MITRE ENGENUITY™ | Center for Threat Informed Defense

2021 IMPACT REPORT

RESEARCH PARTNERS

ATTACKIQ	FOUNDER
BANK OF AMERICA	FOUNDER
citi	FOUNDER
HCA Healthcare	FOUNDER
IBM Security	
JPMORGAN CHASE & CO.	FOUNDER
verizon	

RESEARCH SPONSORS

ANOMALI	
BAE SYSTEMS	
Booz | Allen | Hamilton	FOUNDER
CROWDSTRIKE	
cybereason	
EY Building a better working world	
FORTINET	
FUJITSU	FOUNDER
Google Cloud	
Humana	
Microsoft	FOUNDER
red canary	FOUNDER
SIEMENS	FOUNDER
splunk> turn data into doing.	
usbank	FOUNDER

NON-PROFIT PARTICIPANTS

Analysis & Resilience Center FOR SYSTEMIC RISK	
CIS Center for Internet Security	
CYBER THREAT ALLIANCE	FOUNDER
FIRST Improving Security Together	
FS-ISAC	
GLOBAL CYBER ALLIANCE	
NRF NATIONAL RETAIL FEDERATION	
RETAIL & HOSPITALITY ISAC	

A diverse array of participant organizations, representing some of the most sophisticated security teams from around the world, power the Center for Threat-Informed Defense with their insight, expertise, and support. Critical to all aspects of the Center's R&D program, participants are committed to ensuring that the work done by the Center to "advance the state of the art and state of the practice in threat-informed defense" is made freely available to the public.

PERSPECTIVES FROM OUR MEMBERS

"The Center for Threat-Informed Defense elevates the world's cybersecurity readiness through cutting-edge operational research."

- Carl Wright, Chief Commercial Officer
AttackIQ

"It's hard to overstate the importance of collaboration underway in the Center for Threat-Informed Defense. Participating in the Center's research and development program is one of the many key ways Bank of America demonstrates leadership in cyber security for the benefit of the larger financial sector and the communities we all serve."

- Alex Hutton, Security Executive
Bank of America

"Innovation is a core value to Fortinet and the Center provides a focal point for the community to efficiently collaborate and innovate - so we can continue to be trailblazers. We're proud to be a part of a community that ultimately makes the entire community more secure."

- Derek Manky, Chief of Security Insights and Global Threat Alliances, FortiGuard Labs
Fortinet

"The most important aspect of participating in Center projects is the interaction with the other Center Participants and the MITRE team. We learn a lot throughout the collaborative process gaining valuable insights that help our teams and our customers."

- Ryusuke Masuoka, Research Principal
Fujitsu System Integration Laboratories

"The available research options are all compelling and offer significant value both to our company objectives and the industry as a whole. We have been pleasantly surprised by the careful thought that has been required to choose which efforts to support with our research funds."

- Caleb Chitwood, Manager of Threat Intelligence Services
HCA Healthcare

"Microsoft is a proud Sponsor of the Center and we appreciate the work the Center has done for the betterment of open-source security. The partnership with MITRE is essential to provide better security knowledge and tools to the community and empower organizations to be able to build better defenses and keep pace with the evolving threat landscape. We have had the opportunity to participate in several programs with the Center over the past two years and we are looking forward to many more."

- Tanmay Ganacharya, Partner Director, Microsoft Defender Security Research
Microsoft

"Red Canary is proud to be a Founding Sponsor of the Center for Threat-Informed Defense, where the world's leading security teams are working to make the data, information, and intelligence at our disposal accessible and actionable by the industry at-large. The work that we do furthers our understanding of threats and adversaries, and results in better understood and more effective security solutions, and ultimately better security outcomes for organizations worldwide."

- Keith McCammon, Co-founder and Chief Security Officer
Red Canary

"It is a privilege for our Siemens Cyber Defense teams to collaborate with MITRE Engenuity and industry leading cyber security experts on threat-informed defense initiatives. We are excited to contribute and engage with an ever growing community to continuously improve the state of the art in cyber defense."

- Hans Wallinger, Head Cyberdefense Innovation & Platform
Siemens AG

"The only way for defenders to beat adversaries is by sharing knowledge. The Center allows us to collaborate on research topics with the brightest minds in the industry through a neutral shared party for the betterment of the world."

- Ryan Kovar, Distinguished Security Strategist and Leader of SURGe
Splunk

"Verizon's vision aligns with the Center's mission – we believe that we need to help the community with resources and tooling that makes defenders lives easier."

- Alex Pinto, Senior Manager DBIR Team
Verizon

TABLE OF CONTENTS

7 A letter from the Director

9 FIN6 Adversary Emulation Plan

11 menuPass Adversary Emulation Plan

13 CALDERA Pathfinder

15 ATT&CK for Cloud

17 NIST 800-53 Control Mappings

19 ATT&CK for Containers

21 ATT&CK Workbench

23 Security Stack Mappings Azure

25 Atomic Data Sources

27 ATT&CK Integration into VERIS

29 Security Stack Mappings AWS

31 Threat Report ATT&CK Mapper - TRAM

33 Mapping ATT&CK to CVE for Impact

Since the Center for Threat-Informed Defense launched in November of 2019, we have been hard at work leading the charge to change the game on the adversary and ultimately give the advantage to the defender. Founded with the support of 13 participant organizations, our membership has grown to 30 (as of the publication of this report). Each participant has fully committed to the Center's mission and the value of collaborative research and development in the public interest.

This inaugural impact report serves as a testament not only to the work, but to the critical relationships the Center for Threat-Informed Defense has forged. Powered by the experience, insights and resources of Center participants, we leverage the deep technical expertise of MITRE to advance the state of the art and the state of the practice in threat-informed defense. This impact report is proof positive that this collaboration has already begun to return dividends.

Inside this impact report you'll find summaries of our first thirteen published projects spanning topics including adversary emulation, advancing our understanding of threats to cloud technologies, and linking security controls to the actual threats that they help defend against. True to our public interest mission, all of these projects are freely available to the global community, and we encourage you to explore, use, and help improve these resources. As impressive as this initial set of published releases are, this is just the beginning.

Building on this initial set of projects, we are hard at work on a broad range of exciting new projects. Over the next year we will continue to expand our portfolio of cloud-related projects, as well as explore some new areas including threat modeling in Operational Technology (OT) environments, applying the lessons of MITRE ATT&CK® to malware, and building more foundational resources to help defenders focus on finding and stopping adversaries. The common thread throughout all of this is that is it driven and shaped and made possible by our participants.

In a landscape dominated by reports of the latest security breaches, the work of the Center and the spirit of collaboration with our participants gives me hope for the future. I hope you'll enjoy some of the same optimism as you read through the accomplishments we have achieved together.

Thank you for your continued support.

JONATHAN O. BAKER

Director of Research & Development

December 2021

FIN6 ADVERSARY EMULATION PLAN

Published: 15 September 2020

Summary

The FIN6 Adversary Emulation Plan is the first entry in the Center's growing Adversary Emulation Library. The library is a free resource that gives defenders access to adversary tactics, giving them more tools to assess their defenses.

FIN6 is a cyber-crime group that has stolen payment card data and sold it for profit on underground marketplaces. This group has aggressively targeted and compromised point of sale (PoS) systems in the hospitality and retail sectors. This project developed an adversary emulation plan for FIN6 and added it to the Adversary Emulation Library.

Funding Research Participants

ATTACKIQ Citi

FUJITSU Microsoft

Problem

Understanding defenses from the perspective of the adversary is critical, but often teams lack the resources (expertise and funding) to conduct the adversary emulation exercises.

Solution

Establish a library of standardized intellingence driven adversary emulation plans that can be easily leveraged by cyber defenders.

Impact

Enables cyber defenders to see their defenses from the perspective of the adversary.

> *"Over the course of the last two years, Center experts have applied the MITRE ATT&CK framework to build innovative adversary emulation capabilities, improve cloud security effectiveness, and align threat and risk management frameworks to optimize compliance. And the work is just getting started."*
>
> **- Carl Wright, Chief Commercial Officer**
> **AttackIQ**

MENUPASS ADVERSARY EMULATION PLAN

Published: 04 February 2021

Summary

The menuPass Adversary Emulation Plan is the second entry in the Center's Adversary Emulation Library. The library is a free resource that gives defenders access to adversary tactics, giving them more tools to assess their defenses. The Center recently added FIN6 and menuPass to the library.

menuPass is a threat group that has been active since at least 2006. Individual members of menuPass are known to have acted in association with the Chinese Ministry of State Security's (MSS) Tianjin State Security Bureau and worked for the Huaying Haitai Science and Technology Development Company. menuPass has targeted healthcare, defense, aerospace, finance, maritime, biotechnology, energy, and government sectors globally, with an emphasis on Japanese organizations. In 2016 and 2017, the group is known to have targeted managed IT service providers (MSPs), manufacturing and mining companies, and a university. This project developed an adversary emulation plan for menuPass and added it to the Adversary Emulation Library.

Funding Research Participants

FUJITSU SIEMENS

Problem ⚠

Understanding defenses from the perspective of the adversary is critical, but often teams lack the resources (expertise and funding) to conduct adversary emulation exercises.

Solution 💡

Establish a library of standardized intelligence driven adversary emulation plans that can be easily leveraged by cyber defenders.

Impact ⇛

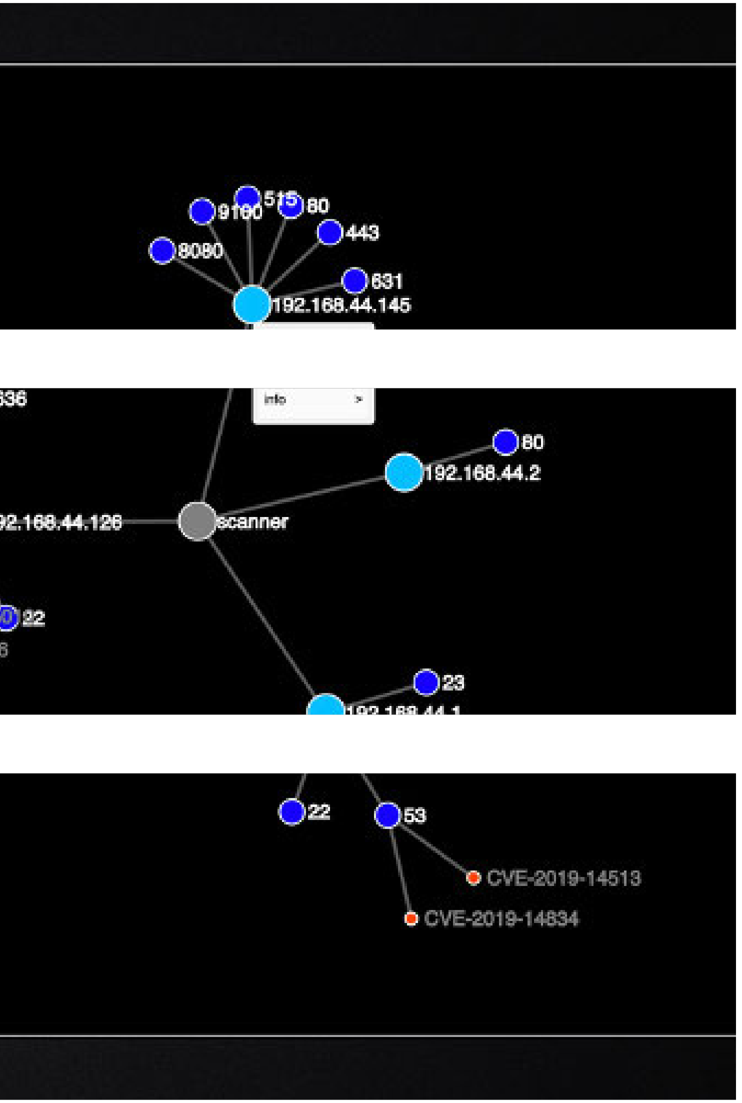
Enables cyber defenders to see their defenses from the perspective of the adversary.

> *"Adversary emulation plans are a high priority for Fujitsu. These should help not just large enterprises with their own red teams, but smaller businesses once the emulations are automated."*

- Ryusuke Masuoka, Research Principal
Fujitsu System Integration Laboratories

CALDERA PATHFINDER

Published: 13 October 2020



Summary

This open-source CALDERA™ plugin helps you understand what a vulnerability exposes to an adversary, and what potential destructive paths an adversary could take within the network as a result of those vulnerabilities. Pathfinder aims to push the boundaries on vulnerability scanning, moving them to the next generation by integrating vulnerability scan data with the CALDERA automated adversary emulation platform. Pathfinder first conducts a scan of a target network, and the results of the scan are ingested into CALDERA's knowledge store, where it can then map out the network. Pathfinder is then able to combine the information from the scan with the power of a breach and attack simulation tool in order to map out potential attack paths within the target network.

Funding Research Participants

SIEMENS

Problem

Traditional vulnerability scanning often lacks the perspective of the adversary and doesn't effectively convey the true impact of a given vulnerability in your organization.

Solution

Push the boundaries on vulnerability scanning, moving them to the next generation by integrating vulnerability scan data with the CALDERA automated adversary emulation platform.

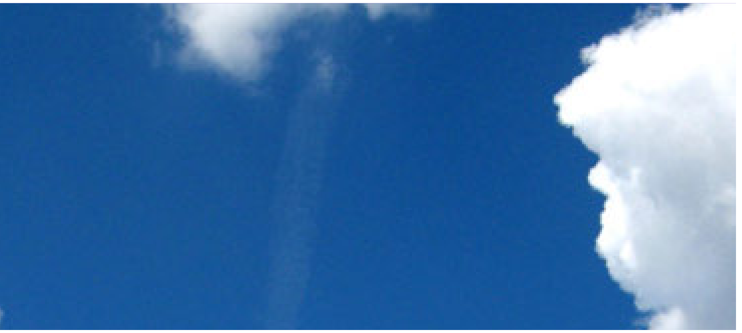
Impact

Show defenders what a vulnerability exposes to an adversary and what potential destructive paths an adversary could take within the network as a result of those vulnerabilities.

> *“Combining the frameworks of CALDERA and SiESTA enables us to establish practical and powerful tooling for OT attack simulation.”*
>
> **- Klaus Lukas, Principal Key Expert ProductCERT**
> **Siemens AG**

ATT&CK FOR CLOUD

Published: 19 August 2020



Summary

This project refined and expanded MITRE ATT&CK's coverage of adversary behaviors in cloud environments. Through our research, we refactored and consolidated the cloud platforms into IaaS, SaaS, Office365, and Azure AD. Next, we overhauled cloud data sources to better align with enterprise ATT&CK. Finally, we expanded cloud technique coverage, adding and updating existing techniques.

Funding Research Participants

ATTACKIQ citi

JPMorgan Chase & Co.

Problem ⚠

Defenders lack visibility into adversary behaviors in cloud technologies, leaving their organizations exposed to emerging threats.

Solution 💡

Expand MITRE ATT&CK to describe adversary behaviors in and against cloud technologies.

Impact ⇒

Simplified defenders use of ATT&CK by aligning ATT&CK's coverage for Cloud TTPs with how organizations are using Cloud in their operations.

> *"The Center for Threat-Informed Defense gives the private sector an influential voice in guiding MITRE Engenuity's current and future research."*
>
> **- Daniel Bernholz, Executive Director in Cybersecurity & Technology Controls**
> **JP Morgan Chase Bank**

NIST 800-53 CONTROLS TO ATT&CK MAPPINGS

Published: 10 August 2021

Summary

This project created a comprehensive set of mappings between MITRE ATT&CK and NIST Special Publication 800-53 with supporting documentation and resources. These mappings provide a critically important resource for organizations to assess their security control coverage against real-world threats as described in the ATT&CK knowledge base, and provide a foundation for integrating ATT&CK-based threat information into the risk management process. With over 6,300 individual mappings between NIST 800 53 and ATT&CK, this resource greatly reduces the burden on the community to do their own baseline mappings – allowing organizations to focus their limited time and resources on understanding how controls map to threats in their specific environment.

Funding Research Participants

ATTACKIQ JPMORGAN CHASE & CO.

Non-Profit Research Participants

CIS Center for Internet Security

Problem

Large and complex security control frameworks such as NIST 800-53 do not relate to actionable TTPs in ATT&CK.

Solution

Create a comprehensive and open curated set of mappings between 800-53 controls and ATT&CK techniques.

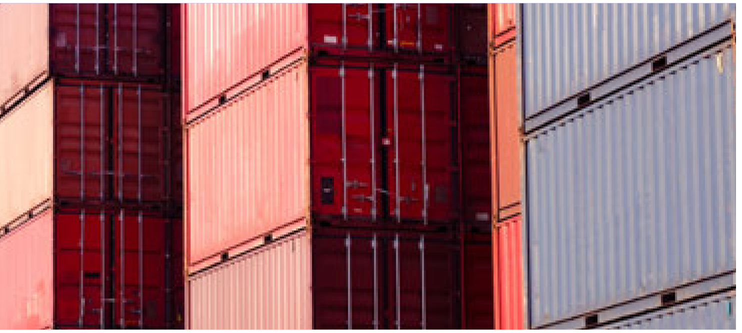
Impact

Defenders can quickly focus on understanding how the controls in use in their environment relate to adversary TTPs of interest to them.

> *“In ground-breaking research, the Center for Threat-Informed Defense aligned the world’s two most important threat and risk management frameworks: MITRE ATT&CK and NIST 800-53. Why is this important? Compliance in and of itself does not equal security. With this research, you can now use MITRE ATT&CK to validate your compliance controls. The result: a revolutionary increase in security readiness.”*
>
> **- Carl Wright, Chief Commercial Officer**
> **AttackIQ**

ATT&CK FOR CONTAINERS

Published: 03 May 2021



Summary

This project investigated the viability of adding container-related techniques into MITRE ATT&CK, leading to the development of an ATT&CK for Containers matrix. This work covers both orchestration-level (e.g., Kubernetes) and container-level (e.g., Docker) adversary behaviors in a single Containers platform, which has been incorporated in version 9 of ATT&CK. The project team worked with contributors from around the world to identify and refine both existing ATT&CK techniques as well as completely new container-specific ones.

The ATT&CK for Containers matrix contains:

- 21 techniques
- 11 sub-techniques
- 8 new container-specific techniques
- 3 new container-specific malware entries

Funding Research Participants

citi JPMorgan Chase & Co.

Microsoft

Problem

Defenders lack visibility into adversary behaviors in and against container technologies, leaving their organizations exposed to emerging threats.

Solution

Expand MITRE ATT&CK to describe adversary behaviors in and against container technologies, including Docker and Kubernetes.

Impact

Brings focus to adversary behaviors in an emergent domain, leveraging the well-understood and widely adopted ATT&CK methodology.

> *“Microsoft’s partnership with the Center for Threat-Informed Defense on investigating and understanding container threats doesn’t stop with the release of its ATT&CK for Containers Matrix. Microsoft will continue to work with the Center to share intelligence and insights from Microsoft’s products, sensors, and research.”*

- Tanmay Ganacharya, Partner Director, Microsoft Defender Security Research
Microsoft

ATT&CK WORKBENCH

Published: 22 June 2021

Summary

ATT&CK Workbench is an easy-to-use, open-source tool that allows organizations to manage and extend their own local version of ATT&CK and keep it in sync with MITRE's knowledge base. Workbench allows users to explore, create, annotate, and share extensions of the ATT&CK knowledge base. Organizations or individuals can run their own instances of the application to serve as the centerpiece to a customized version of the ATT&CK knowledge base, attaching other tools and interfaces as desired. Through the Workbench, this local knowledge base can be extended with new or updated techniques, tactics, mitigations groups, and software. Additionally, Workbench provides the means for a user to share their extensions with the greater ATT&CK community, facilitating a greater level of collaboration within the community than is possible with current tools.

Funding Research Participants

ATTACKIQ

HCA Healthcare

JPMorgan Chase & Co.

Microsoft

verizon

Problem

Defenders struggle to integrate their organization's local knowledge of adversaries and their TTPs with the public ATT&CK knowledge base.

Solution

Build an easy-to-use, open-source software tool that allows organizations to manage and extend their own local version of ATT&CK and keep it in sync with MITRE's knowledge base.

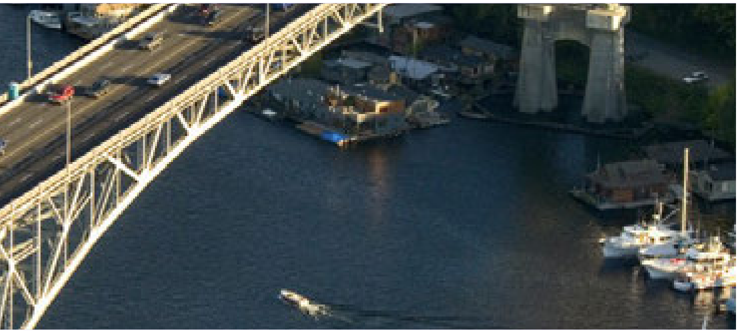
Impact

Drastically reduces the barriers for defenders to ensure that their threat intelligence is aligned with the public ATT&CK knowledge base.

> *"The ATT&CK Workbench is a great platform to layer internal intelligence on top of MITRE ATT&CK."*
>
> **- David Vasil, Security Threat Architect**
> **HCA Healthcare**

SECURITY STACK MAPPINGS AZURE

Published: 29 June 2021



Summary

This project empowers organizations with independent data on which native Azure security controls are most useful in defending against the adversary TTPs that they care about. It achieves this by mapping security capabilities of Azure to the ATT&CK techniques that they can protect, detect, or respond to. This will allow organizations to make threat-informed decisions when selecting which native security capabilities to use to protect their workloads.

Funding Research Participants

ATTACKIQ

EY Building a better working world

HCA Healthcare

JPMorgan Chase & Co.

Microsoft

usbank

verizon

Problem

Users of Azure lack a comprehensive view of how native Azure security controls can help defend against real-world adversary TTPs.

Solution

Build a scoring methodology and use it to create mappings showing how effective native Azure security controls are in defending against specific ATT&CK techniques.

Impact

Empowers defenders with independent data on which Azure controls are most useful in defending against the adversary TTPs they care about.

> *“Azure Security Stack Mappings will provide a way to cross-map a set of ATT&CK techniques against Azure services and vice-versa to help identify the detection use cases that provide the greatest coverage for cloud workloads.”*

- David Vasil, Security Threat Architect
HCA Healthcare

ATOMIC DATA SOURCES

Published: 19 August 2021

Summary

Cyber threat detection starts with understanding the data sources and sensors that can be used to detect a given adversary TTP. Motivated by a lack of detailed data source definitions in MITRE ATT&CK to support defensive cyber operations use cases, we wanted to greatly expand the set of data sources in ATT&CK and research creating an open data model for data sources that would enable defenders to quickly determine if they have the data necessary to detect the adversary TTPs they care about. We worked with Center participants to develop a prototype model for describing data sources, as well as identifying and documenting a set of data sources that would ultimately be contributed to the ATT&CK Data Sources project.

Problem

Existing definitions of data sources necessary to detect adversary behavior are insufficient.

Solution

Create a single, coherent, and open data model for the data sources in ATT&CK and greatly expand upon those data sources.

Impact

Defenders are able to quickly determine if they have the data necessary to detect the adversary TTPs they care about.

Funding Research Participants

HCA Healthcare · red canary · SIEMENS · verizon

"The Atomic Data Sources will help our team understand what sources of telemetry will provide the most value for creating threat detections."

- David Vasil, Security Threat Architect
HCA Healthcare

"You can't detect what you can't see. We've always placed a premium on understanding and providing the value of the data that we leverage for detection and response. The improved Atomic Data Sources will do for security architects, engineers, and researchers what the original ATT&CK model did for detection and response teams: Provide a clear, comprehensive, and common language that we can use to describe the data that we need to observe the techniques leveraged by modern threats."

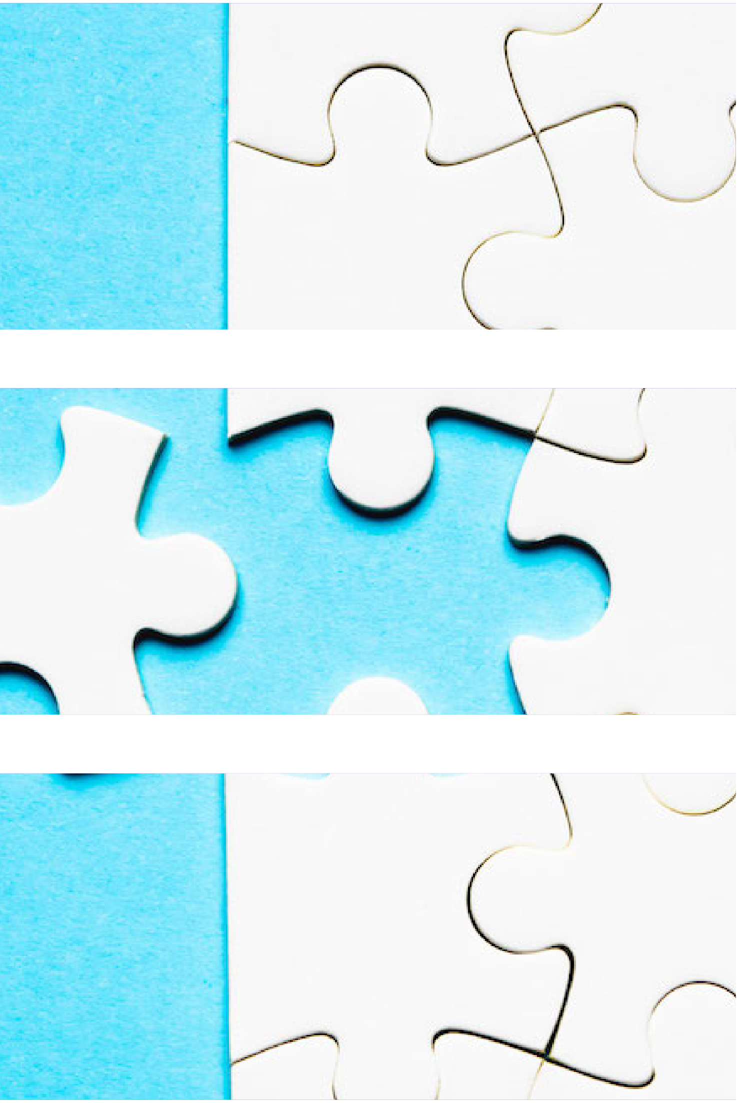
- Keith McCammon, Co-founder and Chief Security Officer
Red Canary

"Data modeling and data governance are key to defenders and developers alike. The results of this project greatly support our continuous efforts to identify data sources that are most helpful in the detection of adversary activity."

- Hans Wallinger, Head Cyberdefense Innovation & Platform
Siemens AG

ATT&CK INTEGRATION INTO VERIS

Published: 26 August 2021



Summary

This project created a mapping and translation layer between VERIS and ATT&CK that allows ATT&CK to describe the adversary behaviors that were observed in an incident coded in VERIS. This creates the opportunity for a joint analysis of the information that ATT&CK describes well (the behaviors adversaries use to attack systems) alongside the incident demographics and metadata that VERIS describes well.

Funding Research Participants

SIEMENS verizon✓

Non-Profit Research Participants

CIS Center for Internet Security®

Problem

Users of the VERIS data model lack a well-defined way to link incidents described in VERIS to the underlying adversary TTPs used in that incident.

Solution

Build and document a common and open method to link data in the VERIS format to specific ATT&CK TTPs.

Impact

Empowers defenders to efficiently tie adversary TTPs to their real-world impact by connecting ATT&CK-based threat intel to VERIS-based incident reports.

> *“We believe that it is critical to empower the community to connect the strategic view provided by VERIS with the more tactical view provided by MITRE ATT&CK.”*
>
> **- Alex Pinto, Senior Manager DBIR Team**
> **Verizon**

SECURITY STACK MAPPINGS AWS

Published: 21 September 2021

Summary

This project empowers organizations with independent data on which native AWS security controls are most useful to defend against the adversary TTPs that they care about. It achieves this by mapping security capabilities of AWS to the ATT&CK techniques that they can protect, detect, or respond to. This will allow organizations to make threat-informed decisions when selecting which native security capabilities to use to protect their workloads.

Funding Research Participants

ATTACKIQ

citi

FUJITSU

SIEMENS

verizon

Non-Profit Research Participants

CIS Center for Internet Security

Problem

Users of AWS lack a comprehensive view of how native AWS security controls defend against real-world adversary TTPs.

Solution

Map the effectiveness of each AWS security control against specific ATT&CK techniques.

Impact

Empowers defenders with independent assessments of which AWS controls are effective to mitigate relevant adversary TTPs.

> *“We have realized that the Security Stack Mappings projects, which align various security frameworks to MITRE ATT&CK, should be very useful in ATT&CK-based SOC assessments.”*
>
> **- Ryusuke Masuoka, Research Principal**
> **Fujitsu System Integration Laboratories**

THREAT REPORT ATT&CK MAPPER (TRAM)

Published: 30 September 2021

Summary

TRAM is an open-source platform designed to advance research into automating the mapping of cyber threat intelligence reports to MITRE ATT&CK. TRAM enables researchers to test and refine Machine Learning (ML) models for identifying ATT&CK techniques in prose-based threat intel reports and allows threat intel analysts to train ML models and validate ML results.

Through research into automating the mapping of cyber threat intel reports to ATT&CK, TRAM aims to reduce the cost and increase the effectiveness of integrating ATT&CK into cyber threat intelligence across the community. Threat intel providers, threat intel platforms, and analysts should be able to use TRAM to integrate ATT&CK more easily and consistently into their products.

Funding Research Participants

citi

HCA Healthcare

Problem

Mapping new threat intel reports to ATT&CK is difficult, error prone, and time consuming.

Solution

Develop an open-source platform for researching the application of NLP and ML to identify TTPs in threat intel reports and allow analysts to validate those TTPs.

Impact

Accelerate research into automated TTP identification in threat intel reports to greatly reduce the time and effort required to integrate new intelligence into cyber operations.

> “*Participating in Center research alongside the other industry thought leaders has helped accelerate and streamline our intelligence and cyber defense programs.*”

- TJ Bean, Director of CyberSecurity
HCA Healthcare

MAPPING ATT&CK TO CVE FOR IMPACT

Published: 28 October 2021

Summary

This research defines a methodology for using MITRE ATT&CK to characterize the potential impacts of vulnerabilities. ATT&CK's tactics and techniques enable defenders to quickly understand how a vulnerability can impact them. Vulnerability reporters can use the methodology to describe the impact of vulnerabilties, enabling defenders to easily integrate vulnerability information into their risk models and identify appropriate compensating security controls. This methodology aims to establish a critical connection between vulnerability management, threat modeling, and compensating controls.

Funding Research Participants

ATTACKIQ

JPMorgan Chase & Co.

Problem

Defenders struggle to integrate vulnerability and threat information and lack a consistent view of how adversaries use vulnerabilities to achieve their goals. Without this context, it is difficult to appropriately prioritize vulnerabilites.

Solution

Develop a methodology to use the adversary behaviors described in ATT&CK to characterize the impact of CVEs, providing much-needed context.

Impact

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 specific vulnerabilities in their environment.

> *"As a Founding Partner, JPMorgan Chase & Co. is actively committed to solving the cybersecurity industry's most pressing challenges."*
>
> **- Daniel Bernholz, Executive Director in Cybersecurity & Technology Controls**
> **JP Morgan Chase Bank**

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.

https://ctid.mitre-engenuity.org/

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

About MITRE Engenuity

MITRE Engenuity is a tech foundation that collaborates with the private sector on challenges that demand public interest solutions, to include cybersecurity, infrastructure resilience, healthcare effectiveness, microelectronics, quantum sensing and next generation communications.

www.mitre-engenuity.org

Document number CT0038

MITRE ENGENUITY™ | Center for Threat Informed Defense