execution

## Goal

To run attacker-controlled code on a victim organization's endpoint as the initial step to achieving broader goals, such as Lateral Movement.

## Techniques Delinea PAM Helps to Mitigate

| Execution | |
|---|---|
| T1651 | Cloud Administration Command |
| T1059 | Command and Scripting Interpreter |
| T1609 | Container Administration Command |
| T1610 | Deploy Container |
| T1203 | Exploitation for Client Execution |
| T1106 | Native API |
| T1053 | Scheduled Task/Job |
| T1648 | Serverless Execution |
| T1129 | Shared Modules |
| T1072 | Software Deployment Tools |
| T1569 | System Services |
| T1204 | User Execution |
| T1047 | Windows Management Instrumentation |

## How Delinea PAM Helps

In short, most *Execution* actions require some level of privileged access – whether on-premises or in the cloud. Through the removal of local admin rights from local and domain accounts, the implementation of least privilege for user accounts, and the restrictive request-based access to privileged accounts, Delinea PAM creates a working environment in which any valid account compromised by a threat actor is unable to perform malicious execution activities.

And in the cloud, by removing local IaaS IAM accounts and using SAML-based federation, Delinea PAM can control who is permitted to log in to IaaS Management Consoles to reduce the attack surface.

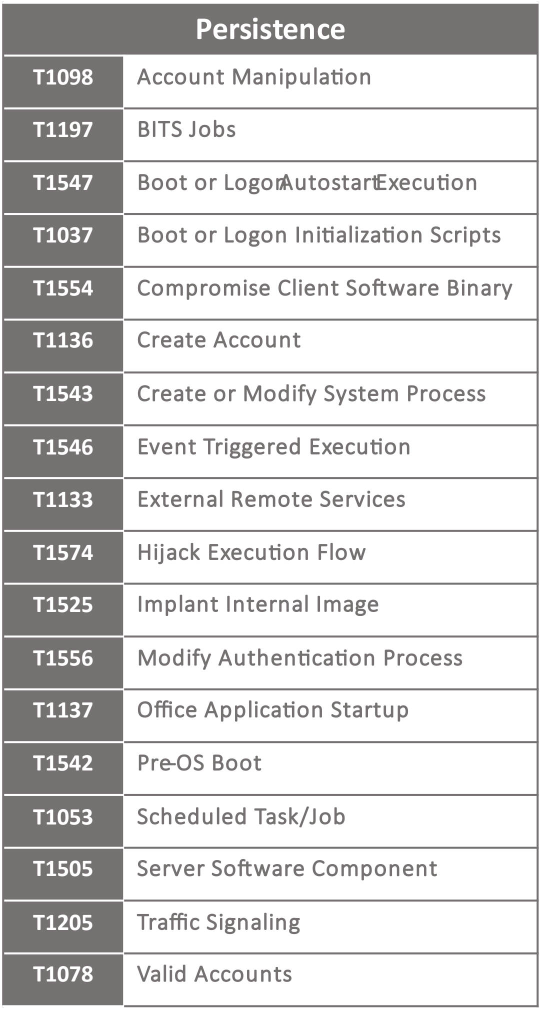
So, should an action within any one of the 13 primary *Execution* techniques require elevated privileges, the action is dead on arrival and can’t be executed.

# Persistence

## Goal

Maintain access to systems regardless of restarts, changed credentials, and other methods of cutting off threat actor access.

## Techniques Delinea PAM Helps to Mitigate



| Persistence | |
|---|---|
| T1098 | Account Manipulation |
| T1197 | BITS Jobs |
| T1547 | Boot or LogonAutostartExecution |
| T1037 | Boot or Logon Initialization Scripts |
| T1554 | Compromise Client Software Binary |
| T1136 | Create Account |
| T1543 | Create or Modify System Process |
| T1546 | Event Triggered Execution |
| T1133 | External Remote Services |
| T1574 | Hijack Execution Flow |
| T1525 | Implant Internal Image |
| T1556 | Modify Authentication Process |
| T1137 | Office Application Startup |
| T1542 | Pre-OS Boot |
| T1053 | Scheduled Task/Job |
| T1505 | Server Software Component |
| T1205 | Traffic Signaling |
| T1078 | Valid Accounts |

## How Delinea PAM Helps

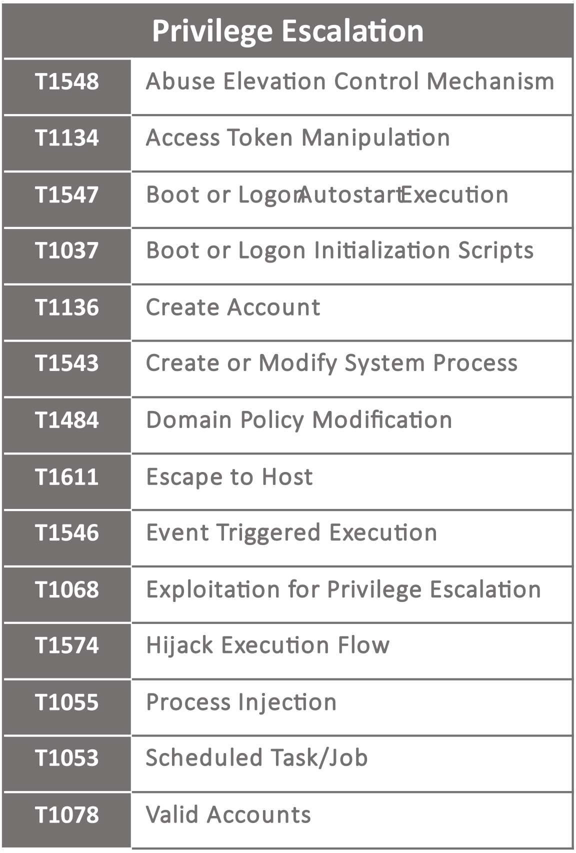
Every one of the *Persistence* techniques – with the exception of the threat actor maintaining a valid account (albeit a valid account with no elevated privileges) they have compromised and, therefore, can continually log back into – requires some form of privileged access to a workstation or server, its' operating system, a cloud environment, or container environment. Delinea PAM strips out and restricts privileged access, thereby reducing a threat actor's ability to persist to almost zero.

# Privilege Escalation

## Goal

To gain elevated privileges and permissions on a system or network.

## Techniques Delinea PAM Helps to Mitigate



| Privilege Escalation | |
|---|---|
| T1548 | Abuse Elevation Control Mechanism |
| T1134 | Access Token Manipulation |
| T1547 | Boot or Logon Autostart Execution |
| T1037 | Boot or Logon Initialization Scripts |
| T1136 | Create Account |
| T1543 | Create or Modify System Process |
| T1484 | Domain Policy Modification |
| T1611 | Escape to Host |
| T1546 | Event Triggered Execution |
| T1068 | Exploitation for Privilege Escalation |
| T1574 | Hijack Execution Flow |
| T1055 | Process Injection |
| T1053 | Scheduled Task/Job |
| T1078 | Valid Accounts |

## How Delinea PAM Helps

Delinea PAM vaults away shared privileged accounts and enforces least privilege on workstations and servers to strictly control privilege elevation, including running executables and API functions used to elevate created credentials. With the threat actor only having access to a lower-level user account, nearly all of the techniques under *Privilege Escalation* are unable to take place.

In cases where *Exploitation for Privilege Escalation* takes place, and an application vulnerability is responsible for granting privileged access to a threat actor, Delinea PAM uses behavior analytics to identify anomalous behavior and alerts security teams to respond.

# Defense Evasion

## Goal

To avoid detection throughout the duration while the system or network is compromised.

## Techniques Delinea PAM Helps to Mitigate

| Defense Evasion | | | |
|---|---|---|---|
| T1548 | Abuse Elevation Control Mechanism | T1601 | Modify System Image |
| T1134 | Access Token Manipulation | T1599 | Network Boundary Bridging |
| T1197 | BITS Jobs | T1027 | Obfuscated Files or Information |
| T1612 | Build Image on Host | T1647 | PlistFile Modification |
| T1140 | Deobfuscate/Decode Files or Informatio | T1542 | Pre-OS Boot |
| T1610 | Deploy Container | T1055 | Process Injection |
| T1006 | Direct Volume Access | T1620 | Reflective Code Loading |
| T1484 | Domain Policy Modification | T1207 | Rogue Domain Controller |
| T1222 | File and Dir. Permissions Modification | T1553 | Subvert Trust Controls |
| T1564 | Hide Artifacts | T1218 | System Binary Proxy Execution |
| T1574 | Hijack Execution Flow | T1216 | System Script Proxy Execution |
| T1562 | Impair Defenses | T1205 | Traffic Signaling |
| T1070 | Indicator Removal | T1127 | Trusted Dev. Utilities Proxy Execution |
| T1202 | Indirect Command Execution | T1535 | Unused/Unsupported Cloud Regions |
| T1036 | Masquerading | T1550 | Use Alternate Authentication Materia |
| T1556 | Modify Authentication Process | T1078 | Valid Accounts |
| T1578 | Modify Cloud Compute Infrastructure | T1600 | Weaken Encryption |
| T1112 | Modify Registry | T1220 | XSL Script Processing |

## How Delinea PAM Helps

Nearly all *Defense Evasion* techniques rely on running within a privileged user context. By properly removing privileged access from user accounts and using policy-based enforcement of access to privileged accounts, each of these techniques above are rendered inoperable.

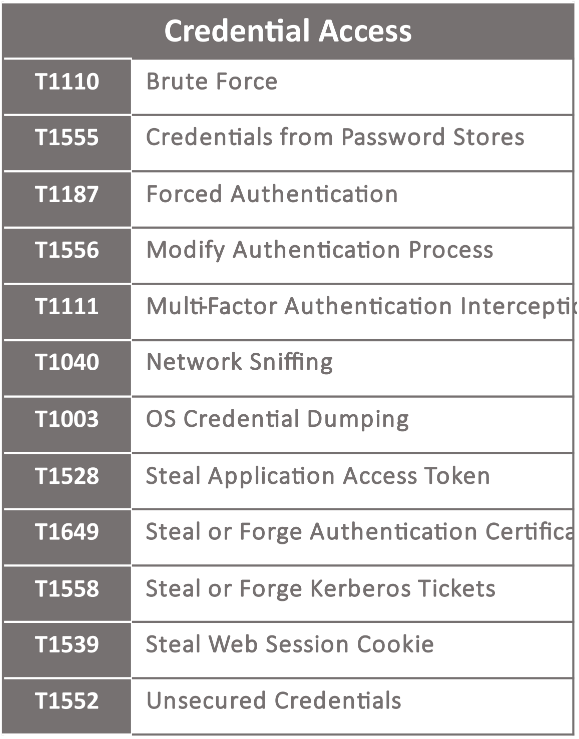
Should an alternative authentication method be used that facilitates bypassing a PAM solution (e.g., exploiting a zero-day vulnerability that yields privileged access) and evades detection, all activity by privileged accounts is analyzed for unusual behaviors, whereby security teams are alerted.

## Credential Access

### Goal

To obtain usernames and corresponding authentication factors (passwords, hashes, Kerberos tickets, etc.).

### Techniques Delinea PAM Helps to Mitigate



| Credential Access | |
|---|---|
| T1110 | Brute Force |
| T1555 | Credentials from Password Stores |
| T1187 | Forced Authentication |
| T1556 | Modify Authentication Process |
| T1111 | Multi-Factor Authentication Intercepti |
| T1040 | Network Sniffing |
| T1003 | OS Credential Dumping |
| T1528 | Steal Application Access Token |
| T1649 | Steal or Forge Authentication Certifica |
| T1558 | Steal or Forge Kerberos Tickets |
| T1539 | Steal Web Session Cookie |
| T1552 | Unsecured Credentials |

### How Delinea PAM Helps

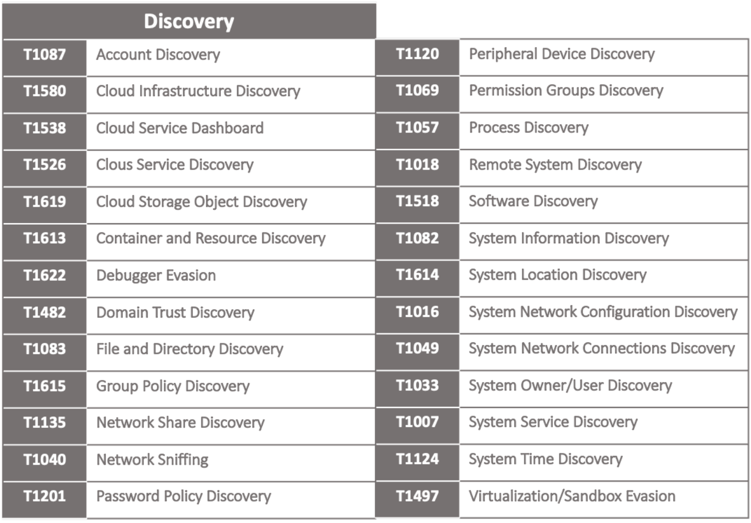
Least privilege, MFA policies, and vaulted privileged credentials all enforced by Delinea PAM removes a threat actor's ability to perform any of the techniques listed above. In cases where authentication is bypassed (as in the case of *Modifying Authentication Processes*, *MFA Interception*, and *Stealing or Forging Kerberos Tickets*) privileged account activity is analyzed for unusual behavior with security teams notified if any is found.

# Discovery

## Goal

To gain information about the compromised system or network.

## Techniques Delinea PAM Helps to Mitigate



| Discovery | | | |
|---|---|---|---|
| T1087 | Account Discovery | T1120 | Peripheral Device Discovery |
| T1580 | Cloud Infrastructure Discovery | T1069 | Permission Groups Discovery |
| T1538 | Cloud Service Dashboard | T1057 | Process Discovery |
| T1526 | Clous Service Discovery | T1018 | Remote System Discovery |
| T1619 | Cloud Storage Object Discovery | T1518 | Software Discovery |
| T1613 | Container and Resource Discovery | T1082 | System Information Discovery |
| T1622 | Debugger Evasion | T1614 | System Location Discovery |
| T1482 | Domain Trust Discovery | T1016 | System Network Configuration Discovery |
| T1083 | File and Directory Discovery | T1049 | System Network Connections Discovery |
| T1615 | Group Policy Discovery | T1033 | System Owner/User Discovery |
| T1135 | Network Share Discovery | T1007 | System Service Discovery |
| T1040 | Network Sniffing | T1124 | System Time Discovery |
| T1201 | Password Policy Discovery | T1497 | Virtualization/Sandbox Evasion |

## How Delinea PAM Helps

Any kind of *Discovery* technique that does not require elevated privileges (e.g., obtaining IP address information with an *ipconfig* command) will certainly be available to the threat actor. Delinea PAM's strength comes into play when critical details that require privileged access are made inaccessible due to the lack of needed access on the part of the threat actor.

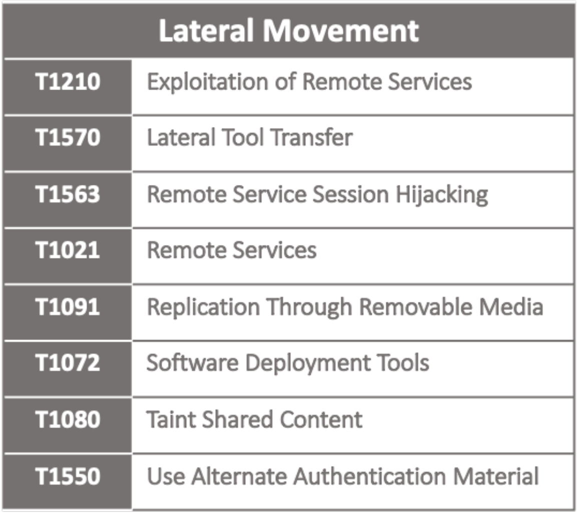
Delinea PAM's management of privileged access in the cloud also assists in mitigating the gaining of access to discover cloud-related infrastructure, services, containers, and storage.

# Lateral Movement

## Goal

To to gain access to and control a remote system within the victim network.

## Techniques Delinea PAM Helps to Mitigate



| Lateral Movement | |
|---|---|
| T1210 | Exploitation of Remote Services |
| T1570 | Lateral Tool Transfer |
| T1563 | Remote Service Session Hijacking |
| T1021 | Remote Services |
| T1091 | Replication Through Removable Media |
| T1072 | Software Deployment Tools |
| T1080 | Taint Shared Content |
| T1550 | Use Alternate Authentication Material |

## How Delinea PAM Helps

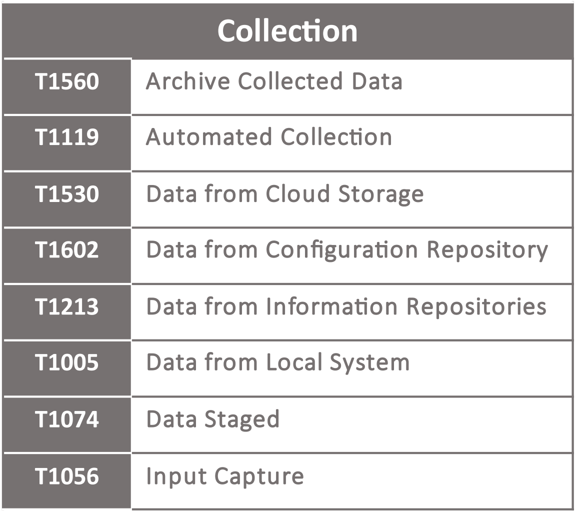
The majority of lateral movement actions relies on the use of malicious tools (read: applications). Delinea PAM prevents the use of such tools within the context of an established least privilege environment. Delinea PAM also enforces MFA on privilege elevation. Think of this as "MFA for sudo" or "MFA for Run as Administrator" and the benefit in preventing lateral movement is clear. Additionally, should a privileged account be compromised, Delinea PAM can detect abnormal behaviors and alert security teams to take action.

# Collection

## Goal

To collect information from various types of repositories, usually to identify data to be exfiltrated.

## Techniques Delinea PAM Helps to Mitigate



| Collection | |
|---|---|
| T1560 | Archive Collected Data |
| T1119 | Automated Collection |
| T1530 | Data from Cloud Storage |
| T1602 | Data from Configuration Repository |
| T1213 | Data from Information Repositories |
| T1005 | Data from Local System |
| T1074 | Data Staged |
| T1056 | Input Capture |

## How Delinea PAM Helps

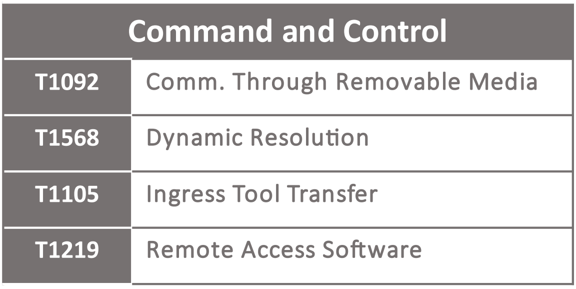
Strict enforcement of least privilege on workstations and servers (whether on-premises or in the cloud) limits visibility and access to resources, the ability to install malicious tools, and the data they wish to collect.

# Command and Control

## Goal

To communicate with attacker-controlled systems both within the victim network and across the Internet using common protocols and communication methods to avoide detection.

## Techniques Delinea PAM Helps to Mitigate



| Command and Control | |
|---|---|
| T1092 | Comm. Through Removable Media |
| T1568 | Dynamic Resolution |
| T1105 | Ingress Tool Transfer |
| T1219 | Remote Access Software |

## How Delinea PAM Helps

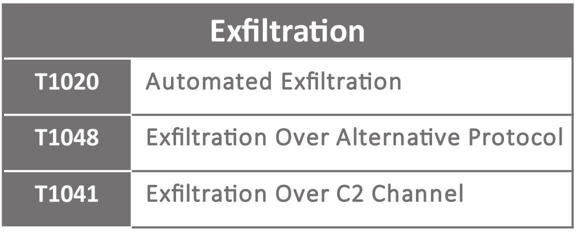
By enforcing least privilege, Delinea PAM can prevent threat actors from gaining privileged access on systems, limiting their ability to make use of malware to establish connections, use protocols such as FTP, use remote access software, and the use of removeable media. Use of remote access software installed for Desktop Support teams (for example) can be controlled to permit access only by specific users.

# Exfiltration

## Goal

To steal data from the victim network using methods to avoid detection.

## Techniques Delinea PAM Helps to Mitigate



| Exfiltration | |
|---|---|
| T1020 | Automated Exfiltration |
| T1048 | Exfiltration Over Alternative Protocol |
| T1041 | Exfiltration Over C2 Channel |

## How Delinea PAM Helps

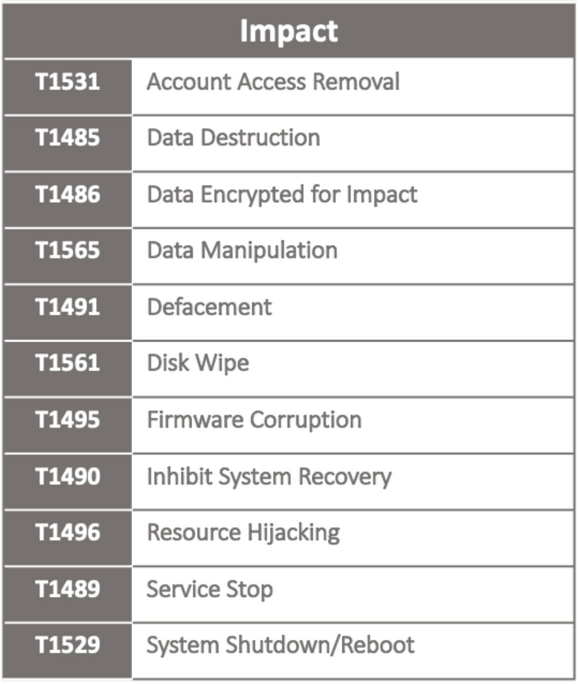
On workstations, the execution of applications used for automatic exfiltration can be blocked using Delinea PAM, as can the use of specific networking protocols for exfiltration, and the installation of Command and Control (C2) malware. On servers, elevation to privileged access is controlled, limiting the ability to run scripting and/or malicious exfiltration tools. And should a privileged account be compromised, analysis of privileged behavior helps to identify unusual communications (read: exfiltration) used to alert security teams.

# Impact

## Goal

To disrupt operations by manipulating, interrupting, or destroying data, systems, and processes.

## Techniques Delinea PAM Helps to Mitigate



| Impact | |
|---|---|
| T1531 | Account Access Removal |
| T1485 | Data Destruction |
| T1486 | Data Encrypted for Impact |
| T1565 | Data Manipulation |
| T1491 | Defacement |
| T1561 | Disk Wipe |
| T1495 | Firmware Corruption |
| T1490 | Inhibit System Recovery |
| T1496 | Resource Hijacking |
| T1489 | Service Stop |
| T1529 | System Shutdown/Reboot |

## How Delinea PAM Helps

Every one of the above techniques requires either system- or domain-level privileged access to accomplish. By enforcing least privilege, limiting privileged use of applications, and restricting access to privileged accounts, threat actors are unable to perform these techniques.

## Mitigating Threat Actions with Delinea PAM

The success of every cyberattack relies completely on whether the threat actor gains enough privileged access to perform the techniques listed in the MITRE ATT&CK Framework.  Through the use of limiting what users can do through least privilege enforcement, as well as restricting when, where, and how privileged access can be utilized, Delinea PAM significantly reduces (if not completely eliminates) the threat surface and a threat actor’s ability to do anything malicious, effectively stopping an attack in its tracks.

**Quickly become conversational about the MITRE ATT&CK Framework.**

The MITRE ATT&CK Framework is more than just a database of threat actions; it serves as the basis for better understanding whether the people, process, and technologies you have in place are actually going to help stop threat actions. In this eBook, you'll learn about how the Framework is organized, how to use it, and how it can serve as the basis for determining where the gaps in your security exist.

## About Derek A. Smith

With over 30 years in the security industry, Derek A. Smith is a former government agent, cybersecurity SME, holds a variety of certifications (CISSP, CEH, CCISO, Security+, etc.), eight college degrees, is a published author, conference speaker, cybersecurity analyst for several international and local television news stations, government program manager, and more.