A CISO'S Guide to MITRE ATT&CK™

ATTACKIQ®

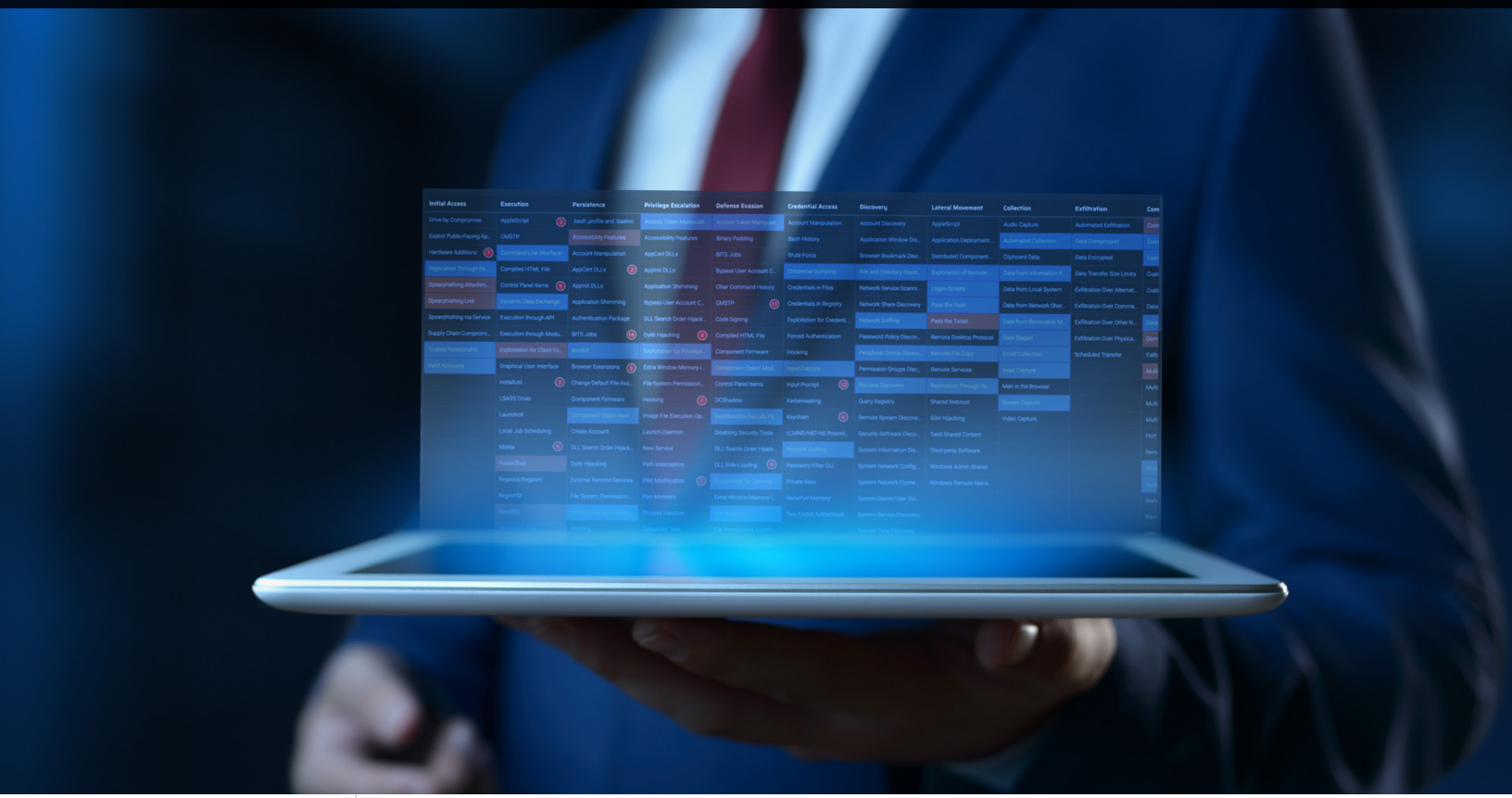
Contents

Notice 3
What is MITRE ATT&CK™? 4
Why is the MITRE ATT&CK Framework Important? 5
MITRE ATT&CK Provides a Common Language 5
How is MITRE ATT&CK Structured? 5
What are ATT&CK Groups and How Can They Help? 5
How Do You Get Started with MITRE ATT&CK? 6
Understanding MITRE ATT&CK Use Cases 6
- Red Team Performance 7
- Blue Team Performance 7
- Threat Intelligence 7
- Security Control Analysis and Selection 7
- Breach and Attack Simulation (BAS) 7

Summary 8

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.



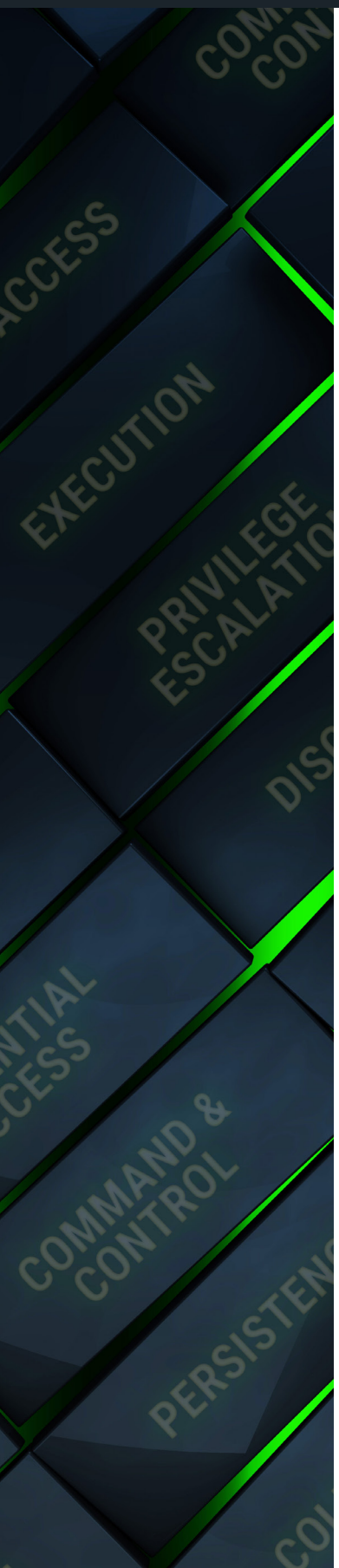
MITRE ATT&CK™

What is MITRE ATT&CK™?

The MITRE Corporation was founded in 1958 as a nonprofit organization. It 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 in the world. MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world data. 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. MITRE's stature in the cyber 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.

The MITRE ATT&CK framework is not the only cybersecurity framework that can help you defend your enterprise. It is complemented by other important frameworks such as COBIT (Isaca.org), Lockheed Martin's Cyber Kill Chain®, ISO/IEC 27001, and the NIST cybersecurity framework. All of these can be an important part of your cyberdefense strategy.



Why is the MITRE ATT&CK Framework Important?

MITRE ATT&CK is, in both depth and breadth, the largest attack knowledge base, providing suggested mitigation techniques, detection procedures, and other important technical information. MITRE has expanded the Kill Chain to include the widest variety of tactics, which are then supported by detailed techniques. This organized approach enables you to methodically select and analyze attacks and also compare them to the capabilities of your security controls in order to understand the gaps. Once understood, you can then rationally expand your security controls and adjust your budgets.

MITRE ATT&CK is perhaps the largest, most 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 management can 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. This provides, for the first time, a common lexicon that enables stakeholders, cyber defenders, and vendors to clearly 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 can be used to describe the procedures of an attacker or attack tools and exactly the techniques which they deploy. The precise lexicon of MITRE ATT&CK enables more precise assessment of threats and a faster, better-targeted response.

How is MITRE ATT&CK Structured?

MITRE ATT&CK enterprise matrix provides a tabular view to 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. Listed below each of the 12 tactics is a column that shows between nine to 67 techniques that might be used to implement a particular tactic. It is often that case that several techniques are used in one or more tactics.

A tactic clearly defines the goals of the attacker. A technique provides a description of the different ways that a cyber attacker can achieve the end goals of the tactic.

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 are 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 - it is as available based upon the sources that MITRE monitors on an ongoing basis.

Here is an example of an ATT&CK group Carbanak that mainly targets banks and the various aliases by which it is known. Carbanak is also sometimes referred to as FIN7, but these appear to be two groups using the same Carbanak malware and so they are tracked separately.

Associated Group Descriptions for Carbanak
Anunak
Carbon Spider

How Do You Get Started with MITRE ATT&CK?

AttackIQ presents the 1,000-foot view that you need to work effectively. You can now logically organize your defenses against the threats you expect. The best place to start is with an analysis of the security controls you have in your environment today. You can map them 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 make prioritized decisions to enhance your defenses. This will enable you to have a better discussion with management over budgets and attendant risk.

Understanding MITRE ATT&CK Use Cases

These are just a few of the many use cases supported by MITRE ATT&CK. We have highlighted a few for 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 environment to see if the defenses work as expected. MITRE ATT&CK can help make all of this consistent, repeatable, and easily communicated.

Blue Team Performance

Blue teams can use MITRE ATT&CK to better understand the components of a potential or ongoing cyber attack. 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 sooner, 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 specific techniques of the attackers to understand if gaps exist, determine risk, and develop and deploy a plan to address them. This helps you answer specific questions about these new or predicted threats such as: "Do we think we are protected against APT23?"

Security Control Analysis and Selection

You can compare and differentiate vendor products against the tactics and techniques you feel you must defend against. 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 Breach and Attack Simulation (BAS) platform supports the automation and operationalization of the MITRE ATT&CK framework. This gives you a powerful capability to continuously test and validate the performance of your security controls against the tactics and techniques in the MITRE ATT&CK framework.

AttackIQ BAS technology leverages MITRE ATT&CK to allow any enterprise to automatically simulate the full attack and expanded kill chain against enterprise infrastructure using software agents, virtual machines, and other means. AttackIQ BAS 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.

The average large enterprise has deployed over 75 security control tools, often with significant overlap and redundancy. For most of these enterprises, it is unclear how well these security controls really

work and what areas and gaps require additional investment. AttackIQ BAS helps you develop a smart strategy, validates that you have a resilient security control architecture, and objectively supports your budgeting decisions.

Often existing security controls are not configured correctly or integrated properly with the security ecosystem. BAS platforms can identify potentially costly misconfigurations that will be found and targeted by malicious actors. In any scenario, your cyberdefense will not work if the security controls do not perform as you expect.

AttackIQ BAS brings scale and flexibility for the largest enterprise. AttackIQ automation 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.

Summary

MITRE ATT&CK brings structure and organization to the understanding of adversarial behavior and provides a detailed knowledge base of actual cyber attack 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 cyber defenders to better prepare against likely attacks, analyze attacks more quickly, and work more efficiently.

Breach and Attack Simulation is a powerful and compelling use case for MITRE ATT&CK. To find out more about how to operationalize MITRE ATT&CK using AttackIQ Breach and Attack Simulation, please reach out to **info@attackiq.com** or visit us at **www.attackiq.com**.

ATTACKIQ
U.S. Headquarters
9276 Scranton Road, Suite 100
San Diego, CA 92121
+1 (888) 588-9116
info@attackiq.com

AttackIQ, a leader in the emerging market of breach and attack simulation, built the industry's first platform that enables red and blue teams to test and measure the effectiveness of their security controls and staff. An open platform, AttackIQ® supports the MITRE ATT&CK Matrix, a curated knowledge base and model for cyber adversary behavior used for planning security improvements and verifying that defenses work as expected. AttackIQ's platform is trusted by leading companies around the world. For more information visit **www.attackiq.com**. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.