ATTACKIQ

White Paper

The Security Practitioner's Guide to MITRE ATT&CK®

Notice

AttackIQ® publications are made available solely for general information purposes. The information contained in this publication is provided on an "as is" basis. Any additional developments or research since the date of publication will not be reflected in this report.

Table of Contents

What is MITRE ATT&CK®?

The MITRE Corporation, a non-profit, was founded in 1958. MITRE Corp. released the MITRE ATT&CK® cybersecurity framework (Adversarial Tactics, Techniques, and Common Knowledge) in 2015. Today, the MITRE ATT&CK framework is the most authoritative, comprehensive, and complete set of up-to-date attack techniques and supporting tactics. Globally-accessible and based on real-world data, the ATT&CK knowledge base is foundational for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. MITRE's stature in the cybersecurity community and the independence of its intellectual property in the ATT&CK matrix make it the ideal platform from which security operations management, executive staff, and boards of directors can objectively evaluate and measure cybersecurity controls' performance, risk, and capability.

MITRE ATT&CK is Complementary and Unique

The MITRE ATT&CK framework is not the only cybersecurity framework that can help you defend your enterprise.

The MITRE ATT&CK framework is not the only cybersecurity framework that can help you defend your enterprise. Other frameworks such as ISACA®'s COBIT, Lockheed Martin's Cyber Kill Chain®, ISO/IEC 27001, and the NIST cybersecurity framework can also be core components of your cyberdefense.

The rate of framework adoption has dramatically accelerated in 2020. Most large enterprises have multiple frameworks in use. Data suggests that in large global enterprises, market share for CIS-CSC, ISO 27001, and ISACA's COBIT (5 and 2019) is well over 30 percent. These frameworks are all popular, along with NIST CSF and the expanded family of NIST cybersecurity standards.

MITRE ATT&CK has experienced rapid adoption due to its unique attributes and particular orientation. MITRE ATT&CK presents the best way to think like an attacker and to understand and anticipate the tactics, techniques, and procedures they will use. MITRE ATT&CK takes cyberdefense planning and preparation to the edge of what is possible today.

Why is the MITRE ATT&CK Framework Important?

MITRE ATT&CK is, in both depth and breadth, the most extensive attack knowledge base, providing suggested mitigation techniques, detection procedures, and other relevant technical information.

MITRE ATT&CK is, in both depth and breadth, the most extensive attack knowledge base, providing suggested mitigation techniques, detection procedures, and other relevant technical information. MITRE has expanded the Kill Chain to include a wide variety of tactics that are then supported by specific techniques. This organized approach enables you to select and analyze attacks methodically and compare them to the capabilities of your security controls to understand the gaps.

Once you understand these gaps, you can then rationally expand your security controls and adjust your budgets. Using the most extensive, in-depth, organized, and strongly supported knowledge base of adversarial behavior, you can review your security controls and gain visibility into gaps in your defenses. Security practitioners can more rapidly and easily identify critical problems for remediation. This objective assessment provides a data-driven approach to prioritizing and scaling your cybersecurity program and budget.

MITRE ATT&CK Provides a Common Language

MITRE ATT&CK has brought a well-matured taxonomy of the tactics and techniques that may be leveraged by any prospective attacker. For the first time, there is a common lexicon that enables stakeholders, cyberdefenders, and vendors to communicate on the exact nature of a threat and the objective assessment of the cyberdefense plan that can defeat it. This common lexicon brings a universal language that precisely describes the procedures of an attacker and the techniques they deploy, enabling a more accurate assessment of threats and a faster, better-targeted response.

How is MITRE ATT&CK Structured?

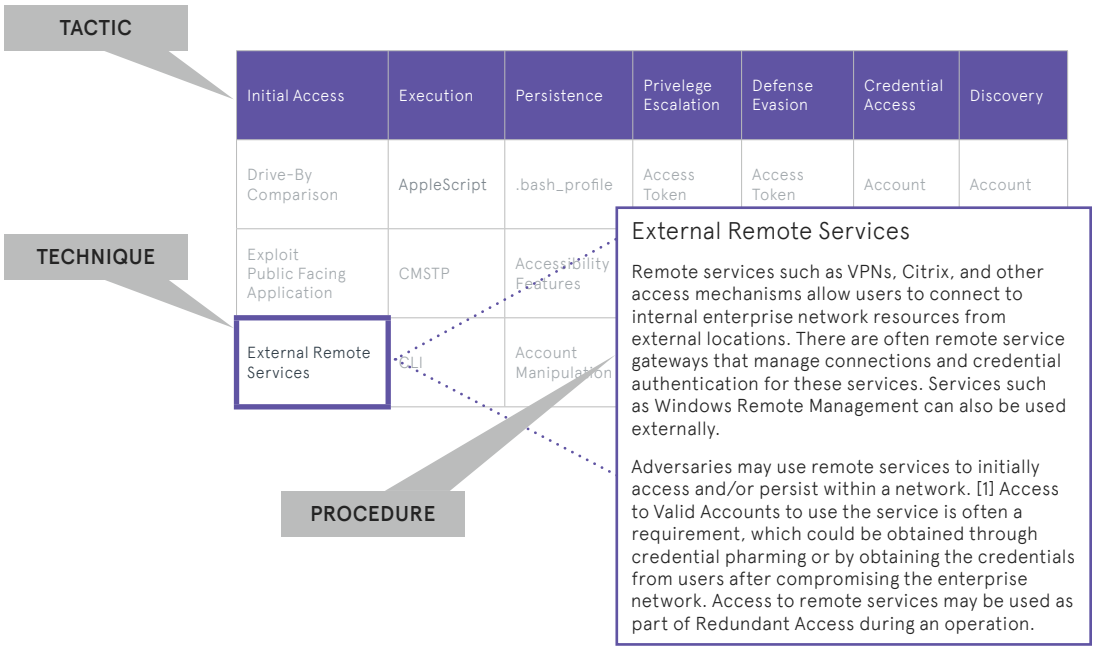
The MITRE ATT&CK enterprise matrix provides a tabular view of all attacker tactics and techniques that might leverage Windows, Mac, and Linux environments. Across the top are headings listing the 12 tactics defined by MITRE ATT&CK. Each of the 12 tactics is a column that shows between nine and 67 techniques that implement a particular tactic. Often, several techniques are used in one or more tactics. A tactic clearly defines the goals of the attacker. A technique describes the different ways that a cyberattacker can achieve the end goals of the tactic.

How is MITRE ATT&CK Structured? (cont.)

MITRE ATT&CK has brought a well-matured taxonomy of the tactics and techniques that may be leveraged by any prospective attacker.

For example, one primary tactic is Initial Access. The Initial Access Tactic column includes all of the techniques that an attacker might use to try and gain higher-level permissions that would then be used, in turn, to compromise your defenses. The MITRE ATT&CK matrix also announced more features to support the cloud in late 2019.

Table - The MITRE ATT&CK Matrix



What are ATT&CK Groups and How Can They Help?

ATT&CK Groups help you identify attackers more precisely. This database shows you all of the known names and suspected identifies of attackers. Most interesting, it also shows you which techniques and software tools were attributed to the different attacker groups. As of Dec. 15, 2019, this section has 91 groups defined and will continue to grow. Note that this data is not necessarily complete. This data is derived from available sources that MITRE monitors on an ongoing basis.

What are ATT&CK Groups and How Can They Help? (cont.)

ATT&CK Groups help you identify attackers more precisely.

An example of an ATT&CK group is the bank-targeting group Carbanak and its various aliases. FIN7 also uses Carbanak malware, but it and the Carbanak group appear to be two separate groups using the same malware, and they are thus tracked separately.

- Associated Group Descriptions for Carbanak
- Anunak
- Carbon Spider

How Do You Get Started with MITRE ATT&CK?

The best place to start is with an analysis of the security controls you have in your environment today. You can map your controls back logically to MITRE ATT&CK to assess the coverage they provide against the tactics and techniques they will likely face in your environment.

Analytically, you can identify gaps against the threats you expect in your environment, determine the risk these gaps provide, and prioritize decisions to enhance your defenses. This analysis will enable you to have a better discussion with management over budgets and attendant risk.

Understanding MITRE ATT&CK Use Cases

We have highlighted just a few of the many use cases supported by MITRE ATT&CK for your review.

Red Team Performance

Improving red team penetration testing performance is a leading use case for MITRE ATT&CK. Red teams can develop and deploy a consistent and highly organized approach to defining the tactics and techniques of specific threats and then logically assess their environments to see if the defenses work as expected. MITRE ATT&CK can help make all of this consistent, repeatable, and easily communicated.

Understanding MITRE ATT&CK Use Cases (cont.)

AttackIQ's Security Optimization Platform is the leading product from an independent vendor in the breach and attack simulation (BAS) market.

Blue Team Performance

Blue teams can use MITRE ATT&CK better to understand the components of a potential or ongoing cyberattack. They can more quickly understand the techniques being used and, combined with an understanding of the particular attacker, can then identify the most likely next steps in the attack chain. All of this can be used to stop an attack before data can be exfiltrated or other damage can be done to business operations. The blue team can also use MITRE ATT&CK to help prioritize and eliminate defensive gaps.

Threat Intelligence

MITRE ATT&CK can be used to more rapidly and effectively integrate your threat intelligence into your cyberdefense operations. Threats can be mapped to the attackers' specific techniques to understand if gaps exist, determine risk, and develop and deploy a plan to address them. This threat map helps you answer specific questions about these new or predicted threats such as "Are we protected against APT23?"

Security Control Analysis and Selection

You can compare and differentiate vendor products against the tactics and techniques against which you must defend. Vendor products also differ — you can work with vendors to better understand their performance against scenarios you select in the BAS platform.

Breach and Attack Simulation (BAS)

AttackIQ's Security Optimization Platform is the leading product from an independent vendor in the breach and attack simulation (BAS) market. AttackIQ's platform automates and operationalizes the MITRE ATT&CK framework, giving you the capability to continuously test and validate the performance of your security controls against all the tactics and techniques in the MITRE ATT&CK framework.

The AttackIQ platform leverages MITRE ATT&CK to allow any enterprise to automatically simulate the full attack and expanded kill chain against enterprise infrastructure. It delivers continuous validation of your enterprise security program. You can find the performance gaps, strengthen your security posture, and improve your incident response capabilities. Breach and attack simulation assesses readiness and validates that your enterprise security systems are performing as originally intended.

Understanding MITRE ATT&CK Use Cases (cont.)

AttackIQ's Security Optimization Platform brings scale and flexibility for the largest enterprise. Automation technology enables the platform to work autonomously and to scale to support the largest global enterprise.

Today, security practitioners face the challenging task of managing and assessing a sprawling proliferation of cybersecurity controls, testers, attempts at "single panes of glass," and code scanners. According to a 2020 presentation by Jon Oltsik, Senior Principal Analyst and Fellow at ESG, a typical enterprise may utilize between 10 and 75 or more security controls across the organization. The sheer number of cybersecurity vendors and unique security controls can become overwhelming in a large organization burdened by regulatory and compliance demands.

For most of these enterprises, it is unclear how well these security controls work and what areas and gaps require additional investment. The AttackIQ Security Optimization Platform helps you develop a smart strategy, validates that you have a resilient security control architecture, and objectively supports your budgeting decisions.

Since security controls are often not configured correctly or integrated correctly with the security ecosystem, the AttackIQ platform helps identify potentially costly misconfigurations that could be found and targeted by malicious actors.

AttackIQ's Security Optimization Platform brings scale and flexibility for the largest enterprise. Automation technology enables the platform to work autonomously and to scale to support the largest global enterprise. This includes support for live production environments — even the small changes to configurations or administration can open new vulnerabilities in your cyberdefense. This helps identify and close the ever-present gap between test environments and live production environments that, undetected, will ultimately compromise the entire organization.

Gaining the Benefits of Security Optimization

In today's cybersecurity organizations, complexity and conflicting signals make it hard for decision makers to set correct priorities and manage risk across the enterprise. The average senior security practitioner manages dozens of security controls and is responsible for meeting even more standards and regulations. Security practitioners are drowning in alerts and data about their security control effectiveness, and the data they do have is often irrelevant, outdated, and subjective.

There is an underlying problem in the cybersecurity ecosystem that no one can solve on their own. Verizon estimates that existing controls should have stopped 82 percent of successful enterprise breaches, but did not. Why? Because security controls are complex systems formed of technologies, people, and processes, and when they fail, they fail silently. This happens mainly for two reasons — misconfiguration or operational execution error — and the only way to know if they are working is to test them continuously. It takes a lot for a modern information security program to function correctly.

Gaining the Benefits of Security Optimization (cont.)

Security practitioners can rationalize their security controls and continuously optimize their security programs to achieve effectiveness, efficiency, and productivity.

Red team testing is manual and sporadic, and red teams can only test a small percentage of the total attack surface. While valuable for some lessons, third-party penetration testing provides a limited, point-in-time perspective on security control effectiveness. It sometimes doesn't offer any meaningful guidance on how to improve your defenses at all. Consequently, despite over a decade of increasing investment in cybersecurity, most organizations lack real data about their cybersecurity effectiveness.

The situation is further complicated by resource scarcity in a period of acute economic change. Security practitioners need to optimize their cybersecurity programs to improve effectiveness, productivity, and efficiency — and now they need to do so with fewer resources. To address these challenges, the cybersecurity team needs to actively and continuously measure its security program's effectiveness.

What does this mean? Let's look at the challenges the adoption of MITRE ATT&CK and a security optimization platform can resolve. Security control rationalization is assessing your security controls' effectiveness; identifying and addressing gaps and overlaps in your security control stack; conducting a risk assessment of your security vendors; and prioritizing, consolidating, and eliminating unnecessary security controls. Security optimization is a management practice of maximizing the efficiency and effectiveness of your total security program (people, process, and technology) by ensuring that existing security investments are measured, monitored, and modified continuously from a threat-informed perspective.

Security practitioners can rationalize their security controls and continuously optimize their security programs to achieve effectiveness, efficiency, and productivity. A robust breach and attack simulation platform can facilitate the process by grounding organizations in a shared understanding of adversaries and their behaviors using the MITRE ATT&CK framework. Through continuous testing with real-world adversary behaviors, a breach and attack simulation platform can increase defenders' insights about their cybersecurity effectiveness by producing evidence of control technology and visibility platform function. Armed with better ideas and improved insights, security practitioners can continuously make better-informed decisions about people, products, and processes, leading to an overall improvement in security and business outcomes.

Summary

Breach and attack simulation using AttackIQ's Security Optimization Platform is a powerful and highly compelling use case for MITRE ATT&CK.

MITRE ATT&CK brings structure and organization to the understanding of adversarial behavior and provides a detailed knowledge base of actual cyberattack tactics, techniques, and procedures. MITRE ATT&CK provides a common language to categorize attackers and their specific behavior in an easily understood way. This allows security practitioners to analyze attacks better, faster, and more efficiently.

Breach and attack simulation using AttackIQ's Security Optimization Platform is a powerful and highly compelling use case for MITRE ATT&CK. To learn more, take a free class on BAS or on how to operationalize MITRE ATT&CK in AttackIQ Academy or visit www.attackiq.com.

ATTACKIQ

U.S. Headquarters
2901 Tasman Dr. Suite 112
Santa Clara, CA 95054
+1 (888) 588-9116
info@attackiq.com

About AttackIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The Company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with the MITRE Center of Threat Informed Defense.

For more information visit www.attackiq.com. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.