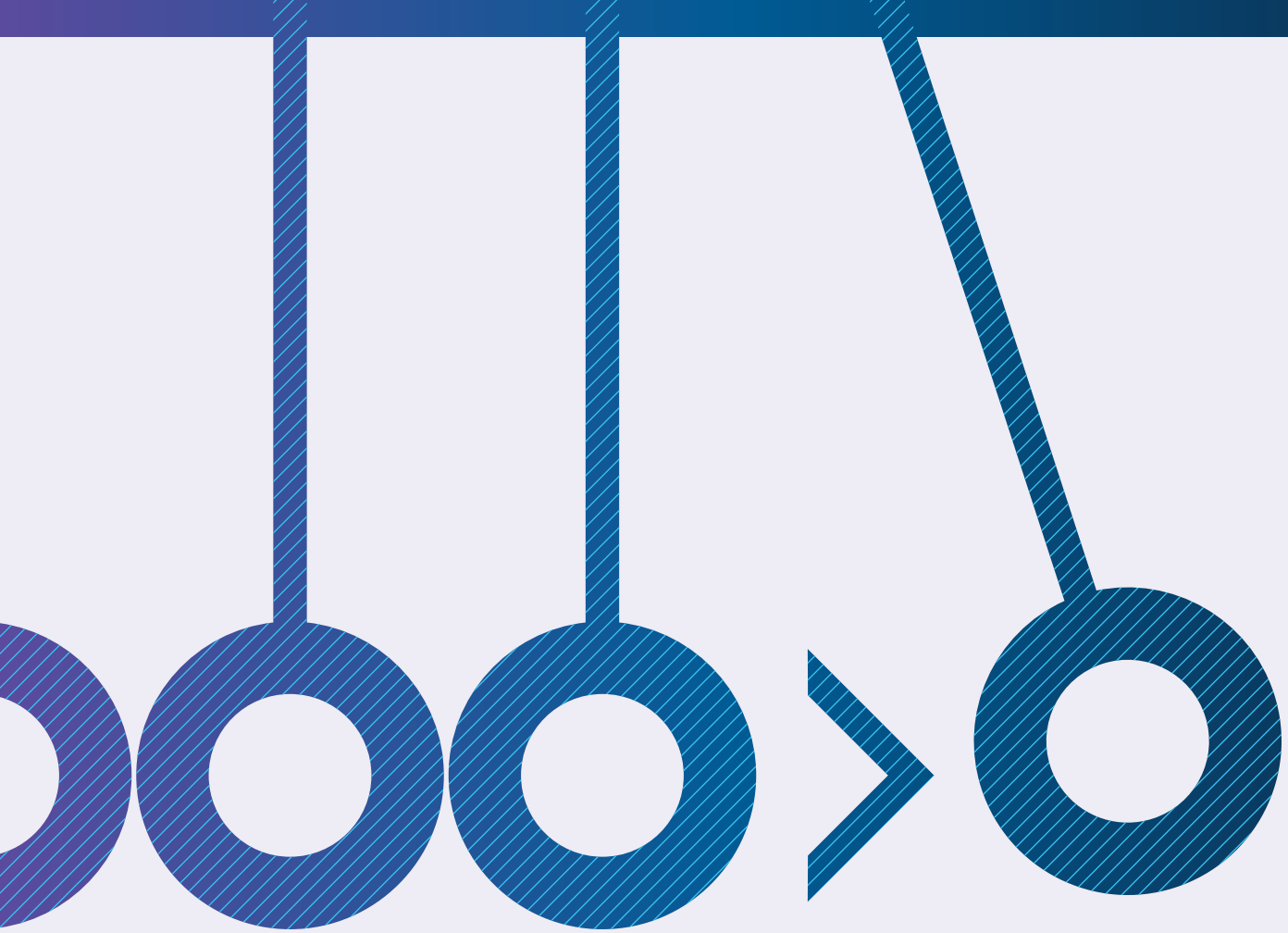


2025 IMPACT REPORT

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.

Participant organizations power the MITRE 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.

Participants ensure that our work is made openly available to defenders around the globe. 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

JPMorganChase
FOUNDER

LLOYDS

Microsoft
FOUNDER

verizon business

RESEARCH SPONSORS

ABBOTT

Booz | Allen | Hamilton®

FOUNDER

ENSIGN INFOSECURITY

FUJITSU

FOUNDER

HIDDENLAYER

Infineon

intel

MARSH

nab

SIEMENS

FOUNDER

sopra steria

standard chartered

NON-PROFIT PARTICIPANTS

AVIATION ISAC

CIS Center for Internet Security®

CSA cloud security alliance®

CYBER THREAT ALLIANCE

FOUNDER

FIRST 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

Without question 2025 was a pivotal year for all of us: our members, the broader threat-informed defense community, and for the MITRE Center for Threat-Informed Defense (CTID). As I look back, I am struck by the way our members consistently show up for one another and for CTID's mission. I am filled with gratitude for the incredible community that makes CTID what it is, and I'm honored and excited to step into the role of CTID Director, partnering with each of you as we shape our future and chart a new course into 2026.

OUR IMPACT

Last year, the Center delivered meaningful impact for defenders worldwide. We launched our largest CTID project in history—the **Secure AI** initiative—uniting 17 members, including all 10 Research Partners, to help define the future of trustworthy AI in cybersecurity. We also expanded our collaboration network with a new effort applying threat-informed defense to combat **financial fraud**. Interest in this project attracted two new members and sparked broad curiosity among cyber defenders seeking to better protect both banks and their customers.

CTID's impact reached five continents in 2025. In Australia, our ATT&CK mappings and Top ATT&CK Techniques grew into local MITRE project extensions for an Australian government sponsor helping prioritize critical ATT&CK techniques and mapping them to Australia's Information Security Manual (ISM). In Singapore and Brussels, threat-informed defenders from around the world gathered for the ATT&CK Community Workshops to share their knowledge and coalesce around a single mission that motives us all: changing the game on the adversary.

OUR COMMUNITY

We were thrilled to welcome three new organizations to CTID within the last year. **Abbott Laboratories** brings a fresh perspective from healthcare technology, strengthening our focus on critical sectors. **Marsh Risk**, our first member from the insurance and risk management community, introduces new dimensions of risk insight and industry collaboration. And **Aviation ISAC**, joining as our newest non-profit participant, represents a global network across airlines, airports, and aviation service providers advancing cyber resilience worldwide.

OUR FUTURE

2026 will be a year of renewed energy and focus for our R&D program. Our **2026 Roadmap** outlines a clear approach to helping defenders across six lines of effort. CTID's work this year will center on turning adversary playbooks into practical defenses at scale, with work spanning robust detection engineering, insider threat, security-control mappings, program level maturity (INFORM), fighting fraud, renewed ATT&CK technique prioritization (TAT2), advanced Attack Flow and TIE analytics, and integrated AI security across projects.

Threat-informed defense will always be a team sport. Your feedback on our research, on how you use CTID resources, and the value of our trainings, workshops, and other engagements is essential to our progress. With your partnership we can continue to refine our work and maximize its impact for defenders everywhere.

Leslie Z. Anderson
Chief Cyber Strategist & Head of Threat-Informed Defense Programs

OUR IMPACT

From Launch to Legacy

1 Mission

Changing the Game on the Adversary

1,100+ Researchers

from 38 countries across 5 continents

50+ Organizations

members and data contributors

Working hand-in-hand to curate, build, test, and release 52 R&D projects in just 6 years in pursuit of advancing the state of the art and the state of the practice in threat-informed defense.


MITRE
REMOVE AMBIGUITY
CWES
MITRE
Center for Threat Informed Defense™
ATT&CK SYNC
COMPARE VERSIONS

MEMBER PERSPECTIVES

"The work CTID does to advance the state of cyber security is directly aligned to our own threat-led strategy and we think it's **critical to our industry.**"

"It's rare that within cybersecurity we are able to place a dollar value on our work to demonstrate impact. But the reporting that the Center provides allows us to **demonstrate ROI** for the work we support in the Center and the benefit of a much larger pool of resources and body of work."

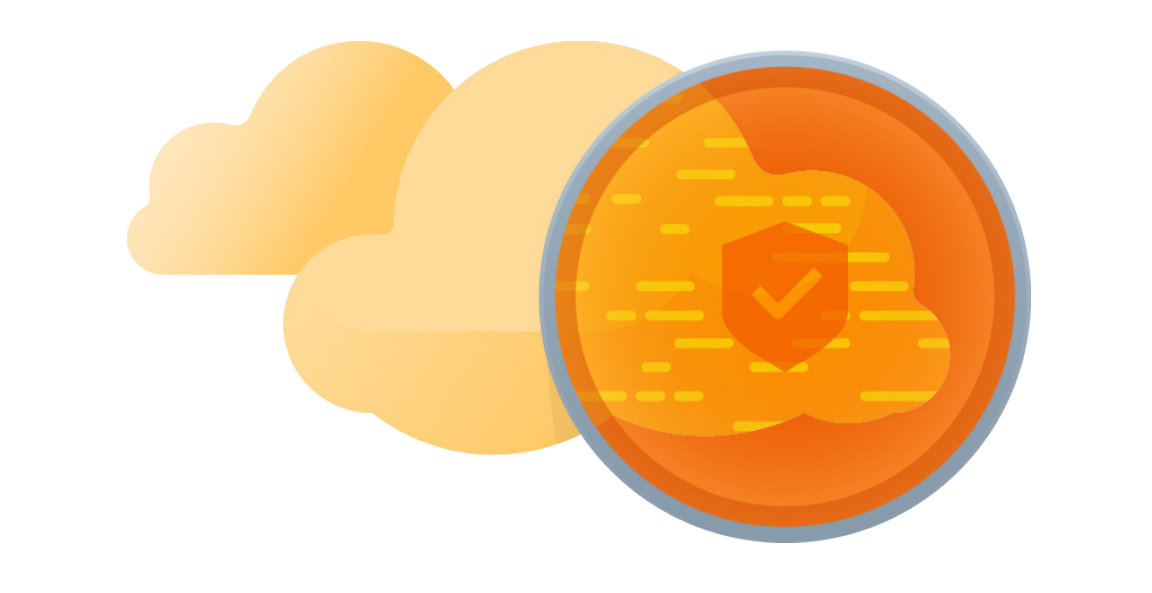
"Through our work on CTID projects, we were able to develop a customer solution that provides organizations with a **robust defense** against insider threats faster and more efficiently than we could have on our own."

"MITRE CTID is helping deliver something we have lacked for years ... **visibility**. Looking forward to driving more new directions."

"**Impressive!** When we joined our first research project we didn't know what to expect. The level of knowledge and expertise from the MITRE CTID 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**."

"The CTID's work showcases the power of a unified approach, where red teams, researchers, and defenders work together to **accelerate innovation** and operationalize security at scale."

"What an honor to be part of this **groundbreaking community**, contributing research and real-world testing strategies that help push threat-informed defense from concept to standard practice."



PUBLISHED JANUARY 2026

THREAT-INFORMED DEFENSE FOR CLOUD SECURITY →

Use our latest mappings to replace assumption-driven cloud defense with evidence-based decisions to stop cloud adversaries in their tracks. With this latest research, you will turn cloud security from a checklist exercise into a threat-informed discipline grounded in real attacks.

PROJECT SPONSORS

citi CROWDSTRIKE FORTINET JPMorganChase

NON-PROFIT PARTICIPANT:

CSA cloud security alliance®

Problem

Threats to cloud computing span multiple security domains, objectives, and layers of cloud technology, making it difficult for organizations to implement effective security controls.

Solution

Establish a threat-informed technical foundation that connects cloud-native security capabilities to the adversary behaviors they are designed to mitigate.

Impact

Defenders apply threat-based approaches to cloud security, control implementation, and security assessments, making defensible decisions grounded in real-world attacks.

> **CTID's mapping of the Cloud Security Alliance's CCM v4.1 to ATT&CK has taken our cloud security strategy to an entirely new level. We've effectively multiplied the power of our existing capabilities by empowering our team to make decisions backed by observed attack behavior. It's a must-have resource for organizations looking to dramatically strengthen their cloud defenses.**
>
> **Heath Montembeault**
> VP, Intelligence Operations—Global Head of Applied Cyber Threat Research, JPMorganChase

PUBLISHED JANUARY 2026

INFORM YOUR DEFENSE →

MITRE INFORM is a program-level assessment designed to show how threat-informed your organization is and where to improve next across cyber threat intelligence, defensive measures, and test and evaluation. Turn insight into action and see your threat-informed posture at a glance and know exactly where to invest next.

PROJECT SPONSORS

ATTACKIQ FORTINET HCA Healthcare infineon LLOYDS

Problem

Teams need a clear, evidence-based way to measure and improve threat-informed defense across their security program.

Solution

MITRE INFORM defines weighted dimensions, components, and maturity levels, paired with an easy-to-use assessment that ties adversary evidence to program-level decisions.

Impact

Organizations can quantify their threat-informed posture, share results across teams, and prioritize high-impact improvements, raising the standard for the security program.

> **“I just completed the INFORM assessment for our organization, and the results provide data-driven insights that further help me focus efforts on the resources that are truly needed.”**

INFORM Your Defense User
Brazil, South America

PUBLISHED JULY 2025

ATTACK FLOW V3 →

This release improves how you build, share, and present flows; it also offers new visualization tools that save time and generate insights. This update includes highly requested features, an improved look-and-feel, and expanded training and documentation.

PROJECT SPONSORS

ATTACKIQ citi FORTINET HCA Healthcare

JPMorganChase nab

NON-PROFIT PARTICIPANT: CYBER THREAT ALLIANCE

Problem

Tracking adversary behaviors one action at a time makes it hard to build effective defenses against multi-phased attacks.

Solution

Create a language, and associated tooling, to describe flows of ATT&CK techniques and combine those flows into patterns of behavior.

Impact

Visualize and communicate how adversaries operate to define defensive actions.

> **HCA Healthcare's third-party pentesters and internal audit were highly impressed by our use of ATT&CK Flow v3 to document our observations of their campaign as well as the visualizations summarizing the techniques we observed. This project makes it easier than ever to quickly document chains of actions and choke points in adversary activities and show that information in easily consumed visualizations for different stakeholders."**
>
> **David Vasil**
> Security Threat Architect, HCA Healthcare

PUBLISHED JUNE 2025

THREAT-INFORMED DEFENSE FOR THE FINANCIAL SECTOR →

Connect adversarial threat mitigations to cybersecurity program resources tailored to the financial sector, namely the Cyber Risk Institute Profile.

PROJECT SPONSORS

citi JPMorganChase

NON-PROFIT PARTICIPANT: FS-ISAC

Problem

The financial services sector faces a complex cybersecurity threat environment and high regulatory standards for cybersecurity program compliance.

Solution

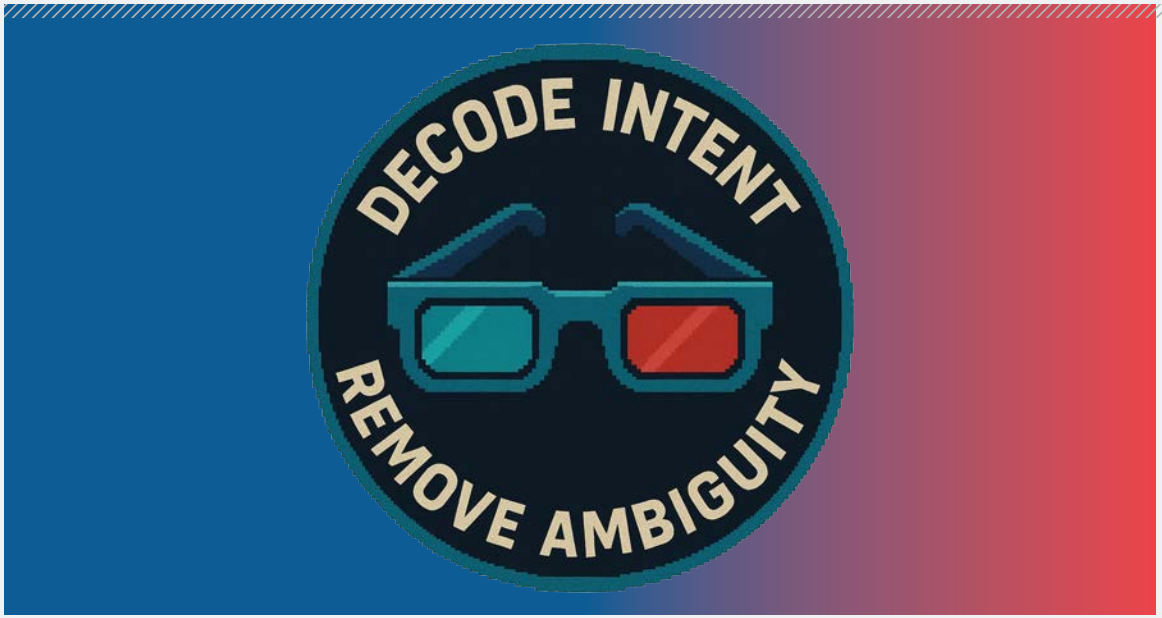
Connect adversarial threat mitigations to cybersecurity program resources tailored to the Cyber Risk Institute Profile.

Impact

Threat-informed defenders in the financial sector have resources aligned with mitigations to support analysis and decision-making as part of a complete cybersecurity program.

> **"Now, financial services firms of all sizes will be able to tie security controls linked to compliance requirements to cyber threats. Threat to control to compliance and reporting just became a whole lot easier!"**

Joshua Magri
President & CEO, Cyber Risk Institute



PUBLISHED MAY 2025

AMBIGUOUS TECHNIQUES V1.0 →

Building upon the research of Summiting the Pyramid, Ambiguous Techniques is a methodology to determine malicious intent behind seemingly benign behavior by applying contextual analysis to ATT&CK techniques. Reduce false positives and uncover adversarial use of living-off-the-land activity.

PROJECT SPONSORS

citi CROWDSTRIKE FORTINET FUJITSU HCA Healthcare LLOYDS Microsoft

Problem

Many ATT&CK techniques, especially those used in living-off-the-land activity, produce observables that are indistinguishable from benign behavior, making it difficult for defenders to determine malicious intent and resulting in unreliable or overly noisy detections.

Solution

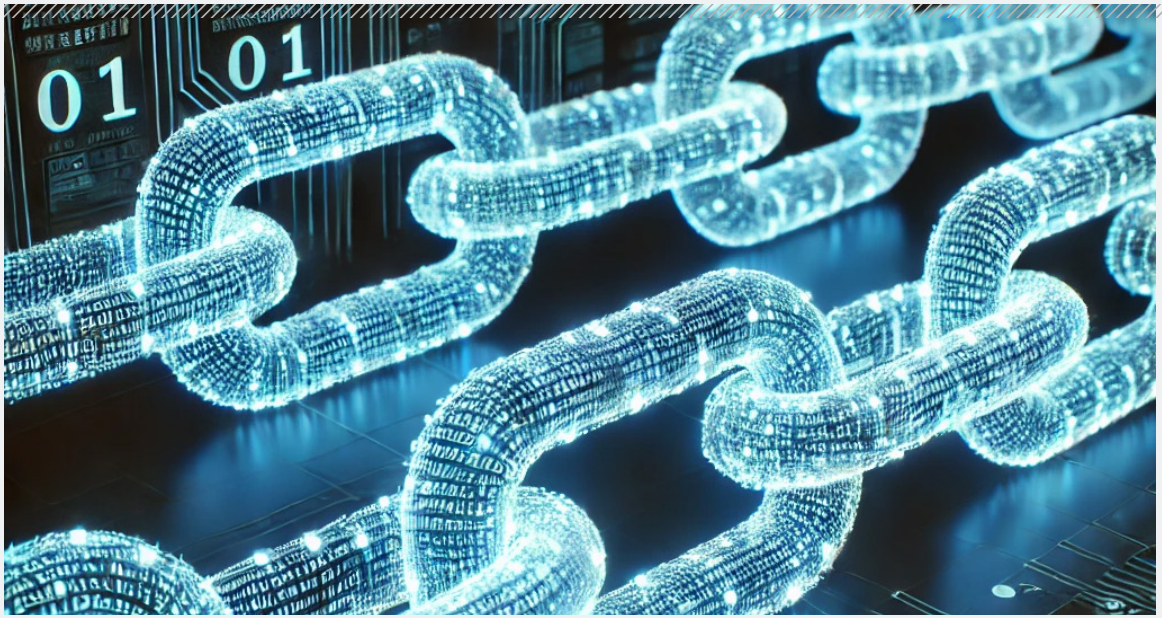
Create a methodology that uses the surrounding context of a detection event to infer the intent of the actor, thus removing the ambiguity.

Impact

Reduce false positives and improve detection accuracy so defenders can prioritize the alerts that truly matter.

> **Ambiguous Techniques exposes a critical reality: modern adversaries deliberately operate in the gray space between benign behavior and malicious action. This growing ambiguity reflects attackers operating with Agentic AI and highly adaptable frameworks— learning, iterating, and reshaping their tradecraft in response to defenses. As a result, advanced analysis of ATT&CK patterns isn't a research luxury anymore; it's an operational necessity."**

Douglas Jose Pereira dos Santos
Director, Advanced Threat Intelligence, Fortinet



PUBLISHED FEBRUARY 2025

PRIORITIZE KNOWN EXPLOITED VULNERABILITIES →

Prioritize Known Exploited Vulnerabilities shows defenders how to take a threat informed approach to vulnerability management.

PROJECT SPONSORS

ATTACKIQ citi HCA Healthcare JPMorganChase Microsoft

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 vulnerabilities.

Solution

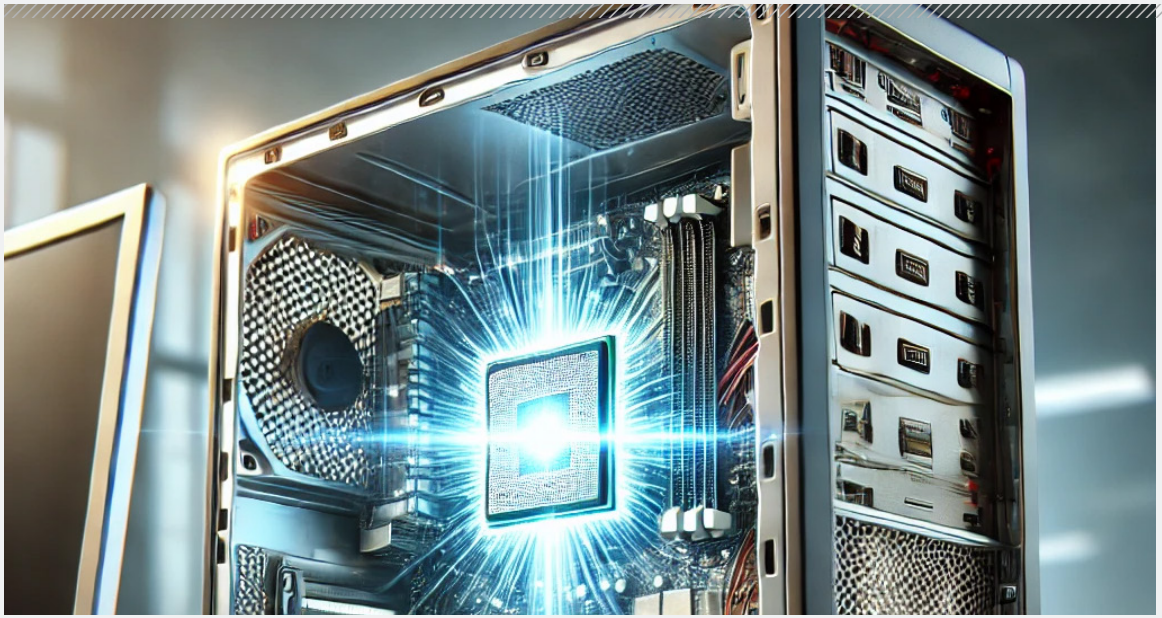
Use the adversary behaviors described in ATT&CK to characterize the impact of a vulnerability. Then, apply that methodology to provide critically needed context to known exploited vulnerabilities.

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 risk posed by specific vulnerabilities in their environment.

> **“The future of defense lies in prioritizing the right vulnerabilities. By connecting adversary behavior to vulnerability, defenders move beyond managing lists of vulnerabilities to reducing real adversary exposure.”**

Jon Baker
VP Threat-Informed Defense, AttackIQ



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.

PROJECT SPONSORS

ATTACKIQ CROWDSTRIKE intel Microsoft

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.

> **"This project brought together industry partners for the first time to map real-world adversary techniques to hardware-enabled security capabilities. By combining expertise across hardware, firmware, operating systems, and security software, the project established a structured, MITRE ATT&CK aligned approach to defending against real world attacks. This collaboration provides the broader industry with a clearer, evidence-based view of how layered security capabilities in widely deployed platforms can be applied to specific threat behaviors."**
>
> **Sanjay Nair**
> Principal Software Engineering Manager, Microsoft Windows

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

JOSEPH OPACKI
Senior Vice President, InfoSec Executive
Bank of America
Founding Research Partner

JOEL SPURLOCK
Vice President Data Science
CrowdStrike
Research Partner

GARRETTSON 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

HEATH MONTEMBEAULT

Global Head of Applied Cyber
Threat Research
JPMorganChase
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

BRIONY SHIPMAN

Head of Cyber Defence
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

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 ultimately 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. Be the first to know about R&D project releases when you sign up to **Stay Informed**.

BECOME A CONTRIBUTOR

Individual contributors play a significant role improving our R&D, providing foundational data to enable research, and scaling the impact of our work. Explore and comment on projects at our **open source repository** on GitHub.

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: Contribute 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 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.

RESEARCH PARTNER

As top-tier participants, Research Partners guide the future direction of threat-informed defense with significant engagement across the Center's research program. Your organization takes a hands-on approach to changing the game on the adversary as a strategic advisor and thought leader.

RESEARCH SPONSOR

Research Sponsors substantially contribute to improving the state of the art and the state of the practice in threat-informed defense. Your organization will contribute expertise, staff, and resources to advance the Center's research program in the public interest and grow with the combined experience of all members.

NON-PROFIT PARTICIPANT

Non-Profit Participants work hand-in-hand with the Center to advocate for the cyber defender and expand our reach. These organizations are often focal points bringing community perspective and influence to accelerate the adoption of threat-informed defense. This unique membership is available by invitation only.

Openness
Members propose ideas

Flexibility
Members choose projects

Collaboration
Members share ideas, research, and funding

Leadership
Members gain invaluable expertise

2026 R&D ROAD MAP

A threat-informed community is essential for effective cyber defense. In 2026, we will focus our R&D program on a clear set of outcomes that help defenders operationalize adversary behavior at scale. Our 2026 roadmap centers on six lines of effort:

Summiting the Pyramid: Increase detection robustness by advancing methodologies, scoring, and telemetry analysis that raise adversary costs and make evasion measurably harder.

Insider Threat: Apply Ambiguous Techniques methods to insider TTPs so programs can distinguish benign from malicious use of common behaviors.

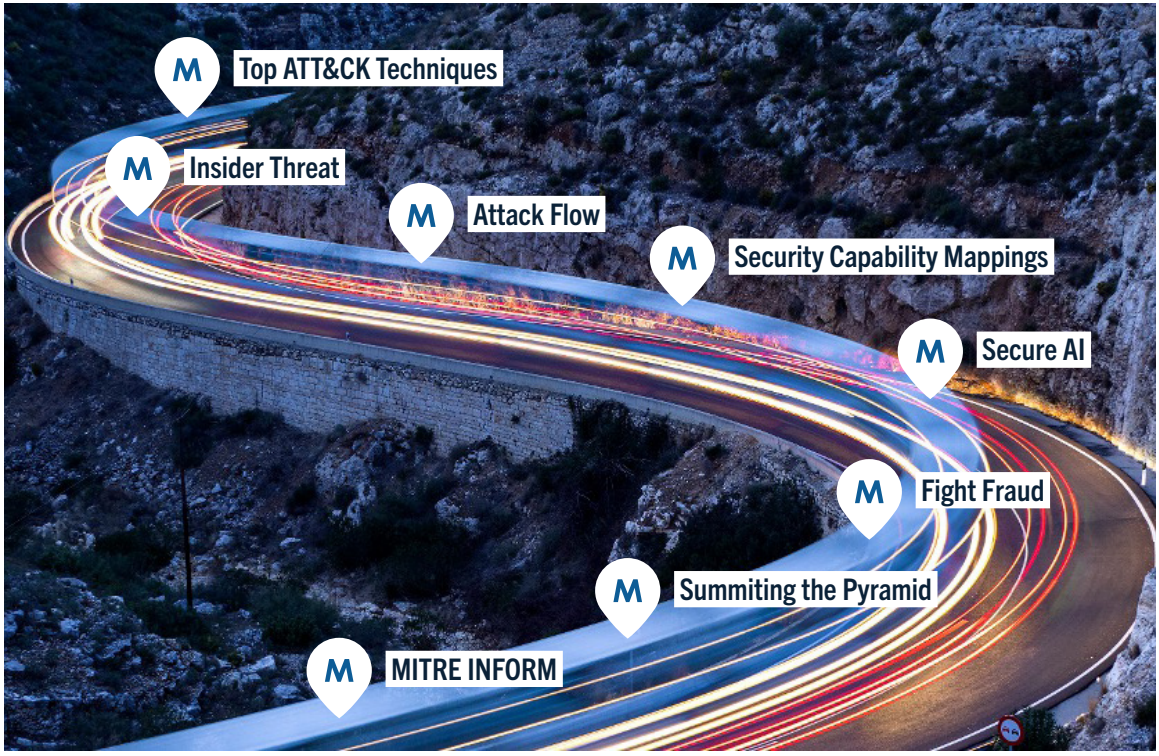
Security Capability Mappings: Expand and modernize mappings between ATT&CK and leading control frameworks, using AI-enabled processes to keep mappings current with ATT&CK and evolving vendor capabilities.

Program Maturity (INFORM): Provide a strategic model to measure and mature threat-informed defense across the entire security program, complementing tactical capability maturity models.

Fight Fraud: Extend the Fight Fraud Framework™ with additional techniques, datasets, and mitigations, connecting cyber detections with material fraud events in more sectors.

Attack Flow and AI Security: Evolve Attack Flow, Technique Inference Engine, and ATLAS to cover more domains and AI-enabled systems, integrating ML and automation to speed emulation design defenses.

This roadmap is designed to guide defenders toward capabilities to adopt, integrate, and scale—so organizations can start quickly, then continuously get better at threat-informed defense.



GET INVOLVED

Scan the QR code or visit
ctid.mitre.org/get-involved →

OUR WORK

Below is 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.

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.

- **ATT&CK Integration into VERIS**
- **CWE with Environmental CVSS Calculator**
- Security Stack Mappings to ATT&CK for **AWS**, **Azure**, **M365**, **GCP**
- **Defending IaaS with ATT&CK**
- **Defending OT with ATT&CK**
- **Mapping ATT&CK to CVE for Impact**
- **NIST 800-53 Control Mappings to ATT&CK**
- **Summiting the Pyramid**
- **Sensor Mappings to ATT&CK**
- **Threat Modeling with ATT&CK**

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**
- **Secure AI**
- **Technique Inference Engine (TIE)**
- **Threat Report ATT&CK Mapper (TRAM)**

FOUNDATION RESOURCES

Make learning and applying threat-informed defense more efficient.

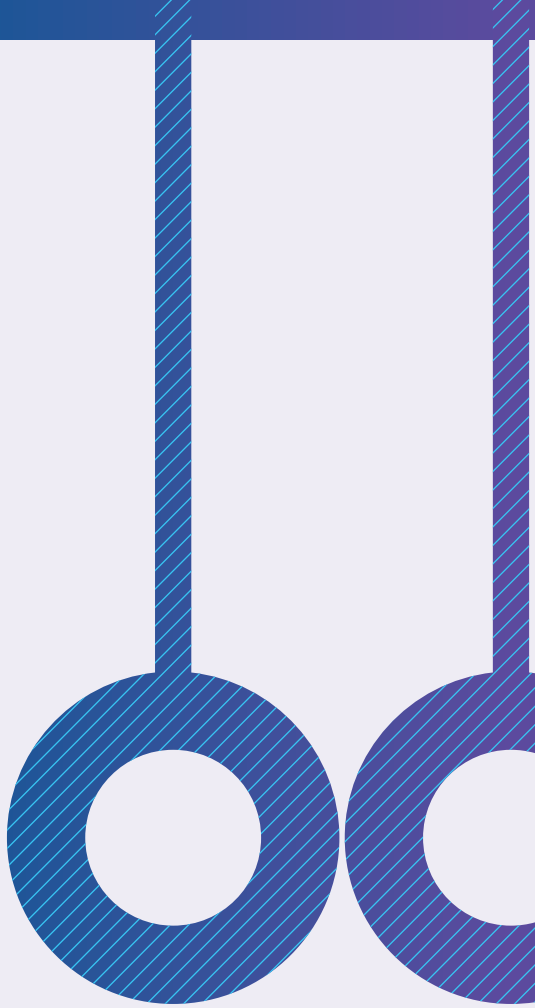
- **ATT&CK Powered Suit**
- **ATT&CK Sync**
- **ATT&CK Workbench**
- **Mappings Explorer**
- **Measure, Mature, and Maximize Threat-Informed Defense (M3TID)**
- **Top ATT&CK Techniques**


SEE OUR WORK
Scan the QR code or visit
ctid.mitre.org/projects

ABOUT THE CENTER FOR THREAT-INFORMED DEFENSE

The Center is a non-profit research and development consortium 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



MITRE | Center for Threat Informed Defense™