

Celebrating Five Years 2019 > 2024

# 2024IMPACTREPORT

**MITRE** | Center for Threat  
Informed Defense™

# MITRE | Center for Threat Informed Defense™

The Center for Threat-Informed Defense unites sophisticated cybersecurity teams from around the world for one purpose—advance threat-informed defense for all. Their insight, expertise, and support make the Center a powerful force in changing the game on the adversary. Together, we learn, identify critical challenges, and create practical solutions for all.

Participant organizations power the Center for Threat-Informed Defense. They bring their operational experience and perspective to guide the program to create timely, relevant, and actionable solutions that security teams can use today.

Together, we advance the state of the art and state of the practice in threat-informed defense.

## RESEARCH PARTNERS

ATTACKIQ®  
FOUNDER

BANK OF AMERICA   
FOUNDER

citi  
FOUNDER

  
CROWDSTRIKE

FORTINET®

HCA   
Healthcare™  
FOUNDER

 IBM Security

JPMorganChase  
FOUNDER


LLOYDS  
BANKING GROUP 

 Microsoft  
FOUNDER

verizon  
business

## RESEARCH SPONSORS

ANOMALI  BlueRock

Booz | Allen | Hamilton\*  
FOUNDER 

   
FOUNDER

Google Cloud  HIDDENLAYER

## NON-PROFIT PARTICIPANTS

  
Analysis &  
Resilience Center  
FOR SYSTEMIC RISK

 CIS. Center for Internet Security\*

   
FOUNDER

  
Improving Security Together

 FS-ISAC

 GLOBAL  
CYBER  
ALLIANCE.

 GLOBAL  
RESILIENCE  
FEDERATION

 Health-ISAC™  
Collaborating for Resilience in Healthcare

 NRF® NATIONAL  
RETAIL  
FEDERATION

 RETAIL & HOSPITALITY  
ISAC

# CONTENTS

Letter from the Director ..... 4

Special Thanks to Our Founders..... 6

Security Stack Mappings—  
Hardware-Enabled Defense ..... 8

Summitting the Pyramid ..... 10

Secure AI..... 12

Technique Inference Engine..... 14

Defending OT with ATT&CK..... 16

Threat Modeling with ATT&CK ..... 18

CWE with Environmental CVSS Calculator.. 20

Security Stack Mappings—  
Microsoft 365..... 22

Measure, Maximize, and Mature  
Threat-Informed Defense..... 24

Mappings Explorer..... 26

Sightings Ecosystem..... 28

Insider Threat TTP Knowledge Base..... 30

Advisory Council..... 32

Become a Benefactor ..... 34

Celebrating the Contributor Community..... 35

How To Get Involved ..... 36

Our Work ..... 38

# LETTER FROM THE DIRECTOR

In November 2019, the Center for Threat-Informed Defense launched with the support of 13 Founders and a pipeline of game-changing research projects. The first of those audacious projects—advance adversary emulation for all with a community library of emulations plans—was released in September 2020. And, by the end of 2021, a total of 13 research projects would be studied, evaluated, developed, and tested by teams of Center Participants for immediate adoption by any threat-informed defender.

## OUR IMPACT

As we celebrate the 5th anniversary of the launch of the Center, we start with our Founders and the alliance of Center Participants that has followed in their footsteps building a legacy of impactful research and development and nurturing a global community of threat-informed defenders.

## OUR COMMUNITY

Over the past five years, the Center has welcomed more than 750 researchers from



“

The fact that these developments are made available to the community free of charge shows how extraordinary this institution is. The world’s brightest minds develop innovative solutions for all of us GLOBALLY.”

**Simone Kraus**

Senior CSIRT Analyst, Orange Cyberdefense

**750+**

RESEARCHERS

**40**

OPEN-SOURCE  
PROJECTS

46 global organizations through our doors to work side-by-side in pursuit of the release of 40 open-source research projects attracting the attention of tens of thousands of ATT&CK community members on social media, by word of mouth, and at conferences and trainings worldwide. Each research project is consistently received by the community with praise, accolades, and sincere gratitude for our work.

## OUR FUTURE

Our successes are a testament to the commitment of our members. In a field that moves at mind-blowing speed, keeping up with the adversary is hard enough, let alone getting one step ahead. The shared experiences of our members and the broader community enable rapid learning and global impact. The Center for Threat-Informed Defense of the future is only as impactful as the members it represents.

Together, we collaborate, learn, and solve operational cybersecurity problems to address member needs and advance threat-informed defense for all.

Learn how the Center’s R&D program works and how your team can be stronger, smarter, and more impactful as a Center Research Participant. I look forward to exploring with you how we can work together.

## JON BAKER

*Director, Center for  
Threat-Informed Defense  
MITRE*



# SPECIAL THANKS TO OUR FOUNDERS

ATTACKIQ®

BANK OF AMERICA 

Booz | Allen | Hamilton®

citi

CYBER  
THREAT  
ALLIANCE

## ATTACKIQ

*Founding Research Partner*

“

AttackIQ is honored to have contributed to this groundbreaking initiative, building a thriving community dedicated to advancing impactful research and driving the adoption of threat-informed defense practices.”

**Carl Wright**

Chief Commercial Officer

## BOOZ ALLEN HAMILTON

*Founding Research Sponsor*

“

Today’s threat landscape has reached a level of complexity never seen before. This requires industry collaboration to create new and rapidly deployable solutions. The Center for Threat-Informed Defense plays a unique and critical role in developing this advanced R&D. As a Founder, Booz Allen celebrates the 5th Anniversary of the Center’s launch and is committed to furthering an environment of continuous collaboration and solution development aimed at countering the adversary.”

**Garrettson Blight**

Vice President

## CYBER THREAT ALLIANCE

*Founding Non-Profit Participant*

“

The mission of Cyber Threat Alliance and the Center for Threat-Informed Defense could not be more aligned today than it was back in 2019. CTA members, some of whom are also Center members, have benefited greatly not only from the Center’s work but from the opportunity to gain insight into the work through our relationship.”

**J. Michael Daniel**

President & CEO



## JPMORGAN CHASE

*Founding Research Partner*



The depth and breadth of the research that JPMC has been a part of as a Founding Partner in the Center for Threat-Informed Defense is far more valuable than if we had been working on our own. Having completed 26 R&D projects in five years is an impressive achievement on its own. But to work alongside and learn from a membership of world-class cybersecurity teams from across industry gave us insight and experiences that we could not have had working on our own.”

**DeKovan Lewis**

Sr. Lead Cybersecurity Architect—  
Cybersecurity & Tech Controls

## MICROSOFT

*Founding Research Partner*



Community is one of Microsoft’s core values both in terms of creating community and giving back to the community. Joining the Center as a Founder provided a clear path to helping us better achieve that goal. Our membership provides Microsoft the opportunity to educate the cybersecurity community, provide the tools the community needs to protect itself, and empower organizations with open-sourced research to be able to build better defenses.”

**Karthik Selvaraj**

Partner Director of Security  
Research

## SIEMENS AG

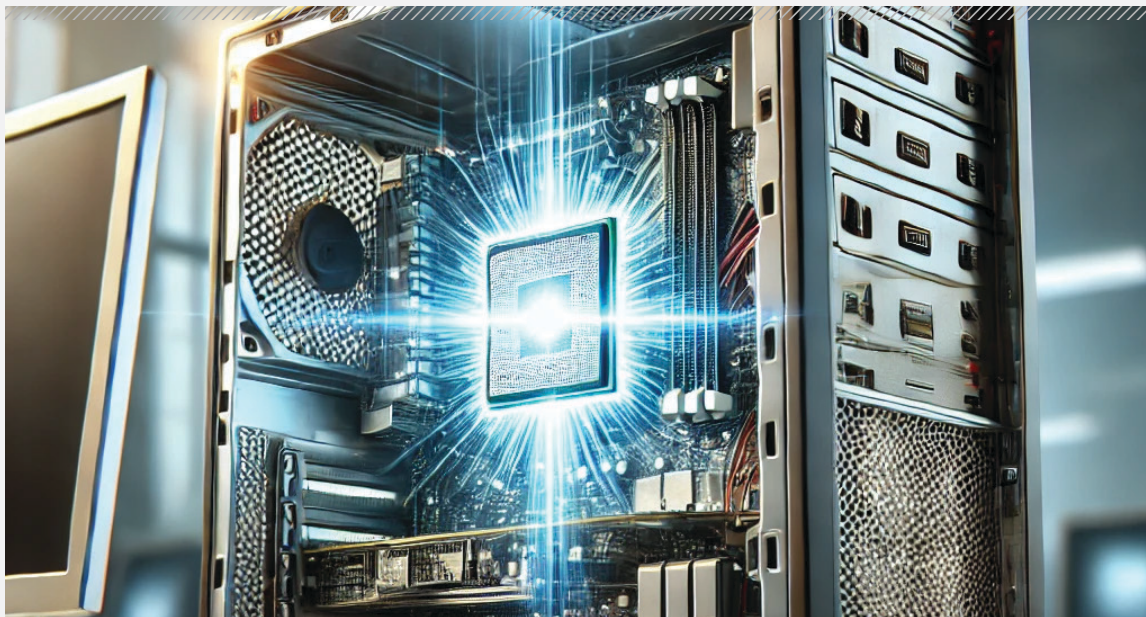
*Founding Research Sponsor*



When we joined the Center as a Founding Research Sponsor in 2019 our mission was to actively contribute and sponsor community efforts on cyber defense advancements and to learn from our engagements with the greater ATT&CK community and industry leading experts. Five years later we are happy to see the number of motivated contributors growing and we are excited to be part of that movement.”

**Michael Pascher**

Senior Key Expert



PUBLISHED JANUARY 2025

## SECURITY STACK MAPPINGS— HARDWARE-ENABLED DEFENSE →

The Security Stack Mappings—Hardware-Enabled Defense project demonstrates full stack threat-informed defense, from the hardware board to the software bytes. These mappings enable threat-informed defenders to understand how these additive capabilities can mitigate real-world adversary behaviors.

### PROJECT SPONSORS

ATTACKIQ®



intel.





## Problem

System security is available at the hardware level to provide protection from adversarial threats; however, these countermeasures are not well known to security practitioners.



## Solution

Apply the security stack mapping methodology to connect hardware security capabilities of standard enterprise-class systems to adversarial behaviors as described in MITRE ATT&CK®.



## Impact

Cyber defenders apply hardware-assisted security features to counter specific adversarial threats and provide defense-in-depth of systems and data, better securing billions of devices.

“

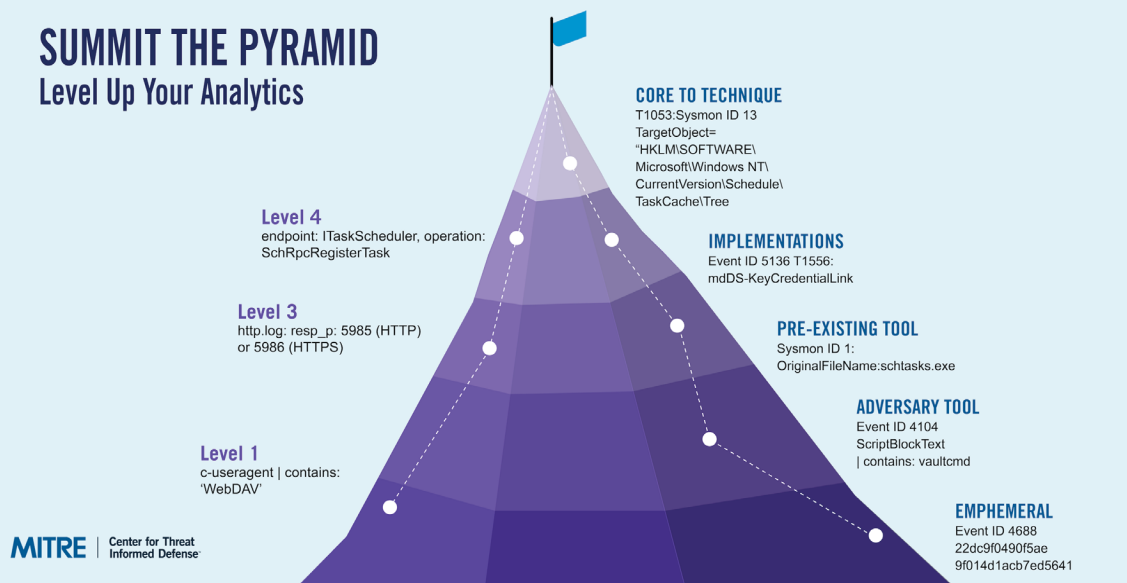
The joint MITRE Center for Threat-Informed Defense mapping project was a priority for Intel's commercial product launch as we wanted to highlight Intel vPro® Security and how our unique capabilities can help mitigate real world attacks. Understanding where silicon-enabled security can bolster security software and the OS to better detect attacks had never been looked at before. This was a valuable opportunity for Intel to partner with the Center and industry to independently validate the mappings.”

**Carla Rodriguez**

VP and GM Intel Client Software Enabling, Intel Corporation

## SUMMIT THE PYRAMID

### Level Up Your Analytics



PUBLISHED DECEMBER 2024

## SUMMITTING THE PYRAMID →

Summitting the Pyramid (STP) guides detection engineers to make cyber analytics more difficult for adversaries to evade. STP's methodology scores analytics against the Pyramid of Pain, helping defenders evaluate and create more robust detections against adversary behavior.

### PROJECT SPONSORS

ATTACK IQ®

FORTINET®

IBM Security



Microsoft



## Problem

Adversaries can easily evade cyber analytics that are dependent on specific tools or artifacts.



## Solution

Create and apply a methodology to evaluate the dependencies inside analytics and make them more robust by focusing on adversary behaviors.



## Impact

Shift the advantage towards defenders with improved analytics that catch adversaries even as they evolve and detect future campaigns.

“

Establishing a reliable detection model is essential, even as TTPs evolve. Summiting the Pyramid II addresses this challenge by offering an enhanced methodology to evaluate analytics against the Pyramid of Pain. This enables defenders to measure the effectiveness of their detections and adapt to adversary techniques faster and more effectively.”

**Carl Wright**

Chief Commercial Officer, AttackIQ





PUBLISHED DECEMBER 2024

## SECURE AI →

In collaboration with MITRE ATLAS™, the Secure AI project brings a threat-informed approach to understanding threats to AI-enabled systems, emulating them, and mitigating them. The project facilitates rapid communication of evolving vulnerabilities in the AI security space through effective incident sharing and boosts community knowledge of threats to AI-enabled systems.

### PROJECT SPONSORS

ATTACK IQ®



Booz | Allen | Hamilton®



JPMorganChase







## Problem

AI-enabled systems are susceptible to traditional cybersecurity vulnerabilities, and new attacks based on the unique characteristics of AI-enabled systems.



## Solution

Accelerate the development of MITRE ATLAS to meet industry needs in AI security, including incident sharing, new threats to Generative AI, and mitigations.



## Impact

Secure organizations against the unique emergent attack surfaces that arise in complex AI-enabled systems.

“

Advancing community-wide knowledge of threats to AI is crucial to enabling its secure adoption. By partnering with industry leaders across financial, healthcare, technology, and public sectors, we collectively build upon MITRE ATLAS to deepen our understanding of AI threats and develop comprehensive and effective mitigation strategies.”

**Malcolm Harkins**

Chief Security & Trust Officer, HiddenLayer

“

The level of knowledge and expertise from the Center for Threat-Informed Defense team and other industry partners made engaging in this project quite a learning experience. We found ourselves watching, listening and learning, and really benefiting from their knowledge. These people really understand their stuff.”

**John Walsh**

VP Business Development, BlueRock



PUBLISHED SEPTEMBER 2024

## TECHNIQUE INFERENCE ENGINE →

Know your adversary's next move with the Technique Inference Engine (TIE), a machine learning-powered tool that infers unseen adversary techniques, providing security teams actionable intelligence.

### PROJECT SPONSORS



IBM Security



NON-PROFIT  
PARTICIPANT:





## Problem

Detections only find techniques for which we have an alert and fall short of guiding us to other likely-used techniques.



## Solution

A model to infer an attacker's next technique, based on observed adversary operations.



## Impact

Analysts identify more intrusion methods with fewer detections and thus reduce mean time to respond.

“

TIE is a game-changer for integrating threat intelligence into cyber operations. Predicting adversary activities based on observed techniques will undoubtedly enhance how threat hunters, SOC analysts, and CTI teams operate. TIE is a huge step towards helping us stay ahead of the adversary.”



PUBLISHED AUGUST 2024

## DEFENDING OT WITH ATT&CK →

Defending Operational Technology (OT) with ATT&CK provides a customized collection of MITRE ATT&CK® techniques tailored to the attack surface and threat model for OT environments. The resultant resources can be used by organizations that use OT to evaluate and employ security controls for real-world adversary behaviors targeting those environments.

### PROJECT SPONSORS

ATTACK IQ®

Booz | Allen | Hamilton®

ENSIGN  
INFOSECURITY

SIEMENS

NON-PROFIT  
PARTICIAN:  GLOBAL  
CYBER  
ALLIANCE.



## Problem

Organizations need to understand the techniques adversaries use against OT and the enterprise systems that manage OT.



## Solution

Develop a straightforward approach to understanding and working with the techniques applicable to OT.



## Impact

Organizations defend against the full set of techniques against OT.

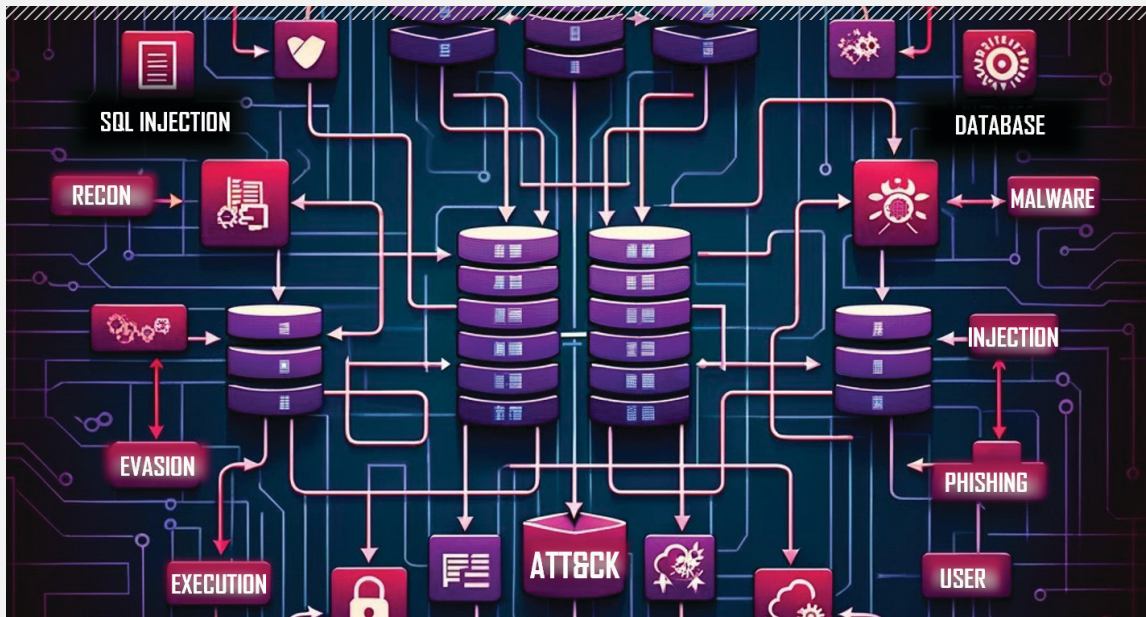
“

Our involvement in the Defending OT (DOT) with ATT&CK initiative, in collaboration with the Center for Threat-Informed Defense, underscores our commitment to advancing OT security and significantly enhances our expertise in OT defence. The customised collection of MITRE ATT&CK techniques, tailored to address the unique attack surface and threat landscape of OT environment, will contribute to greater cybersecurity for Critical Information Infrastructure.”

**Dr. Jonathan Goh**

Director of Machine Learning Operations and OT Analytics, Ensign InfoSecurity





PUBLISHED JULY 2024

## THREAT MODELING WITH ATT&CK →

Threat Modeling with ATT&CK defines how to integrate MITRE ATT&CK® into your organization's threat modeling practice. This process is intended for universal application to any system or technology stack (large or small) using existing threat modeling methodologies like STRIDE, PASTA, or Attack Trees.

### PROJECT SPONSORS





## Problem

There is a lack of guidance on how to best utilize ATT&CK to improve existing threat modeling practices.



## Solution

Develop a process to integrate ATT&CK into existing threat modeling methodologies that will enable companies to identify critical assets, assess threats to these assets, measure existing defensive capabilities, and recommend mitigations.



## Impact

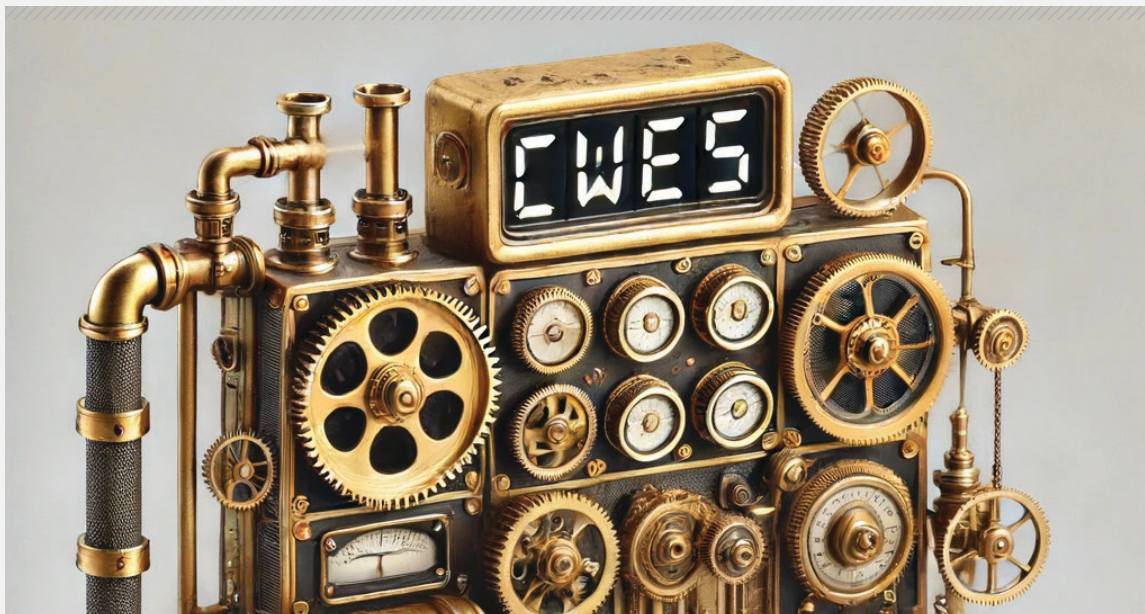
Companies will tailor their defensive investments to mitigate threats to their most critical assets.

“

It is imperative for any organization to understand adversary capabilities, identify defensive gaps, and prioritize mitigation strategies. Threat modeling with ATT&CK supports this endeavor by defining a method for incorporating curated knowledge of adversary tactics and techniques, as documented in MITRE ATT&CK, into your organization's threat modeling approach.”

**Hans Wallinger**

Senior Director Cybersecurity Intelligence & Automation, Infineon



PUBLISHED JUNE 2024

## CWE™ WITH ENVIRONMENTAL CVSS CALCULATOR →

The software industry is faced with managing large numbers of software weaknesses (commonly identified by static-scanning tools using CWE ID reference), alongside large numbers of software vulnerabilities (CVEs®), which all sit across many assets with differing security requirements. The calculator enables software development teams to score and prioritize software weaknesses empirically based on data in the National Vulnerability Database (NVD).

### PROJECT SPONSORS







## Problem

Without a common system of comparison across CWEs and CVEs that factors in environmental context, engineering teams cannot effectively prioritize their work, and thus waste cycles on wrong things while they miss opportunities to secure systems.



## Solution

The CWE with Environmental CVSS Calculator will provide output that effectively enables a CWE in a specified environment to be priority ranked against a CVE in the same or different environment.



## Impact

Software development teams will focus their limited resources on addressing the most dangerous issues.

“

The CWE with Environmental CVSS Calculator is an important part of a risk-based strategy and enables a more cohesive analysis of software weaknesses and vulnerabilities.”



PUBLISHED APRIL 2024

## SECURITY STACK MAPPINGS—MICROSOFT 365 →

The project presents a comprehensive mapping of M365's native security features against MITRE ATT&CK®, detailing how these capabilities can protect, detect, and respond to cyber threats. By reviewing M365 documentation, the project identifies security actions that can mitigate adversary behaviors, providing a valuable tool for organizations to improve their threat-informed defense strategies.

### PROJECT SPONSORS

ATTACKIQ®

citi

JPMorganChase

verizon  
business

NON-PROFIT  
PARTICIPANT:

CIS. Center for Internet Security®



## Problem

Users of M365 lack a comprehensive view of how native M365 security controls can help defend against real-world adversary TTPs.



## Solution

Create mappings to show which M365 native security controls can defend against specific ATT&CK techniques.



## Impact

Empower defenders with independent assessments of which M365 controls mitigate relevant adversary TTPs.

“

Adversary behavior can no longer be a guessing game. Users of M365 greatly needed this resource of independent assessments and a comprehensive view of how M365 product security capabilities can be used to mitigate real-world threats. With these mappings we're doing more than just checking the box.”

**DeKovan Lewis**

Senior Lead Cybersecurity Architect—Cybersecurity & Tech Controls, JPMorgan Chase



PUBLISHED APRIL 2024

## MEASURE, MAXIMIZE, AND MATURE THREAT-INFORMED DEFENSE →

The Measure, Maximize, and Mature Threat-Informed Defense (M3TID) project defines threat-informed defense and the key activities associated with its practice. The project captures insights and best practices for what it means to be threat-informed across a security program, expanding the dimensions of threat-informed defense into key components that organizations can measure against and implement. With M3TID organizations can assess and understand the current and future state of their threat-informed defense program.

### PROJECT SPONSORS

ATTACK IQ®



HCA+  
Healthcare™

IBM Security

JPMorganChase



SAFE

verizon  
business



## Problem

Using a threat-informed defense is one of the most effective ways to defend yourself against cyber-attacks, yet there is no definitive guidance on how to create and mature threat-informed defense.



## Solution

Create a foundational resource that defines threat-informed defense, all of its components, and develop a solution to measure, maximize, and mature threat-informed defense.



## Impact

Organizations can strategically enhance their cybersecurity capabilities, optimize resource allocation, and improve defenses against cyber-attacks, contributing to a stronger and more resilient infrastructure.

“

M3TID is a fantastic resource that helps organisations understand their threat-informed defense posture, while also providing a framework through which organisations can chart their own course, measure the efficacy, and make decisions implementing the threat-informed defense model.”

**David West**

Head of Cyber Threat Management, National Australia Bank





PUBLISHED MARCH 2024

## MAPPINGS EXPLORER →

Mappings Explorer is a hub for defenders to explore security capabilities mapped to MITRE ATT&CK®. This resource enables cyber defenders to understand how security controls and capabilities protect against the adversary behaviors catalogued in the ATT&CK knowledge base. Our mappings bridge the threat-informed approach to cybersecurity with traditional cyber hygiene and enable threat-informed decision making by relating real-world threats to corresponding security capabilities.

### PROJECT SPONSORS

ATTACKIQ®



JPMorganChase



IBM Security



## Problem

Defenders lack a single resource to view defensive capabilities mapped to the adversarial attack techniques in ATT&CK.



## Solution

Create a central hub that provides access to all mappings, and offer standard tools and processes for developing mappings to ATT&CK.



## Impact

Defenders can easily access and explore mapped security controls from the perspective of the ATT&CK techniques they mitigate.



Mappings Explorer allows our team to identify available mitigating security controls for specific techniques associated with particular threats we're investigating. The amount of native security controls that MapEX demonstrates can mitigate adversary threats was a welcomed surprise that will end up saving us time and money. Mappings Explorer is a gamechanger!"



PUBLISHED MARCH 2024

## SIGHTINGS ECOSYSTEM →

This project provides cybersecurity defenders and researchers with critical insight into real-world adversary behaviors mapped to ATT&CK. The ecosystem fundamentally advances the collective ability to see threat activity across organizational, platform, vendor, and geographical boundaries. Voluntarily contributed raw “sightings”, or observations of specific adversary TTPs, are anonymized, and aggregated to produce insights into the most commonly used attacker techniques.

### PROJECT SPONSORS

ATTACKIQ

FORTINET

HCA  
Healthcare

JPMorganChase

verizon  
business

NON-PROFIT  
PARTICIAN:



CYBER  
THREAT  
ALLIANCE





## Problem

Defenders lack visibility into which adversary behaviors they should focus their attention on first.



## Solution

Build an ecosystem for organizations to safely contribute ATT&CK-specific detection data, empowering defenders to have clear insights what techniques attackers use in the wild.



## Impact

The sightings ecosystem injects real-world data and insights from that data into the decision-making process of defenders, allowing them to focus their resources on the highest priority problems.

“

Two years of data collection and analysis—that included 198 countries, 1.6 million sightings, and 353 unique techniques—led to a Sightings project outcome that provides defenders truly impactful insights into common adversary behavior, including techniques adversaries use and how they apply them.”

**Douglas Santos**

Director, Advanced Threat Intelligence, Fortinet's FortiGuard Labs



PUBLISHED MARCH 2024

## INSIDER THREAT TTP KNOWLEDGE BASE →

The Insider Threat Tactics, Techniques, and Procedures (TTP) Knowledge Base advances our collective understanding of the technical mechanisms that insider threats use. With this knowledge, insider threat programs and security operations centers can detect, mitigate, and emulate insider actions on IT systems to stop insider threats. Utilizing the Knowledge Base, cyber defenders across organizations will identify insider threat activity on IT systems and limit the damage.

### PROJECT SPONSORS

JPMorganChase





## Problem

SOCs and insider threat analysts need to know which technical mechanisms are used by insiders, and what controls mitigate insider threats.



## Solution

Develop an open knowledge base of the tactics, techniques, and procedures used by insiders in IT environments.



## Impact

Defenders detect, mitigate, and emulate insider actions on IT systems and stop them.

“

Our participation in the Insider Threat Project alongside members from other organizations provided valuable insights. While all participants were well-versed in insider threat concepts, each organization's program was tailored to its specific industry and threat landscape. These discussions broadened our perspective and highlighted potential areas for program improvement.”

**Garrett Speace**

Insider Threat Operations, Verizon Business

## ADVISORY COUNCIL

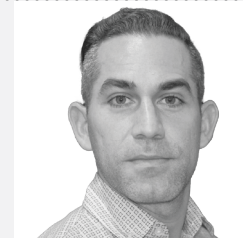
The Advisory Council is comprised of one Advisor from each Founding Center Participant and each Research Partner to provide strategic guidance and executive advocacy in support of the Center's mission. Advisors apply their executive experience to guide the Center as we evolve our strategy, model, and approach to advancing threat-informed defense.

Advisors bring their skill and experience in the industry to guide the direction of the Center's mission and strategy. Their advice is invaluable in ensuring alignment between the Center's mission and the best possible use of its resources with the aim of meeting the needs of the community at large.



**CARL WRIGHT**

Chief Commercial Officer  
AttackIQ  
*Founding Research Partner*



**ELVIS VELIZ**

Global Head of Vulnerability  
Assessments and Cloud Security  
Operations  
Citi  
*Founding Research Partner*



**BRIAN CARVALHO**

Head of Cyber Security  
Architecture & Innovation  
Bank of America  
*Founding Research Partner*



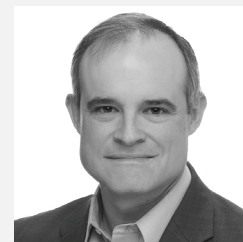
**JOEL SPURLOCK**

VP Data Science  
CrowdStrike  
*Research Partner*



**GARRETTSO BLIGHT**

Vice President,  
Global Government  
Booz Allen Hamilton  
*Founding Research Sponsor*



**MICHAEL DANIEL**

President and CEO  
Cyber Threat Alliance  
*Founding Non-Profit*



### **DEREK MANKY**

Chief Security Strategist & VP  
Global Threat Intelligence  
Fortinet  
*Research Partner*



### **DEKOVAN LEWIS**

Sr Lead Cybersecurity Architect  
—Cybersecurity & Tech Controls  
JPMorgan Chase Bank, N.A.  
*Founding Research Partner*



### **DR. MARTIN OTTO**

Head of Cybersecurity Research  
US  
Siemens AG  
*Founding Research Sponsor*



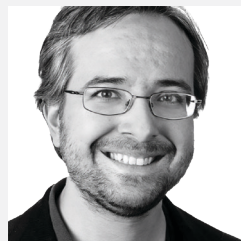
### **SYOICHI KANZAKI**

Senior Expert, National Security  
Business Unit  
Fujitsu  
*Founding Research Sponsor*



### **DEREK WHIGHAM**

Chief Product Owner, Chief  
Security Office  
Lloyds Banking Group  
*Research Partner*



### **ALEX PINTO**

Associate Director, Security  
Research—DBIR  
Verizon Business  
*Research Partner*



### **TJ BEAN**

Chief Information Security  
Officer  
HCA Healthcare  
*Founding Research Partner*



### **KARTHIK SELVARAJ**

Partner Director Security  
Research  
Microsoft  
*Founding Research Partner*

# BECOME A BENEFACTOR

BENEFACTORS ADVANCE CRITICAL, PUBLIC INTEREST CYBERSECURITY THROUGH CHARITABLE GIVING. BENEFACTORS ARE GLOBALLY RECOGNIZED FOR SUPPORTING INDEPENDENT RESEARCH



BECOME A BENEFACTOR

Scan the QR code or visit  
[ctid.mitre.org/donate](https://ctid.mitre.org/donate) →

# CELEBRATING THE CONTRIBUTOR COMMUNITY

Individual contributors play a significant role improving our R&D, providing foundational data to enable research, and scaling the impact of our work.



## SECURE AI

Participate in the AI Incident sharing platform to accelerate community awareness of threats to AI enables systems and support research into techniques to emulate and mitigate those threats.

## STOP INSIDER THREATS

Contributors to the community's first cross-sector, multiorganizational, community-sourced body of Insider Threat data inspired by ATT&CK empower defenders to detect, mitigate, and emulate insider actions on IT systems.

## SIGHTINGS ECOSYSTEM

Contribute data to support community-wide awareness of adversary behaviors in the wild. This foundation data set drives innovation in threat-informed defense and provides defenders with critical insight to enable technique prioritization.



BECOME A CONTRIBUTOR

Scan the QR code or visit [ctid.mitre.org/contributors](https://ctid.mitre.org/contributors) →



## HOW TO GET INVOLVED

Advancing threat-informed defense globally is only possible with the support of a global community. Achieving a truly global impact requires individual contributors that embrace our work and share their feedback to drive continual improvement, organizations that believe in our mission and financially support our public interest R&D program, and research collaborators that keep us focused on the most pressing challenges and deliver their technical expertise and resources to tackle those challenges. Join us in our mission in the way that fits you and your organization. Together we can change the game on the adversary.



### USE THE WORK

Widespread adoption of the Center's R&D is essential to increasing its impact. Using our work to advance threat-informed defense in your organization goes a long way to changing the game on the adversary. Letting us know how you are using the Center's R&D allows us to continually refine our work to make it easier to adopt and more impactful.

### BECOME A BENEFACTOR

Benefactors are critical to enabling the threat-informed defense global community to advance critical public cybersecurity programs through charitable giving. Benefactors are globally recognized for supporting independent research in the public interest.



GET INVOLVED TODAY

Scan the QR code or visit  
[ctid.mitre.org/get-involved](https://ctid.mitre.org/get-involved) →



## BECOME A CENTER PARTICIPANT—GUIDE THE R&D PROGRAM

As a sophisticated user of ATT&CK, your organization is at the helm of the Center's R&D program. Our Participants are thought leaders and innovators that address hard problems and shape ideas into game-changing solutions. Center Participants fund the Center's R&D program and actively collaborate in the development of all Center R&D understanding that their contributions go a long way to changing the game on the adversary.



### Openness

Members propose ideas



### Flexibility

Members choose projects



### Collaboration

Members share ideas, research, and funding



### Leadership

Members gain invaluable expertise

# OUR WORK

Together with Participant organizations, the Center advances threat-informed defense with open-source software, methodologies, and frameworks. Here you will find a directory of research and development projects released to the global cyber community since the launch of the Center in November of 2019. Together, these projects advance the three core disciplines of threat-informed defense.



## CYBER THREAT INTELLIGENCE

*Increase threat-intel effectiveness and advance knowledge of adversary behaviors.*

- [ATT&CK for Cloud](#)
- [ATT&CK for Containers](#)
- [Attack Flow](#)
- [CTI Blueprints](#)
- [Insider Threat TTP Knowledge Base](#)
- [Threat Report ATT&CK Mapper \(TRAM\)](#)

## TESTING & EVALUATION

*Bring the adversary perspective to test and evaluation to understand defensive posture.*

- [CALDERA Pathfinder](#)
- [Micro Emulation Plans](#)
- [Adversary Emulation Plans for FIN6, menuPass, OceanLotus](#)

## DEFENSIVE MEASURES

*Systematically advance our ability to detect and prevent adversary behaviors.*

- [NIST 800-53 Control Mappings to ATT&CK](#)
- [ATT&CK Integration into VERIS](#)
- [Security Stack Mappings to ATT&CK for AWS, Azure, M365, GCP](#)
- [Defending IaaS with ATT&CK](#)
- [Mapping ATT&CK to CVE for Impact](#)
- [Sensor Mappings to ATT&CK](#)

## FOUNDATION RESOURCES

*Make learning and applying threat-informed defense more efficient.*

- [ATT&CK Powered Suit](#)
- [ATT&CK Sync](#)
- [ATT&CK Workbench](#)
- [Top ATT&CK Techniques](#)



**SEE OUR WORK**

Scan the QR code or visit  
[ctid.mitre.org/projects](https://ctid.mitre.org/projects) →

## ABOUT THE CENTER FOR THREAT-INFORMED DEFENSE

The Center is a non-profit, privately funded research and development organization operated by MITRE. 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 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.

**For more information, contact:**  
[ctid@mitre.org](mailto:ctid@mitre.org)

**MITRE** | Center for Threat  
Informed Defense™

© 2025 THE MITRE CORPORATION. ALL RIGHTS RESERVED. Approved for Public Release; Distribution Unlimited 25-0939