MITRE ENGENUITY | Center for Threat Informed Defense | CYCOGNITO

Adoption Spotlight

CyCognito Adopts Mapping ATT&CK to CVE for Impact

SILVER
Center for Threat-Informed Defense
AFFILIATE
MITRE ENGENUITY

R&D Project Introduction

The Center for Threat-Informed Defense (Center and its participants developed an approach to using MITRE ATT&CK® to help defenders understand the impact of a vulnerability. Defenders lacked a consistent view of how adversaries use vulnerabilities and there was no standard approach to integrating vulnerability and threat information. The Center developed a methodology that uses ATT&CK to characterize the impact of CVEs. CVEs linked to ATT&CK techniques form a crucial contextual bridge between vulnerability management, threat modeling, and compensating controls, empowering defenders to better assess the true risk posed by vulnerabilities in their environment.

About CyCognito

CyCognito solves one of the most fundamental business problems in cybersecurity: seeing how attackers are most likely to break into your organization and how you can eliminate exposure. The company does this with a transformative platform that automates offensive cybersecurity operations to provide reconnaissance capabilities superior to those of attackers.

Why CyCognito Adopted Mapping ATT&CK to CVE for Impact

CyCognito chose this project to help customers understand related risks associated with detected vulnerabilities. This mapping of CVEs to the ATT&CK framework and techniques helps defenders better understand the impact and risk posed by specific vulnerabilities in their environments forming a contextual bridge to determine proper remediation and mitigation strategies.

How CyCognito Uses Mapping ATT&CK to CVE for Impact

CyCognito incorporated the Mapping ATT&CK to CVE for Impact project directly into our platform. For every CVE found, a corresponding mapping to the related ATT&CK techniques is displayed immediately alongside.

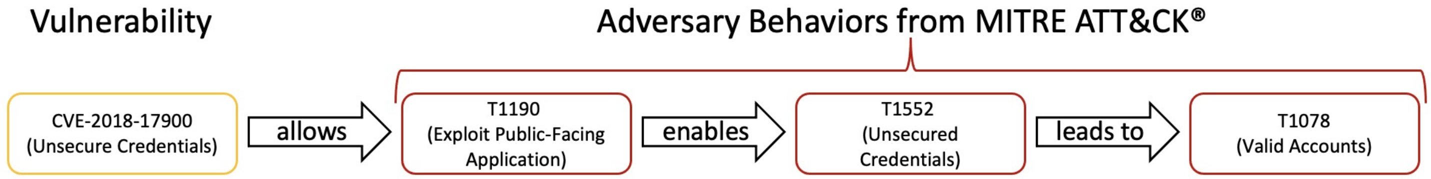
Our customers will find a dedicated MITRE ATT&CK section with robust context including underground activity on adversary usage and tactics. In many cases, CyCognito will also provide code samples that can be used to verify or actually exploit the vulnerability. Further, CyCognito provides specific, detailed instructions on how to remediate or mitigate the vulnerabilities creating a closed-loop process of discover, validate, and defend.

By providing this comprehensive, closed-loop view of the related risks and protection strategies, CyCognito is helping our customers significantly and measurably reduce cyber risks related to internet-facing assets.

> “CyCognito is committed to helping businesses prevent breaches by providing them with unparalleled attack surface visibility, data exposure, and risk detection across previously unknown and unmanaged assets, and our partnership with the MITRE Engenuity Center for Threat-Informed Defense expands these capabilities, providing our customers and partners with specific MITRE ATT&CK details to help customize their cyber defenses and improve their ability to successfully identify and address cyber risk within their organizations.”
>
> - Rob Gurzeev, CEO and Co-Founder
> CyCognito

About the R&D Research Mapping ATT&CK to CVE for Impact

The Center published a methodology that uses the adversary behaviors defined in ATT&CK to describe the potential impact of a CVE entry. Defenders can use ATT&CK's tactics and techniques to quickly understand how a vulnerability can impact them, enabling defenders to integrate vulnerability information into their risk models and identify appropriate compensating security controls.


Vulnerability
Adversary Behaviors from MITRE ATT&CK®
CVE-2018-17900 (Unsecure Credentials)
allows
T1190 (Exploit Public-Facing Application)
enables
T1552 (Unsecured Credentials)
leads to
T1078 (Valid Accounts)

This project establishes a critical connection between vulnerability management, threat modeling, and compensating controls. Enabling vendors, researchers, vulnerability databases, and other producers of vulnerability information to standardize the way they describe the impacts of vulnerabilities. When used with security control frameworks that are mapped to ATT&CK, CVE's with ATT&CK technique references should enable defenders to better understand their compensating controls for a given CVE. Project resources available on GitHub include:

- **Methodology Mapping:** The methodology for mapping ATT&CK techniques to vulnerability records to describe the impact of a vulnerability.
- **Getting Started Guide:** After you review the methodology, this guide suggests an approach to starting small and increasing your use of ATT&CK as you get comfortable with the methodology.
- **CVE Mappings:** Set of CVEs with ATT&CK mappings created in the process of developing the methodology.
- **CVE JSON Schema Extension:** An extension to the CVE JSON schema that introduces a taxonomy mapping object that can be used to include ATT&CK for describing impact.

The Methodology

The methodology uses ATT&CK to characterize the impact of a vulnerability as described in the CVE list. ATT&CK techniques provide a standard way of describing the methods adversaries use to exploit a vulnerability and what adversaries may achieve by exploiting the vulnerability. Using ATT&CK techniques to describe a vulnerability makes it easier for defenders to integrate vulnerabilities into their threat modeling.

The methodology categorizes three steps in a potential attack:

- **Exploitation Technique:** The method used to exploit the vulnerability.
- **Primary Impact:** The initial benefit gained through exploitation of a vulnerability. **Secondary**
- **Impact:** What the adversary can do by gaining the benefit of the primary impact.

The project defined three methods to map ATT&CK techniques to vulnerabilities:

- **Vulnerability Type:** This method group's vulnerabilities with common vulnerability types (e.g., cross-site scripting and SQL injection) that have common technique mappings.
- **Functionality:** This method group's common mappings based on the type of functionality the attacker gains access to by exploiting the vulnerability.
- **Exploit Technique:** This method groups common mappings depending on the method used to exploit the vulnerability.

Supporting Tools & Resources

The project helps vulnerability report authors by providing a clear, consistent approach to describing the impacts and exploitation methods of a vulnerability. The methodology allows vulnerability reporters to use ATT&CK to create richer, more consistent vulnerability reports that help defenders rapidly assess the risk of a vulnerability and leverage the full range of resources linked to ATT&CK. Now we need the community's help to apply the methodology at scale.

With an established foundation in place for the community to build upon, broad community engagement is our next focus. We need ongoing engagement with the CVE CNA community, threat intel teams, and end users to make the case for adoption and to collect feedback.

Defenders can help by reviewing the methodology and the set of CVEs that we mapped and let us know what you think. Be an advocate and ask your vendors to include ATT&CK references in their vulnerability reports.

Vulnerability reporters are critical to realizing our goal of connecting threat and vulnerability management. You can help by reviewing the methodology and applying it in your vulnerability reports. Help build the corpus of vulnerability reports with ATT&CK references.

MITRE ENGENUITY. Center for Threat Informed Defense

For more information:
ctid@mitre-engenuity.org
ctid.mitre-engenuity.org

About the Center for Threat-Informed Defense

The Center is a non-profit, privately funded research and development organization operated by MITRE Engenuity. The Center's mission is to advance the state of the art and the state of the practice in threat-informed defense globally. Comprised of participant organizations from around the globe with highly sophisticated security teams, the Center builds on MITRE ATT&CK®, an important foundation for threat-informed defense used by security teams and vendors in their enterprise security operations. Because the Center operates for the public good, outputs of its research and development are available publicly and for the benefit of all.

CYCOGNITO

For more information:
info@cycognito.com
www.cycognito.com