ATTACKIQ®

White Paper

The CISO's Guide to Better Vulnerability Management Using MITRE ATT&CK®

How combining known threat behaviors with vulnerability management can help CISOs better manage enterprise cybersecurity risk.

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

Executive Summary

Threat-informed Defense Becomes a Reality

As the digitalization of private and public sector organizations continues at pace, the volume of security vulnerabilities increases. According to a new list of critical vulnerabilities published by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), there are at least 290 key vulnerabilities in the world today that present significant cybersecurity risks to organizations, leaving them vulnerable to adversary exploitation and attack. The challenge is that no security team can quickly close all those vulnerabilities without major increases in resourcing. And the new CISA list is a pared down list of crucial vulnerabilities; large enterprises may have thousands and thousands of vulnerabilities within their information technology (IT) enterprises.

Chief information security officers (CISOs) therefore need to prioritize which vulnerabilities they fix first. Until now, that prioritization has been difficult to achieve. With no link between vulnerability management and threat management, security teams have lacked a clear, comprehensive means of understanding how adversaries might exploit existing vulnerabilities to achieve their strategic objectives.

This information gap has now been bridged with the publication of a new mapping methodology by MITRE Engenuity's Center for Threat-Informed Defense: Mapping ATT&CK to CVE for Impact. The methodology uses the MITRE ATT&CK framework, which catalogs common adversary tactics and techniques, to characterize the impact of each of the vulnerabilities described in the MITRE Corporation's list of Common Vulnerabilities and Exposures (CVE).

Aligning CVE to ATT&CK provides a clear, standardized way to describe the methods adversaries use to exploit a vulnerability, and what adversaries may achieve by doing so. By using an ATT&CK technique to examine a vulnerability, defenders adopt a threat-informed defense and place the adversary at the center of their defensive planning. A threat-informed defense strategy helps organizations prioritize which vulnerabilities to close and which attack tactics and techniques to prepare to defend themselves against. Practically, the methodology delivers a focused list of which adversary tactics and techniques to include in your testing strategy and through an automated breach and attack simulation (BAS) platform.

By adopting this new methodology, CISOs and security teams can save time and resources when it comes to vulnerability management and gain a better understanding of their organization's overall cybersecurity posture. With the clear picture that the ATT&CK-CVE alignment provides, organizations can move forward to validate their security controls and optimize their investments.

Vulnerability Patching: CISOs' Sisyphean Task

In the Greek myth, when Sisyphus dared to challenge the Gods, he was set an impossible task as punishment: to roll a boulder up a vast hill. The trouble was that every time Sisyphus neared the summit, the bolder simply rolled back down. For many CISOs this vision of a never-ending hell may seem somewhat familiar. Vulnerability patching is to CISOs what the bolder is to Sisyphus. Every time an exploitable flaw in a software, firmware, hardware, or service component is identified and remedied, another one springs up.

For CISOs engaged in this endless game of whack-a-mole, the job is getting more difficult by the day due to the ongoing digital transformation of business, which was greatly accelerated by the COVID-19 pandemic. Some research indicates that during the pandemic companies have accelerated the digitization of their customer and supply-chain interactions and their internal operations by three to four years.[1] But as digital systems and the infrastructure that provides them proliferate, so too do vulnerabilities.

A Mountain to Climb

The scale of the challenge was recently thrown into the starkest possible light by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). In its landmark Binding Operational Directive (BOD) 22-01, "Reducing the Significant Risk of Known Exploited Vulnerabilities," CISA published a catalog of 290 common security flaws that threaten federal agencies. CISA mandates that federal agencies fix these vulnerabilities, and strongly recommended that private sector enterprises follow suit.[2]

The size of this task should not be underestimated. On average it takes between 60 and 150 days[3] to patch a vulnerability, so working through the full CISA list would take around 17,400 to 43,500 personnel days. No organization has the resources required to fix every vulnerability across every application in a short period of time, particularly when skilled cybersecurity professionals are in thin supply.[4]

We should also not forget the inherently Sisyphean nature of this task. Even if a motivated and well-resourced CISO could tick off the entire CISA list, by the time they finished, there would be a new round of vulnerabilities to patch. The enterprise IT landscape will have changed in the interim, growing and introducing new flaws and vulnerabilities.

[1] McKinsey & Company, How COVID-19 has pushed companies over the technology tipping point and transformed business forever, October 5, 2020
[2] Manikanta Immanni, CISA Listed 290 Vulnerabilities Affecting Federal Civil Agencies, November 3, 2021
[3] Susan Morrow, Time to patch: Vulnerabilities exploited in under five minutes?, Infosec, August 2, 2021
[4] Hope Reese, The cybersecurity skills gap persists for the fifth year running, Techrepublic, August 16, 2021

A Matter of Priorities

In the real world of constrained resources, CISOs and their teams must prioritize. All security vulnerabilities are important, but they are not equally important. In an imperfect world, the best tack for CISOs to take is to focus on defending the business's high-value assets against known threats that are most likely to cause the greatest damage.

This idea has been gaining currency in the area of cybersecurity for a number of years. On a national strategic level, it was first given momentum by Section 9 of the 2013 U.S. government Executive Order "Improving Critical Infrastructure Cybersecurity," signed by President Barack Obama. Section 9 orders a "risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."[5] For the first time, the Section 9 list drove a risk-based approach to national critical infrastructure cybersecurity.

Just as some national infrastructures are more important than others, so too are some enterprise assets more worthy of protection than others. These are the assets that are of high value to both the infrastructure owner and to the attackers, or those assets that would incur heavy regulatory fines in the event of a breach.

The industry in question is also an important consideration; attack volumes and methods vary according to the nature of a company's business and operations. According to the U.S. Department of Health and Human Service, breaches in the health sector increased by over 150 percent in 2020. This was thanks in part to the rise in workers accessing company infrastructure through client portals, resulting in a spike in application-specific and web application attacks.[6]

> *"In our experience, a strong cybersecurity strategy provides differentiated protection of the company's most important assets, utilizing a tiered collection of security measures."*[9]
>
> ***— McKinsey & Company***

There is also a clear cost incentive for CISOs. Around 50 percent of a company's systems are not critical from a cybersecurity perspective.[7] By refocusing investment on crucial assets, enterprises can save up to 20 percent of their total cybersecurity costs.[8]

[5] The White House, Executive Order -- Improving Critical Infrastructure Cybersecurity, February 12, 2013
[6] Rene Millman, Cyber attacks on manufacturing up 300% in a year, May 11, 2021
[7-9] McKinsey & Company, Perspectives on transforming cybersecurity, March 2019

Defending Against Real-world Threats

The question is, therefore, this: how can CISOs expand the prioritization-based approach to the area of vulnerability management given (a) the number of vulnerabilities there are and (b) the range of ways that attackers can exploit each of these vulnerabilities.

Historically, CISOs have been unable to answer this question easily. In part, this is due to the limitations of a framework-based approach to security. CISOs work through security and privacy frameworks such as NIST Special Publication 800-53 to ensure that their enterprise systems comply with recommended controls and settings. The hope is that if a vulnerability is exploited by a bad actor, the best practices provided by the framework will provide sufficient defense.

The issue with this approach is that it means the enterprise is secured according to an abstract understanding of what attackers might do, rather than what they actually are doing. There is no way for CISOs to know that they are protecting their organizations against the real threats that they face.

What's required is a way to span the gap between the vulnerabilities that organizations know they have and the way these vulnerabilities are being exploited in the real world. Doing so requires integrating threat management and vulnerability management into a unified framework to achieve a complete view of the organization's risk landscape. By uniting vulnerability and threat management, threats can be emulated, security controls tested, and vulnerabilities closed on the basis of known threat behaviors.

The lack of integration between threat and vulnerability management has been a blind spot for CISOs until now. A new methodology published by MITRE Engenuity's Center for Threat-Informed Defense closes this gap and for the first time provides the means for CISOs to prioritize vulnerability management effectively.

Prioritizing Vulnerability Management Using ATT&CK and CVE

The Center for Threat-Informed Defense's methodology, which was produced in partnership with AttackIQ and JP Morgan Chase, draws on two crucial sources: the adversary behaviors described in the MITRE ATT&CK catalog and the vulnerabilities recorded in the CVE list (Common Vulnerabilities and Exposures). As a reminder:

- **CVE** is "an international, community-based effort that maintains a community-driven, open data registry pf publicly known cybersecurity vulnerabilities."[10] CVE is operated by the MITRE Corporation, a not-for-profit organization which is funded by the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency Vulnerability Management Component.
- **MITRE ATT&CK** is "a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. 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."[11]

> *"When used in a vulnerability report, ATT&CK's tactics and techniques enable defenders to quickly understand how a vulnerability can impact them, helping defenders integrate vulnerability information into their risk models and identify appropriate compensating security controls."*[12]
>
> ***— MITRE Corporation***

The new methodology, Mapping ATT&CK to CVE for Impact, enables CISOs and their teams to use the adversary behaviors described in ATT&CK to characterize the impact of CVEs. This is a significant step forward for CISOs as it allows them to understand the context around vulnerabilities, such as the ways in which attackers exploit vulnerabilities.

For the first time, it is possible for CISOs to bridge vulnerability management, threat modelling, compensating controls, and security optimization to understand the true risks posed by specific vulnerabilities in their systems.

[10] CVE.org, About the CVE program
[11] Mitre.org, MITRE ATT&CK
[12] Jonathan Evans et al, CVE + MITRE ATT&CK to Understand Vulnerability Impact, MITRE-Engenuity, October 27, 2021

The Methodology in Action

What does the Mapping ATT&CK to CVE for Impact methodology look like in practice? The Center for Threat-Informed Defense mapped multiple vulnerabilities in the CVE to the ATT&CK framework, here's just one by way of example.

In the scenario illustrated in Figure 1, an attacker is looking to exploit the known vulnerability of "unsecure credentials" (this is listed in CVE as CVE-2018-17900). Mapping to the ATT&CK framework, we can see that the vulnerability enables the attacker to use the tactic of "exploiting a public facing website (Tactic 1190 in the MITRE ATT&CK framework). As a result, the attacker can exploit the "unsecured credentials" tactic (T1552) and from there move on to "access valid accounts" (T1078).

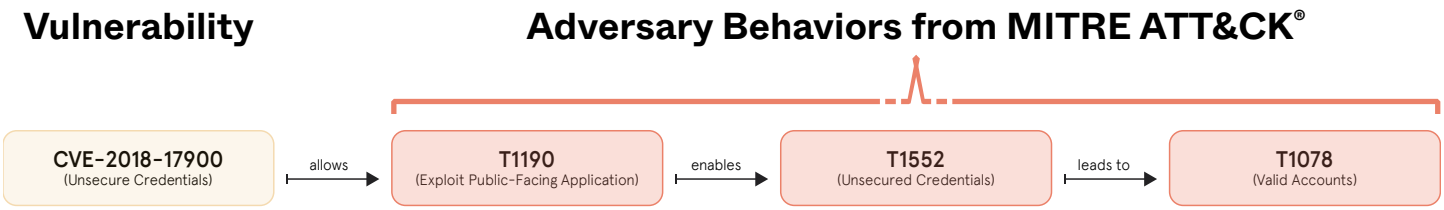

Figure 1: Use case for the Mapping ATT&CK to CVE for Impact methodology

As is clear from this example, the Center's research provides CISOs with a logical alignment and strategic understanding of an adversary that could prove decisive in protecting their enterprise. If CISOs know which threat groups, tactics, and techniques are of greatest concern, they can prioritize vulnerability management and security optimization.

Threat-informed Defense Delivered

Threat-informed defense has been a long sought-after prize for CISOs. With the arrival of the Center's new methodology the concept has finally been made reality. There are many benefits to CISOs from mapping MITRE ATT&CK to CVE; here are some of the most important:

- **Streamline risk management.** By aligning vulnerability and threat management, CISOs can greatly reduce the risks associated with cyberattacks, leveraging vulnerability reports that go beyond technical details to outline the higher-level goals and methods of malicious actors. This broader understanding of vulnerability, vector, and intent, enables security teams to rapidly assess their cybersecurity risks and align their security control frameworks (i.e., NIST 800-53) to the threat behaviors in ATT&CK. From there, the CISO's team can focus on building a robust mitigation plan.

- **Improve your testing strategy.** The methodology helps organizations prioritize their security testing according to the attack techniques that are the greatest risk for their businesses. Organizations can use the CVE-ATT&CK alignment to prioritize the security controls that they test first.

- **Increase sector-specific protection capabilities.** In contrast to the rigid, one-size-fits all approach that comes with protecting enterprises by complying with security frameworks, mapping ATT&CK to CVE provides tailored risk analysis on the basis specific industries. As a result, it reflects the sectoral differences between companies, and enables CISOs to identify the vulnerabilities and attack techniques most relevant to their specific industry.

- **Save personnel time.** Just as the introduction of CVE and ATT&CK saved CISOs the time associated with carrying out their own vulnerability and threat research, the combined mapping of both frameworks helps save time by enabling CISOs to quickly understand how a vulnerability can impact their organization. Given how stretched security resources are in many organizations, this is a significant value-add.

Putting the Methodology Into Practice

The Center for Threat-Informed Defense has laid the foundations for a new way of managing cybersecurity risk, one that starts from real-world attack behaviors and works backward to prioritize vulnerability mitigations. For CISOs looking to leverage the methodology, here are two initial recommendations to get you started:

1. **Incorporate ATT&CK into vulnerability records.** This is a simple task that should take around five minutes per vulnerability record. The process involves three steps:

    a. *Start with the attacker's tactics.* ATT&CK lists a set of techniques than an attacker may use to achieve their tactical goal. Because there are fewer tactics than techniques, and they may apply to a broader range of vulnerabilities, it makes sense to start there. Use the list of tactics outlined in the methodology to describe your vulnerability information to ensure consistency and standardization.

    b. *Build out incrementally.* If you are unable to get the level of information you need from the ATT&CK tactics, bring in information from the vulnerability type mappings. Start with the tactic that gives you most cause for concern and integrate the associated techniques one-by-one.

    c. *Create chains of techniques.* Start to map how an adversary chains several techniques together. In this step, you can use the AttackIQ Anatomic Engine to automate a chain of attacks. Usually an attacker will tie about three techniques in combination to achieve their tactical goal, but more can be included. On the basis of known threats, by building chains of possible techniques that an adversary might use, you give security teams better context for detecting and mitigating a specific vulnerability.[13]

2. **Prioritize key defense capabilities to test.** Automated testing is a core component of achieving cybersecurity readiness today, and this new mapping can enhance your testing strategy. The methodology gives a natural prioritized list of real-world attacks that you should emulate first, and that are of lower priority. With its deep library of scenarios and assessments, you can use the AttackIQ Security Optimization Platform to operationalize the tactics, techniques, and procedures of the MITRE ATT&CK framework, making the most of this methodology. Operating under a purple team construct, your red and blue teams can use the MITRE ATT&CK framework and a breach and attack simulation platform to tighten up your security program. That's what it means to practice a threat-informed defense.

[13] See GitHub, Center For Threat-Informed Defense, attack_to_cve, Getting Started for more information

Conclusion

Shifting the Dial on Risk Management

For years, the adversary had the advantage when it came to targeting vulnerabilities. MITRE ATT&CK helps solve this problem by showing you which vulnerabilities matter most to the adversary — and therefore matter most to you. This new research furthers the practice of threat-informed defense, enabling CISOs to prioritize their defense initiatives on the basis of known vulnerabilities and attack techniques. For more on how to put MITRE ATT&CK and a threat-informed defense into practice, enroll in AttackIQ's expert led courses through AttackIQ Academy at academy.attackiq.com.

ATTACKIQ
U.S. Headquarters
171 Main Street Suite 656
Los Altos, CA 94022
+1 (888) 588-9116
info@attackiq.com