WHITE PAPER

IronNet™

5 practical ways for a CISO to use the MITRE ATT&CK® Framework

INTRODUCTION

A framework for frameworks

Aligning to frameworks is a sound approach for building or maturing a cybersecurity program. Why start from scratch? Frameworks such as NIST Cybersecurity Framework and ISO 27001, for example, offer standardized and prioritized guidance for strategic decision-making and best practices. Creating a risk register, ensuring backup processes, and developing an asset management program for high-value assets are foundational. All are elements of a strong and holistic cybersecurity program.

Yet a major gap remains. Indeed, these widely adopted frameworks may provide essential guidance for structuring and governing a security program, but they were never designed to provide the practical direction every CISO needs for identifying current cyber threats and evaluating whether controls already deployed will be sufficient to defend against them.

This is where the MITRE ATT&CK® Framework comes into play: it is a way to complement the common programmatic frameworks in order to evaluate the ability of your security capabilities to combat current cyber threats.

In the past, the process of determining the goal of an adversary was essentially based on institutional knowledge and gut instincts. Now, the specific attack characteristics mapped across ATT&CK® can provide valuable and objective insights into the target of the threat and its current phase. This perspective allows your SOC team to pinpoint the potential impacts on your organization, evaluate the effectiveness of your existing protection and controls, and prioritize your response.

Prescribed support for your risk assessment activities

ATT&CK® follows the threat intrusion cycle and delivers a crowd-sourced deep dive into how attacks are built and carried out, detailing the common methods and ramifications. By mapping adversaries' tactics, techniques, and procedures (TTP) — based on real-world observations — within a standardized matrix, you can more clearly see where you need to better batten the security hatches. Accordingly, it is an effective and useful resource for seeing and analyzing the structure of an attack and assessing where it has (or potentially may have) an impact on your organization.

From there, you can identify whether you have the capabilities you need to detect the relevant threats. In this way, you can leverage ATT&CK® to inform and support your risk assessment activities.

Take special note of this most important aspect of the MITRE ATT&CK® Framework for CISOs in particular:

It provides a clear way for you to measure your team's capabilities — at both baseline and over time — in relation to threat trends.

By looking to the matrix to help measure your team's capabilities, you can justify training and investment decisions in a very defensible manner based on the detection gaps revealed. You can track the performance of your team's defensive posture against adversaries.

But this process can be challenging for any CISO, regardless of your SOC team's maturity or the cybersecurity initiatives you currently have implemented across your people, process, and technology. Where do you begin? And what are practical use cases for using the MITRE ATT&CK® Framework in this way?

MITRE | ATT&CK®

1. A more granular approach to **clearly defining corporate risk**

Begin with identifying corporate risk in a granular way, as enabled by ATT&CK®. A theoretical scenario illustrates what this means.

Suppose, for example, that you receive intelligence that "APT33 is targeting the financial sector." As CISOs, we have to be honest with ourselves: few of us really know what this means. And, more important, can you answer the following questions realistically:

"Do we really have the capabilities we need to detect that particular threat and effectively respond to it?"

"How good are the detection tools I've already invested in?"

Without question, these are challenging questions for any CISO to answer off the bat. When your team gives an "I don't know" answer, it often means "no."

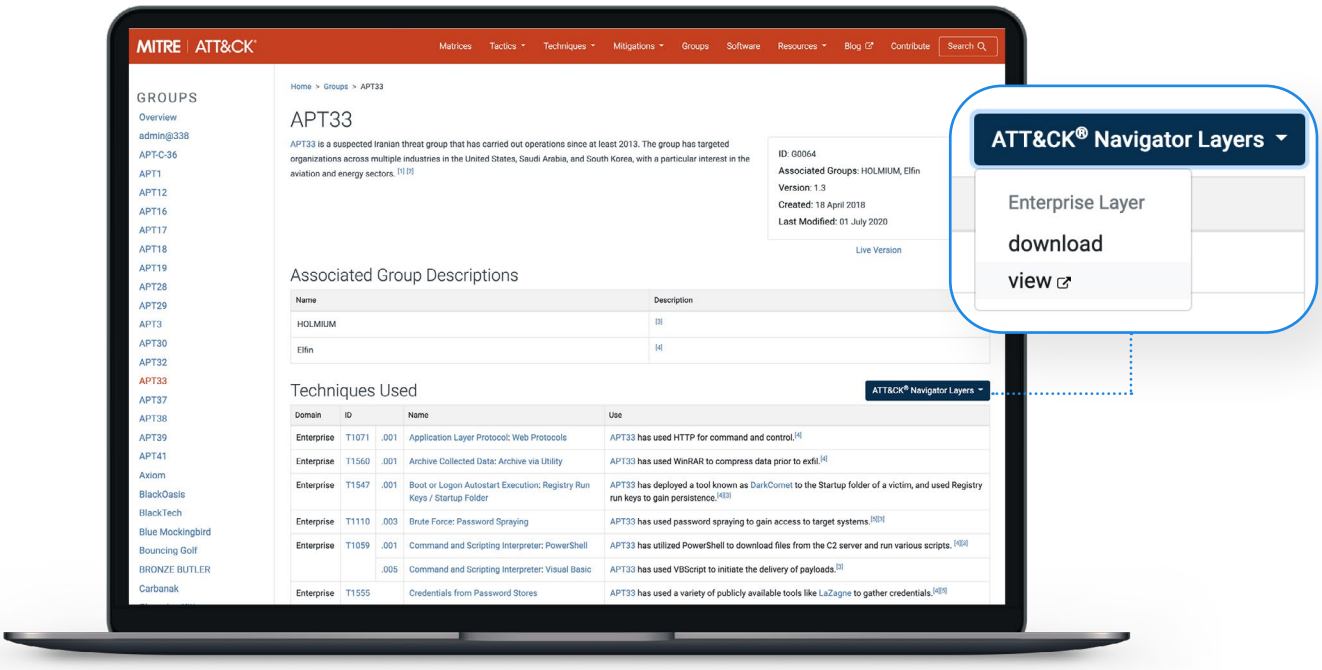
By using the MITRE ATT&CK® Framework strategically, however, you can proactively seek practical answers to these questions as part of your internal and external assessment activities. Here are some questions to use in that assessment:

1. What does the attack surface look like for other companies in my sector?
2. What real-world observations have been made regarding these threats?
3. Do I have the internal and external resources (people, processes, and technology) to respond to these specific threats?
4. How can I best detect the specific adversarial techniques, captured in the MITRE ATT&CK® Framework?
5. Will my current technology stack identify these threats, which reflect behaviors on the network, or only known signatures and Indicators of Compromise?
6. How early in the intrusion cycle can the SOC team see such a threat?

2. Adopting a **confidence-level approach** to assessment

Although everyone's environment is different and has unique capabilities and vulnerabilities, everyone can take a confidence-level approach to assessing the risks specific to the enterprise by using ATT&CK® as a lens for their own team.

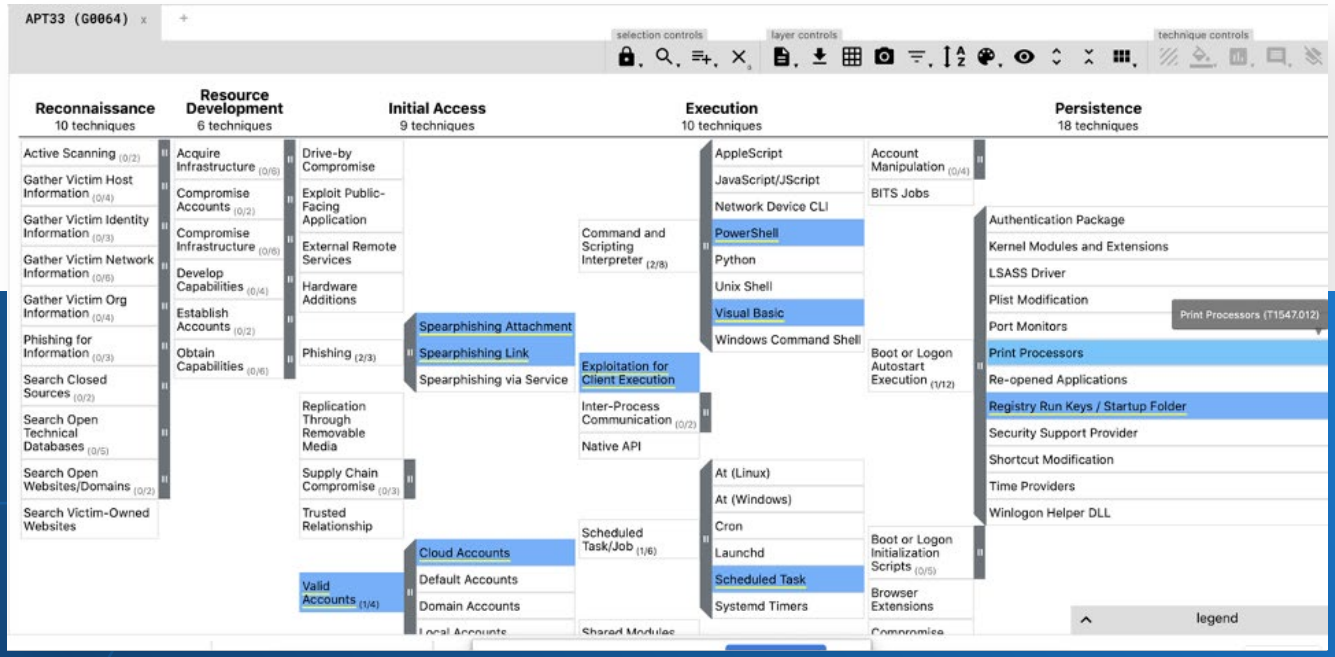
Coming back to the aforementioned example, let's assume a financial firm receives a notice from the FBI that APT33 is targeting its organization. By using the ATT&CK® matrix, the security team can assess their current ability to defend against this threat.



By visiting the APT33 page on the ATT&CK® site, you can get a sense of the techniques and software used; however, the real power of this site can be realized by using the ATT&CK® Navigator.

In this format, you can get a good visualization of the attacks leveraged by this attacker and where they fit into the intrusion cycle. Then you can start to determine if you have the capability to detect these threats in your environment.

Visualization of APT33 TTPs



From here, in a separate doc, make a list of the items highlighted in blue.

Detection Capabilities

	High	Med	Low
Valid Accounts			
Spearphishing Attachment			
Spearphishing Link			
Cloud Accounts			
Power Shell			
Visual Basic			

Rating your capabilities

Now you can start to determine your ability to detect the specific techniques associated with the attack. There is no need to be too granular; instead, simply note your visibility in that area. High (green) indicates logs/capabilities exist, Medium (yellow) logs/capabilities may exist, and Low (red) logs/capabilities do not exist.

- High: Logs/capabilities exist
- Medium: Logs/capabilities may exist
- Low: Logs/capabilities do not exist

Direct your threat hunters, threat intelligence, or incident response teams to those green and yellow items to determine if they can identify impacted systems, or to help guide your future capability acquisition strategy.

For red items, prioritize them based on the TTPs you have learned about the adversary, and work with technical teams to determine if improvements can be quickly implemented. Consider if capabilities can be obtained simply with a license upgrade or logging configuration, or whether a longer-term solution of training, services, or product changes is needed.

3. **Assessing the maturity** of internal teams

After your team identifies TTPs and their relevant impact on your organization, you will want to create benchmarks for measuring your ability to defend at every stage. This is not a one-size-fits-all effort. The question to ask, then, is, "What is the likelihood of this risk vs. the potential damage that it would cause at my specific organization?" Map the risk scenarios against current capabilities to see if the identified risk meets a material risk to the business. Between your internal teams, external partners, and the technology capabilities, you can see where you are more susceptible to a threat or bad actor.

Since ATT&CK® provides a formalized, common language and community-agreed upon framework, if you know the adversary is showing signs of step 1, 2, and 3, then you have a good sense of what's coming for step 4. In short, it's a playbook. Before the MITRE ATT&CK® Framework, there were people who fundamentally knew that hacking is not magic, but this expertise did not rise to a mature understanding of how these techniques fit together. Now, with ATT&CK®, you can gain a panoramic view of the threat, recognize its lifecycle and target, and enable proactive defenses instead of reactive ones. The next step is to look at the tactics to assess where your company is the strongest or the weakest. For example,

"Our team has a weakness in Recon, so we need to take measures to enhance our security posture by working toward being able to identify port scanning on our business-critical resources."

"We lack experience with lateral movement and know that is the path adversaries are taking right now, so we need to first increase visibility into the different segments of our network in order for our security team to begin implementing analytics that have visibility into the avenues used for lateral movement."

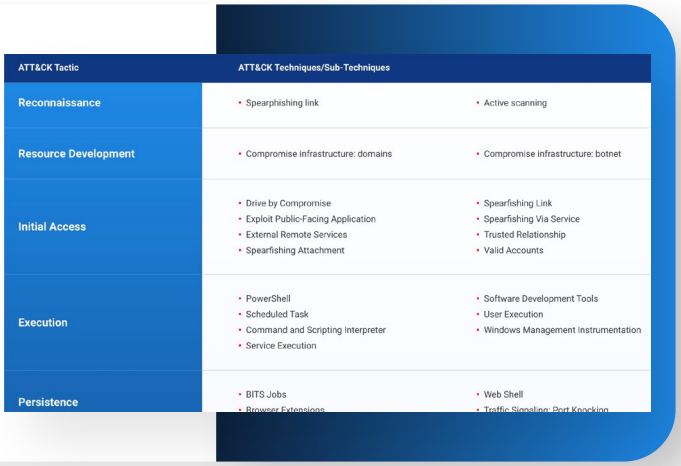
"After the SolarWinds/SUNBURST supply chain attack, we are aware of a gap in visibility in Command and Control (C2) methods leveraging DNS tunneling which could bypass our detections. Based on the risk it poses, we will need to implement new capabilities to filter through the benign DNS traffic and increase our ability to view the suspicious and malicious DNS activity."

4. **Increasing your visibility** of the threat landscape

The risk assessment exercise often reveals that network detection and response (NDR) capabilities are missing from a robust cybersecurity program. In fact, all TTPs mapped to the ATT&CK® matrix are based on adversarial behaviors on the network. Being able to detect these behaviors early in the intrusion cycle is crucial. While hackers can easily change signatures, it's difficult for them to change their TTPs, or behaviors, quickly.

An NDR platform rounds out your detection capabilities of such behaviors, or those "unknown" threats that are identifiable only by how they behave on the network. These are the threats that signature-based tools and endpoint detection and response (EDR) solutions can miss, making NDR an essential part of what Gartner® coined as the SOC Visibility Triad, which suggests the level of security visibility you need to defend. NDR platforms, such as IronNet's IronDefense, are especially effective at detecting threats on these portions of the ATT&CK® Framework for Enterprise.

See a snapshot of how IronDefense analytics map to the ATT&CK® Framework.

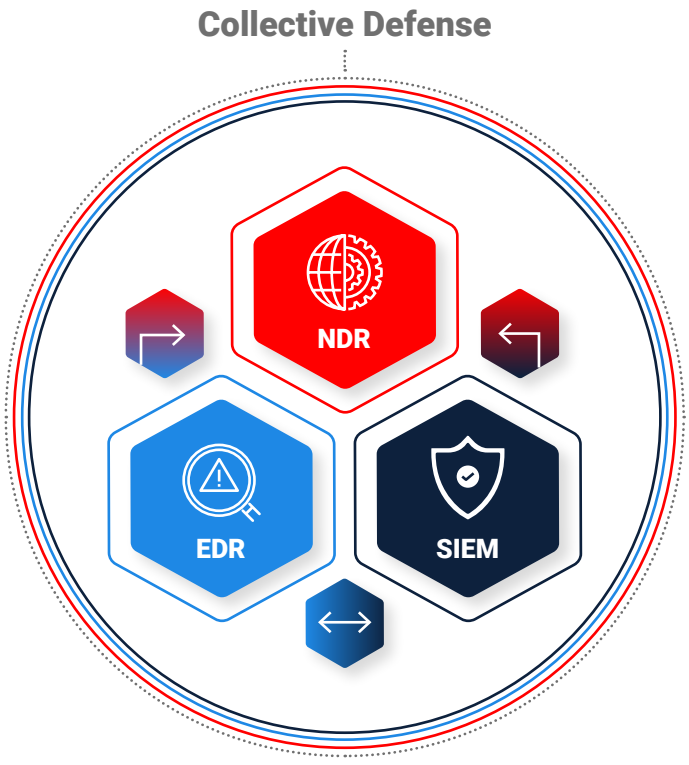


ATT&CK Tactic	ATT&CK Techniques/Sub-Techniques	
Reconnaissance	• Spearphishing link	• Active scanning
Resource Development	• Compromise infrastructure: domains	• Compromise infrastructure: botnet
Initial Access	• Drive by Compromise • Exploit Public-Facing Application • External Remote Services • Spearfishing Attachment	• Spearfishing Link • Spearfishing Via Service • Trusted Relationship • Valid Accounts
Execution	• PowerShell • Scheduled Task • Command and Scripting Interpreter • Service Execution	• Software Development Tools • User Execution • Windows Management Instrumentation
Persistence	• BITS Jobs • Browser Extensions	• Web Shell • Traffic Signaling: Port Knocking

In short, the truth is in the traffic. Given that the network is ubiquitous, all movement to and from an endpoint is via the network. What's more, the network is so vast that it is nearly impossible for an attacker to fully cover their tracks.

This is why companies are increasingly turning to NDR solutions. With the right artificial intelligence (AI)/machine learning (ML) algorithms in your defense portfolio, you can tackle the challenge of processing voluminous amounts of network data to identify indicators of malicious behaviors. Armed with behavioral analytics, an NDR solution such as IronNet's IronDefense completes the kind of security toolset needed for effective cyber defense.

Collective Defense in cybersecurity draws on behavioral analytics and orchestrates threat information sharing in real time, generating a dynamic relationship among SIEM, EDR, and NDR tools. IronNet's IronDome, the platform that empowers this collaborative engagement, is the engine that can transform the SOC Visibility Triad into a dynamic pyramid, making each tool stronger and more effective.



5. **Strengthening your defensive posture** now and over time

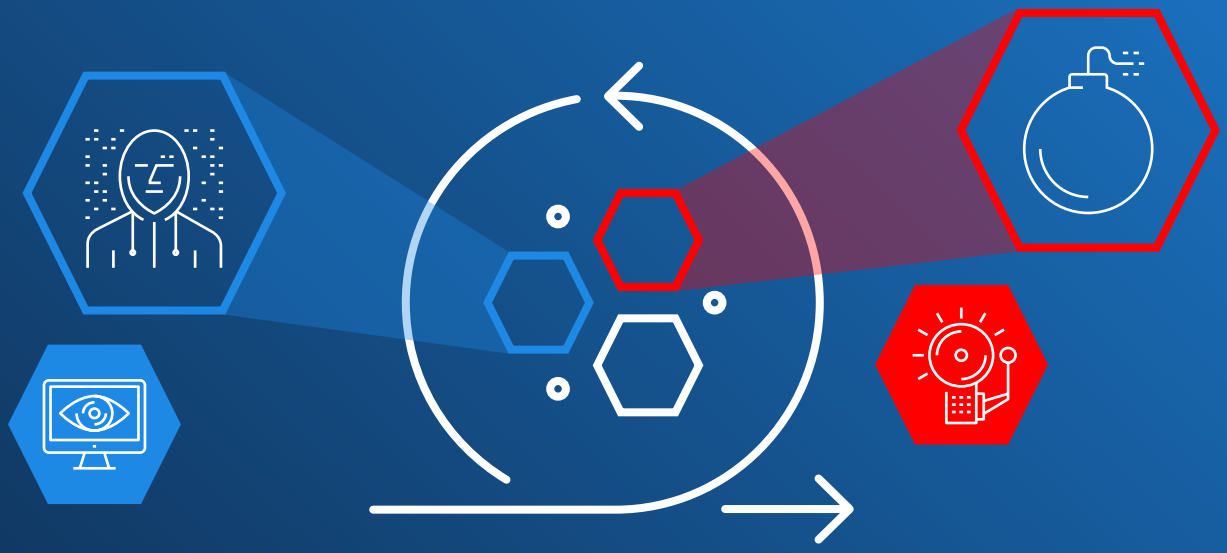
The beauty of ATT&CK® is that it is a living, breathing matrix. As such, it allows you to look at threats in the here and now as well as trends over time, enabling you to align your posture in relation to immediate and emerging threats. The framework provides rationale for making the agile decision to deprioritize X project in response to Y current threat. It helps you pivot to align your team and capabilities against specific, observed threats.

What's more, detecting and understanding threats is not just about what we know today from a retrospective position. The MITRE ATT&CK® Framework is established so well as an open-source matrix that it will help uncover and reveal other attack groups that are coming into play, changes in attack groups, and/or changes in TTPs as adversaries cherry-pick their targets with altered TTPs.

CONCLUSION

Detecting threats "left of boom"

In military vernacular, the phrase "left of boom" refers to disrupting insurgent activity before the adversaries can build or plant bombs. The same holds true for cyber activity: stop the adversaries before they reach the exploitation or exfiltration phases. If you do not — or cannot — act fast enough, you're giving valuable dwell time to the network intruder to achieve a successful heist of your organization's data; loss of network, system, or asset control; or drain of money.



But your "right of boom" internal capabilities need to be strong first. The MITRE ATT&CK® Framework can be used to gain clarity of your organization's weak spots and, in turn, to prioritize cybersecurity projects. Measuring and strengthening your team's capabilities will focus your security transformation and fortify your ability to respond to cyber threats captured globally across the ATT&CK® matrix.

In this way, the MITRE ATT&CK® Framework is a fundamental and practical way for you to assess your organization's ability to defend against cyber threats.

IronNet™

Connect with us to learn how to partner with IronNet to strengthen your company's security posture.