

2023IMPACTREPORT



Center for Threat Informed Defense

The Center for Threat-Informed Defense brings together highly sophisticated cybersecurity teams from around the world to advance threat-informed defense for all. Taking a threat-informed approach to cyber defense allows cybersecurity teams to focus on the most critical threats to their organizations and align capabilities to successfully mitigate, detect, and respond to those threats. Center Participants bring their insight, expertise, and support to all aspects of the Center's R&D program and demonstrate their commitment to the public good by ensuring that Center R&D is made freely available to all. Together, our members are a powerful force in changing the game on the adversary.

This annual report features the work of 37 sophisticated cybersecurity teams working in partnership to advance 29 open-source projects that improve cyber defense for the whole community. This report captures the energy and passion that Center Participants bring to advancing threat-informed defense for all. Use it as a reference and share it with your teams and colleagues to further change the game on the adversary.

RESEARCH PARTNERS

ATTACK IQ®
FOUNDER

BANK OF AMERICA 
FOUNDER


FOUNDER


CROWDSTRIKE

FORTINET®

HCA 
Healthcare™
FOUNDER

 IBM Security

JPMORGAN CHASE & CO.
FOUNDER



 Microsoft
FOUNDER

verizon✓

RESEARCH SPONSORS

ANOMALI

BAE SYSTEMS

Booz | Allen | Hamilton®

FOUNDER

ENSIGN
INFOSECURITY

FIS

FM Global

FUJITSU
FOUNDER

Google Cloud

Infineon

intel

nab

next
www.nextdlp.com

SAFE

SIEMENS
FOUNDER

standard
chartered

tenable

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

GLOBAL
RESILIENCE
FEDERATION

Health-ISAC™
Collaborating for Resilience in Healthcare

NRF® NATIONAL
RETAIL
FEDERATION®

RETAIL & HOSPITALITY
ISAC

PERSPECTIVES FROM OUR MEMBERS

ATTACKIQ

Founding Research Partner

“Organizations continue to deal with an ever-escalating frequency and severity of cyber-attacks. It is imperative that more security teams adopt a threat-informed defense mindset to better manage the increase in operational tempo and achieve better security outcomes. AttackIQ is a proud founding member of the Center, demonstrating our commitment to advance this important work for all.”

—**Carl Wright**, Chief Commercial Officer

BOOZ ALLEN HAMILTON

Founding Research Sponsor

“Our national preparedness hinges on continuous collaboration and strategic partnerships. The Center plays a pivotal role in advancing our capacity to proactively thwart threats, address meaningful vulnerabilities, and safeguard our critical infrastructure. As a Founding Research Sponsor, Booz Allen is steadfast in our commitment to actively engage in the Center’s innovative research ecosystem.”

—**David Forbes**, Director of Cyber Physical Defense

CROWDSTRIKE

Research Partner

“At CrowdStrike, we are committed to helping organizations solve real-world problems and to improve their security posture. Through our partnership with the Center, we sponsor projects and lend our expertise to advance the industry’s understanding of adversaries and help defenders to build an effective cybersecurity strategy for their enterprise.”

—**Joel Spurlock**, VP Data Science

CYBER THREAT ALLIANCE

Founding Non-Profit Participant

“The Center has provided key capabilities to the cybersecurity community such as Attack Flow or CTI Blueprints. These tools are a force multiplier for defenders, enabling a better understanding of adversary activities and proactive defense. As cyber threats continue to evolve, the need for the Center’s research has never been greater.”

—**Michael Daniel**, President & Chief Executive Officer

FORTINET

Research Partner

“Fortinet has a long history of collaborating with global experts, pursuing a common goal of making our digital world more secure. We believe our work with the Center’s research program drives projects that will have a meaningful and positive impact on the abilities of cyber defenders worldwide to continue to detect and mitigate the latest attack vectors.”

—**Derek Manky**, Chief Security Strategist and Global Vice President of Threat Intelligence at FortiGuard Labs

FUJITSU

Founding Research Sponsor

“We highly value the Center as a collaborative space where interaction with industry leaders and MITRE experts takes place. Engaging in projects that are both exciting and impactful within this dynamic environment is something we take great pleasure in.”

—**Ryusuke Masuoka**, Technical Advisor

HCA HEALTHCARE

Founding Research Partner

“The Center has provided us with a valuable lens into the tactics and strategies of cyber threat actors. By embracing threat-informed defense principles and collaborating with industry experts, we are able to develop practical methodologies that enable the industry and our organization to implement near predictive cybersecurity measures and optimize intelligence capabilities.”

—**TJ Bean**, Chief Information Security Officer

LLOYDS BANKING GROUP

Research Partner

“Lloyds is proud to work with MITRE on some of the key security challenges of today. We believe the Center’s ability to break down barriers between organizations and work collectively to develop cutting-edge solutions and strategies offers a unique opportunity to contribute and benefit from advancing the state of the art. We have seen the benefits that result from this approach, and we are excited to continue as a Research Partner.”

—**Derek Whigham**, Chief Product Owner, Chief Security Office

SIEMENS AG

Founding Research Sponsor

“The Center does an excellent job in helping organizations turn threat-informed defense from a slogan into an actionable cybersecurity strategy. We appreciate the Center’s efforts with supporting organizations to leverage MITRE ATT&CK in an ideal way, mapping ATT&CK to other relevant security frameworks and sharing its experiences and knowhow with the community.”

—**Michael Pascher**, Senior Key Expert, Cybersecurity

VERIZON

Research Partner

“We at Verizon have always been interested in empowering folks and to provide them with the frameworks and tools so they can guide themselves. This work is never easy, but through our partnership with the Center, the work becomes easier. We can flip the coin from technical to strategic and tackle new challenges.”

—**Alex Pinto**, Associate Director, Security Research - DBIR, Verizon Business

Contents

Letter from the Director 6

Sensor Mappings to ATT&CK 8

OceanLotus Adversary Emulation Plan 10

Summitting the Pyramid 12

Threat Report ATT&CK Mapper (TRAM) 14

ATT&CK Workbench II..... 16

CTI Blueprints..... 18

ATT&CK Integration into VERIS..... 20

Adversary Emulation Library..... 22

Attack Flow 2.1 22

Sync Up With ATT&CK Sync 23

Celebrating the Contributor Community 24

Benefactors Advance Critical R&D..... 25

Advisory Council..... 26

How To Get Involved 28

Our Work 30



Center for Threat-Informed
Defense wins 2023 Global Infosec
Cybersecurity Research Award

LETTER FROM THE DIRECTOR

In reflecting upon the growth and successes of the Center throughout 2023, I am reminded of how the Center has evolved and in awe of the shape it has taken. Launching four years ago with 13 Founders, Center membership has nearly tripled to 37 Research Participants. Our members put aside competitive interests and bring their unique, global, cross-sector perspectives together for the purpose of collaborating with one another to turn out nearly 30 research and development projects for the benefit of the entire global cybersecurity community. Truly a remarkable evolution of growth and impact.

Then, I am reminded of the people who have invited us to talk to their organizations or speak at their conferences about our work. I think about the people we’ve met at conferences, interacted with on social media, and heard from by email or our web site who are eager to connect with the Center. Some want to connect to contribute data to a project. Others want to connect to gather insight on a project they hope to use. Others want to receive project releases and Center news. And many want to know how they can

join or otherwise get involved with the Center. Regardless of how, the reason they want to connect is the same ... to join the Center for Threat-Informed Defense community and advance threat-informed defense.

And so, it makes sense to me that we should continue to cultivate this organically developed community. The Center has supported the EU ATT&CK Community Workshop in Belgium for several years, and we will continue to do so in 2024 and beyond. We are also pleased to launch an Asia-Pacific (APAC) ATT&CK Community Workshop in Singapore in 2024. In the spirit of the EU ATT&CK Community Workshop, we will unite defenders in the region to share, learn, and advance threat-informed defense together. The enthusiasm from Center members and friends in the region offering their support is a sure sign that the APAC workshop is destined for success.

In 2023, we were afforded more opportunities to expand the reach of our work than we could possibly accept having presented the Center's research to nearly two dozen audiences around the globe. In March, the Center launched its Advisory Council of senior level executives to provide strategic guidance and

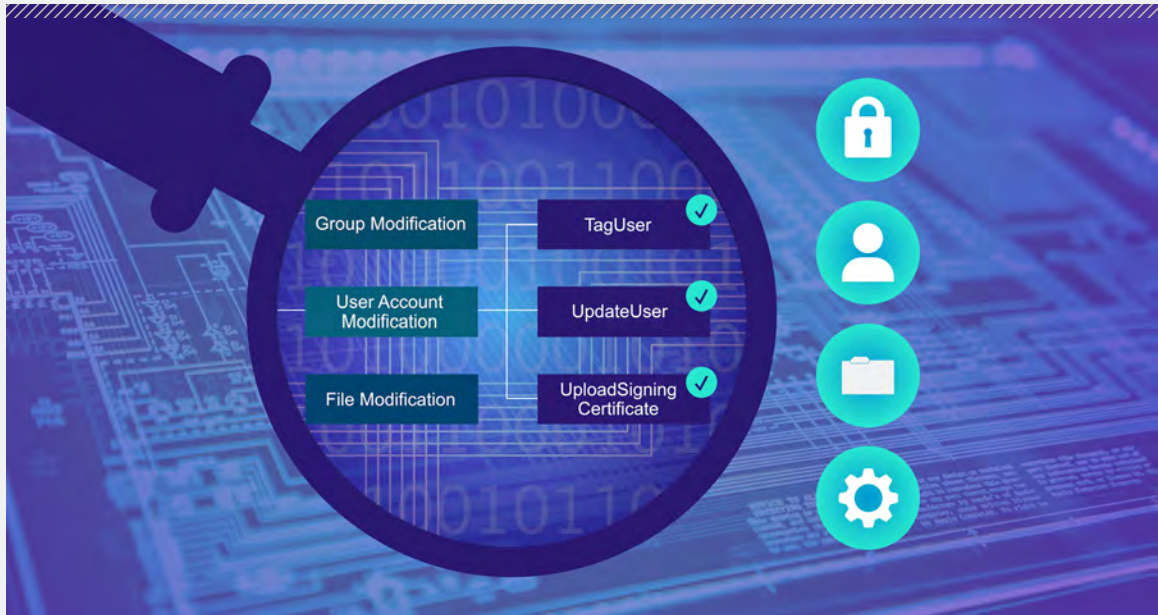
executive advocacy in support of the Center's mission. Also launched in March, the Center's Benefactor Program gives organizations the opportunity to support MITRE ATT&CK®, Caldera™, MITRE Engage™, and the Center for Threat-Informed Defense through charitable giving. In April, the Center accepted the Cyber Defense Magazine 2023 Global InfoSec Next Gen Award for Cybersecurity Research at the RSA Conference in San Francisco. And, in October the Center reached a social media milestone—10,000 [LinkedIn](#) followers. These are just a few of the many initiatives undertaken this year to further the impact of our work on the global cyber community.

I invite you to explore this 2023 Impact Report with an eye toward community. Consider peers, thought leaders, and innovators in your sphere who would not only benefit from but contribute to the Center for Threat-Informed Defense community and invite them to join us.

Thank you for your continued support,

JONATHAN BAKER
*Director, Center for
Threat-Informed
Defense*





PUBLISHED DECEMBER 2023

SENSOR MAPPINGS TO ATT&CK →

Sensor Mappings to ATT&CK gives cyber defenders the information needed to identify and understand cyber incidents occurring in their environment. Various tools and services are available to collect system or network information, but it is not always clear how to use those tools to provide visibility into specific threats and adversarial behaviors occurring in an environment. These mappings between sensor events and ATT&CK data sources allow cyber defenders to create a more detailed picture of cyber incidents, including the threat actor, technical behavior, telemetry collection, and impact.

PROJECT SPONSORS





Problem

Cyber defenders need to connect which tools, capabilities, and events detect specific adversary behaviors.



Solution

Link adversary behaviors to defenders' tools, capabilities, and sensors through ATT&CK Data Sources.



Impact

Defenders collect and analyze the data necessary to observe adversary behaviors.



The project is key to us as it not only provides mappings for several widely used toolsets, but also establishes a repeatable methodology for performing future mappings. The Center's methodology puts consistency and repeatability at the core of the work, enabling us to use this approach with confidence going forward."

—ALEX WALLACE, Intelligence Technology Lead, Chief Security Office, Lloyds Banking Group

PROJECT SPONSORS



IBM Security

JPMORGAN CHASE & CO.



SIEMENS

verizon✓



PUBLISHED OCTOBER 2023

OCEANLOTUS ADVERSARY EMULATION PLAN →

OceanLotus (aka APT32, SeaLotus, APT-C-00) is a suspected Vietnam-based threat group that has been active since at least 2014. The group has targeted multiple private sector industries as well as foreign governments, dissidents, and journalists. This project adds the first macOS and Linux focused plans to the Adversary Emulation Library for red and blue teams to systematically test their defenses against real-world adversary behaviors.

PROJECT SPONSORS

ATTACKIQ®



FUJITSU





Problem

Threat intel reporting shows that adversaries are increasingly targeting macOS and Linux systems, and there are no public adversary emulation plans for macOS and Linux with an explanation of defenses from the perspective of the adversary.



Solution

We have created an emulation plan for OceanLotus that starts on macOS and ends on a Linux host with explicit defensive telemetry for a full scope purple teaming perspective.



Impact

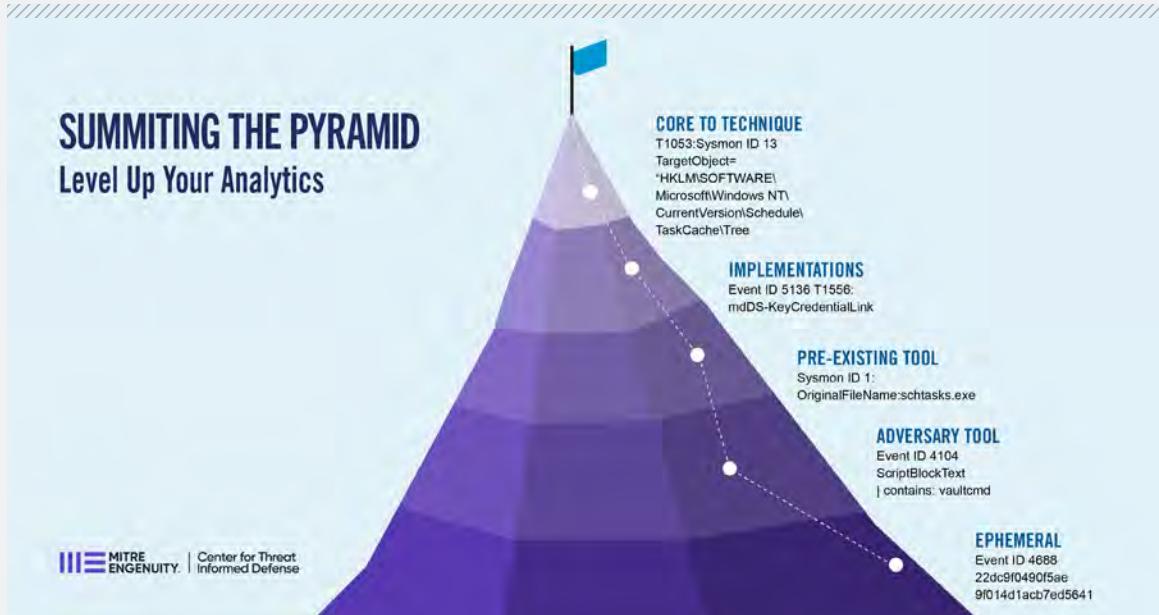
This is the first emulation plan released publicly that enables a purple team operation on macOS and Linux, providing visibility into environments inaccessible with current prior resources.

“Security teams can be more proactive by leveraging Center projects to evaluate organizational cyber readiness. With the OceanLotus emulation plan, the Center produced a resource that allows security teams to better understand their ability to defend against the adversary.”

—CARL WRIGHT, Chief Commercial Officer, AttackIQ

“This emulation project offers a comprehensive exploration of OceanLotus, along with an in-depth understanding of penetration testing techniques applicable to macOS environments.”

—KOTARO OHSUGI, Researcher, Fujitsu



PUBLISHED SEPTEMBER 2023

SUMMITTING THE PYRAMID →

Many analytics are dependent on specific tools or artifacts. Adversaries can easily evade these with low-cost changes that exploit the dependencies. This project developed a method to evaluate analytics relative to the adversary's cost to evade. We further created approaches and tips for defenders to make their analytics less evadable. We demonstrated the methodology with a core set of analytics.

PROJECT SPONSORS





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.



In the ever-evolving field of security, there is a constant need to improve our detection of adversary behavior. The Summiting the Pyramid project is a strategy to enhance detection capabilities by making analytics harder to evade. Microsoft joined this effort with two main objectives. First, we aim to ensure that these analytic improvements fully leverage the OS's instrumentation to produce robust, high-quality detections. Second, we are identifying potential enhancements to our existing events and logging mechanisms. Both goals are geared towards benefiting the security community as a whole and we look forward to our continued collaboration.”

—**GIERAEL ORTEGA**, Security Researcher, Microsoft



PUBLISHED AUGUST 2023

THREAT REPORT ATT&CK MAPPER (TRAM) →

The cybersecurity community has been working for years to automatically identify adversary tactics, techniques, and procedures (TTPs) in cyber threat intelligence (CTI) reports. With advances in machine learning and artificial intelligence, TRAM is a solution that is measurably effective at solving that problem. Previous iterations of TRAM focused on creating a data annotation tool and using supervised learning methods to extract and predict TTPs. Our latest project improves the quality of the training data and makes effective use of fine-tuned Large Language Models (LLMs) for model training and predictions. We have improved the speed and accuracy of TTP mappings to meet defenders’ demands.

PROJECT SPONSORS



JPMORGAN CHASE & CO.





Problem

The cybersecurity community needs to identify which adversary TTPs are found in CTI reports. This task of mapping TTPs is difficult, error-prone, and time-consuming.



Solution

Train a LLM on data for the TRAM tool to automatically find TTPs.



Impact

CTI analysts will automatically, accurately, and efficiently identify ATT&CK TTPs in CTI reports.



Extracting ATT&CK techniques from threat intelligence automatically makes it much easier for organizations to index and get value from the reporting they consume. This is a powerful application of modern Natural Language Processing to solve the human problems of cybersecurity.”

—TED DRIGGS, Principal Project Manager, Crowdstrike



PUBLISHED AUGUST 2023

ATT&CK WORKBENCH II →

The ATT&CK Workbench enables teams to explore, create, annotate, and share extensions of the ATT&CK knowledge base. This work increases the utility of using Workbench as a local knowledge base that can be extended with a team’s new or updated techniques, tactics, mitigations groups, and software.

PROJECT SPONSORS





Problem

Defenders struggle to integrate their organization's local knowledge of adversaries and their behaviors with MITRE ATT&CK.



Solution

Expand and improve the open-source software tool, ATT&CK Workbench, to allow organizations to better manage and extend their own local version of ATT&CK and keep it in sync with the official ATT&CK knowledge base.



Impact

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



What's better than ATT&CK? ATT&CK with your own custom knowledge baked in! Workbench has been key to our ability for extending ATT&CK with our internal knowledge, annotations, and references.

Being able to augment and annotate ATT&CK with our own campaigns, threat actors, notes, and other intelligence has been pivotal in how we leverage the ATT&CK framework.

HCA Healthcare partnered with the Center to tackle this project because we believe being able to extend ATT&CK with our own internal intelligence is the next step in our ATT&CK maturity journey.”

—**DAVID VASIL**, Security Threat Architect, HCA Healthcare



PUBLISHED JUNE 2023

CTI BLUEPRINTS →

CTI Blueprints developed an approach and prototype tool for creating narrative cyber threat intelligence (CTI) reports that analysts need in the form they need them. Reports produced using CTI Blueprints include structured STIX content, are tagged with ATT&CK reference, and enable operational defensive cyber analysis, analytics testing, and adversary emulation. We will establish a new normal for cyber threat intelligence. Producers will create actionable intelligence for their consumers, and consumers will take specific threat-informed action.

PROJECT SPONSORS

ATTACKIQ®

BAE SYSTEMS

citi

CROWDSTRIKE

JPMORGAN CHASE & CO.

SIEMENS

standard
chartered

verizon✓



Problem

Threat intel producers need clear and concrete guidance and tools to create finished intelligence that meet defenders' needs.



Solution

Answer defenders' critical questions through actionable intelligence reports created from expert-developed templates that reflect defenders' use cases.



Impact

Threat intelligence producers create actionable intelligence that their users can operationalize immediately.

“ One of the enduring challenges for threat intelligence is the need to reach different stakeholders with the same intelligence, but they all have different roles, frames of context and needs. CTI Blueprints was an exciting opportunity for us to get involved with the Center as their thinking matched where we saw the natural evolution of threat intelligence heading. We provide threat intelligence reporting to customers and their TI teams across 45 countries in government and commercial spaces, and the more people across the ecosystem we can get using CTI Blueprints, the more the ecosystem as a whole will benefit.”

—**ADRIAN NISH**, Head of Cyber Portfolio, BAE Systems Digital Intelligence



PUBLISHED APRIL 2023

ATT&CK INTEGRATION INTO VERIS →

ATT&CK Integration into VERIS updates and expands the translation layer between VERIS and ATT&CK allowing ATT&CK to describe the adversary behaviors that were observed in an incident coded in VERIS. These connections allow for joint analysis of the information that ATT&CK describes well alongside the incident demographics and metadata that VERIS describes well.

PROJECT SPONSORS





Problem

Users of the VERIS data model lack a well-defined way to link incidents described in VERIS to the underlying adversary tactics, techniques, and procedures (TTPs) used in that incident.



Solution

Build and document a common and open method to link data in 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.

“ In a world where the regulatory pressure of incident reporting is increasing, leveraging reporting taxonomies that are clear and useful for the defenders is the key to maximize the utility of any such program.”

—ALEX PINTO, Associate Director, Security Research—DBIR, Verizon Business

“ The Center’s work on VERIS and the ATT&CK mapping in its second iteration shows continued and great commitment to bringing those two frameworks with similar but different angles together. The Center delivered project management and execution in the expected and usual high-quality way, pivoting from real-world use cases into the mapping topic while also extending the deliverables in the tooling area.”

—THOMAS PENTEKER, Head of Siemens Cert, Siemens AG

ADVERSARY EMULATION LIBRARY →

The Adversary Emulation Library provides a set of common off the shelf emulation plans—Full Emulation Plans and Micro Emulation Plans—that your organization can use to understand how your defenses actually fare against real-world threats.

Emulation plans are an essential component in testing current defenses for organizations that are looking to prioritize their defenses around actual adversary behavior.













Six new Micro Emulation Plans were added to the library in April 2023 bringing the total number of plans in the library to 12: Apache

RCE, Data Exfiltration, DLL Sideload, Log Clearing, Reflective Loading, and User Execution.

ATTACK FLOW 2.1 →

Originally launched in March 2022, Attack Flow moves defenders from tracking individual adversary behaviors to tracking the sequences of behaviors that adversaries use to achieve their goals. By looking at combinations of behaviors, defenders learn the relationships between them: how some techniques set up other techniques, or how adversaries handle uncertainty and recover from failure.

The project supports a wide variety of use cases: from blue team to red team,

Micro Emulation	Full Emulation
Emulate compound behaviors across 2–3 techniques	Emulate adversary operation
 Executable in seconds	 Executable in hours
<i>E.g., Fork & Run Process Injection</i>	<i>E.g., FIN6 adversary emulation plan</i>
 Easy to automate	 Easy to automate
 Validate atomic analytics	 Validate atomic analytics
 Validate chain analytics	 Validate chain analytics
 Evaluate SOC against a specific set of TTPs	 Evaluate SOC against a specific set of TTPs
 Evaluate SOC holistically against specific groups	 Evaluate SOC holistically against specific groups

from manual analysis to autonomous response, and from front-line worker to the C-suite. Attack Flow provides a common language and toolset for describing complex, adversarial behavior.

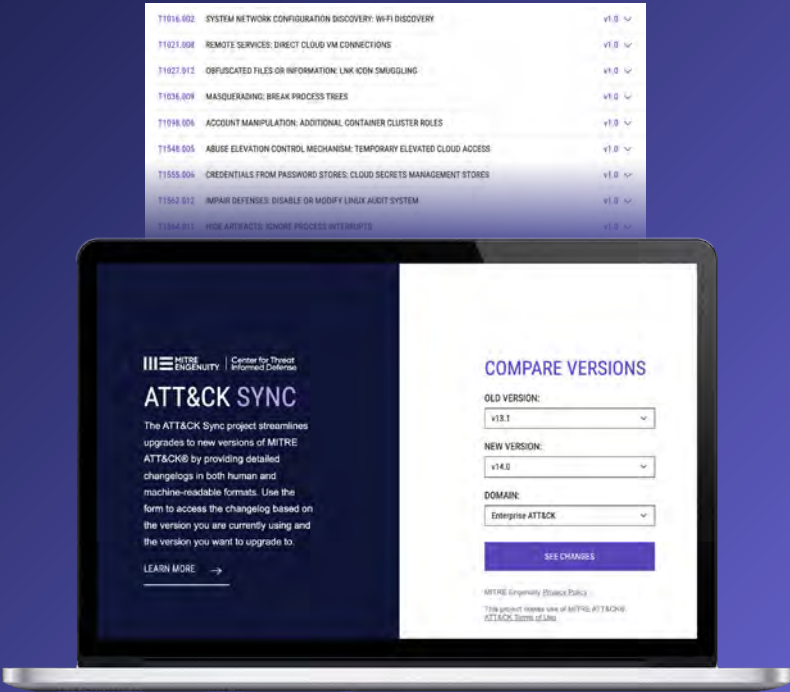
The Attack Flow 2.1 release in August of 2023 enhanced usability and lowered the barrier to entry for defenders looking to change the way they visualize attacks.

SYNC UP WITH ATT&CK SYNC →

ATT&CK Sync streamlines upgrading to new versions of MITRE ATT&CK by providing tools and resources to migrate existing projects to current ATT&CK versions in a timely and efficient manner. The

ATT&CK knowledge base is updated twice per year, and with each new ATT&CK release, these projects fall behind and need updates. ATT&CK Sync was released in the spring to support ATT&CK v13 and updated in the fall following the

release of ATT&CK v14. ATT&CK Sync provides tools and a methodology that organizations can use to implement their own solutions for keeping up with latest version of ATT&CK, saving time and effort for all.



CELEBRATING THE CONTRIBUTOR COMMUNITY

Advancing threat-informed defense globally is only possible with community support and contributions.



STOPPING INSIDER THREATS →

Contributors to the **Insider Threat TTP Knowledge Base** are founders of the community's first cross-sector, multiorganizational, community-sourced body of insider threat data inspired by ATT&CK. With this collection of insider threat TTPs, as a foundation, defenders will detect, mitigate, and emulate insider actions on IT systems.

Thanks to their contributions, we have analyzed over 300 indicators of insiders and have identified 28 unique ATT&CK techniques and 16 different log types that can be used to detect insiders.

300+
INDICATORS

28
TECHNIQUES

16
LOG TYPES

ADVERSARY TRACKING →

The **Sightings Ecosystem** project is a foundational resource that injects real-world data and insights into the decision-making process of defenders that no single organization could build on its own. We salute the data contributors that created a global view of threat activity mapped to ATT&CK.

Thanks to community contributions, we were able to analyze 1.6 million sightings between August 2021 to November 2023, which included 353 unique techniques, and originated from 198 countries.

1.6M
SIGHTINGS

353
TECHNIQUES

198
COUNTRIES

BENEFACTORS ADVANCE CRITICAL R&D

We are grateful to our Benefactors, recognizing their critical role in advancing threat-informed defense through their financial support for public cybersecurity programs such as MITRE ATT&CK®, Caldera™, MITRE Engage™, and the Center for Threat-Informed Defense.

OUR BENEFACTORS



BECOME A BENEFACTOR TO
ADVANCE THREAT-INFORMED
DEFENSE FOR ALL →



ADVISORY COUNCIL

Advisors from each Founding Participant and each Research Partner 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 to the Center bring to bear their skill and experience to guide and advance the Center's mission. 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 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



GARRETTSOON BLIGHT

Managing Director of Global
Cyber (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



SRIDHAR MUPPIDI

IBM Fellow, VP & CTO
IBM Security
Research Partner



KARTHIK SELVARAJ

Partner Director Security
Researcher
Microsoft
Founding Research Partner



SYOICHI KANZAKI

Senior Expert
Fujitsu
Founding Research Sponsor



SHAHAN SUDUSINGHE

Global Head of Cybersecurity
Monitoring and Response
JPMorgan Chase Bank
Founding Research Partner



DR. MARTIN OTTO

Head of Cybersecurity Research
US
Siemens AG
Founding Research Sponsor



TJ BEAN

Chief Information Security
Officer
HCA Healthcare
Founding Research Partner



DEREK WHIGHAM

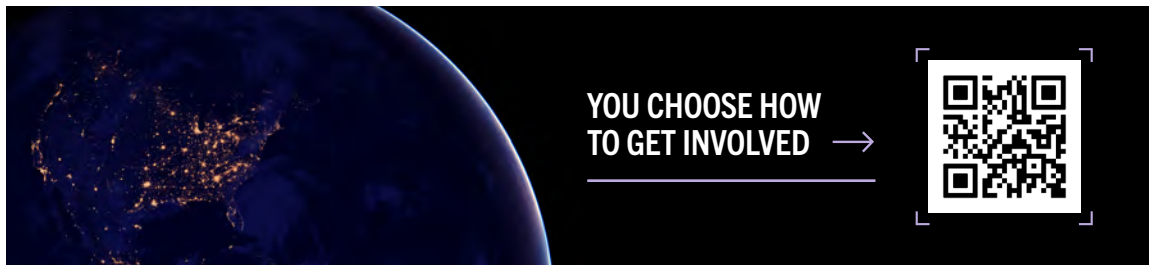
Chief Product Owner, Chief
Security Office
Lloyds Banking Group
Research Partner



ALEX PINTO

Associate Director, Security
Research—DBIR
Verizon Business
Research Partner

HOW TO GET INVOLVED



SUPPORT THE MISSION

The Center’s mission is simple: Advance the state of the art and the state of the practice in threat-informed defense globally. In the Center, sophisticated cybersecurity teams from around the world come together to research and develop solutions to critical challenges. We then make the results of our work freely available.

ADOPT THE FREELY AVAILABLE R&D

Use our work to advance threat-informed defense in your organization. Your application of Center R&D ensures that it is relevant and impactful and takes us closer 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, making it easier to use and more impactful.

BECOME A BENEFACTOR—ADVANCE R&D IN THE PUBLIC INTEREST

Benefactors scale and advance threat-informed defense for all with their charitable giving. Their support sustains critical public cybersecurity programs such as MITRE ATT&CK®, Caldera™, MITRE Engage™, and the Center for Threat-Informed Defense. Benefactors are globally recognized for supporting independent research in the public interest.

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 industry thought leaders and innovators that address hard problems and shape ideas into game-changing solutions in cybersecurity. In addition to paying membership dues, Center Participants fund our R&D program and actively collaborate in the development of all Center R&D understanding that their contributions are changing the game on the adversary.

✓

RESEARCH PARTNER

As top-tier participants, Research Partners contribute significant resources to the Center’s R&D program and, indeed, the future direction of threat-informed defense. Your organization will take a hands-on approach to changing the game on the adversary and improving the state of the art and the state of the practice in threat-informed defense.

✓

RESEARCH SPONSOR

Research Sponsors make up the largest segment of the Center’s membership and are the backbone of our work. Your organization will have the opportunity to contribute expertise, staff, and resources to advance the Center’s research program in the public interest.

✓

NON-PROFIT PARTICIPANT

Non-Profit Participants are the grass roots of the Center working hand-in-hand to advocate for the cyber defender and expand the reach of our work. Non-Profit Participants are a unique level of membership which is available by invitation only.

+



Openness
Members propose ideas



Flexibility
Members choose projects



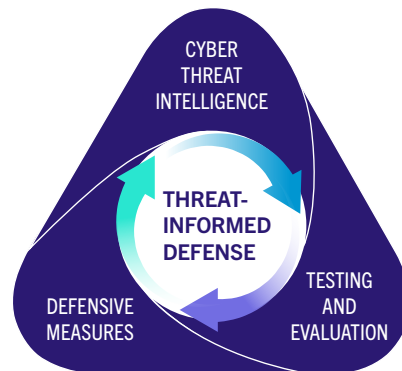
Collaboration
Members share ideas, research, and funding



Leadership
Members gain invaluable expertise

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

- [ATT&CK for Cloud](#)
- [ATT&CK for Containers](#)
- [ATT&CK Workbench](#)
- [ATT&CK Powered Suit](#)
- [Cloud Analytics](#)
- [Threat Report ATT&CK Mapper \(TRAM\)](#)

TESTING & EVALUATION

- [CALDERA Pathfinder](#)
- [FIN6 Adversary Emulation Plan](#)
- [Insider Threat TTP Knowledge Base](#)
- [menuPass Adversary Emulation Plan](#)
- [Micro Emulation Plans](#)
- [Sightings Ecosystem](#)
- [Top ATT&CK Techniques](#)

DEFENSIVE MEASURES

- [ATT&CK Integration into VERIS](#)
- [Attack Flow](#)
- [Atomic Data Sources](#)
- [Defending IaaS with ATT&CK](#)
- [NIST 800-53 Control Mappings](#)
- [Security Stack Mappings—Google Cloud Platform](#)
- [Security Stack Mappings—Amazon Web Services](#)
- [Security Stack Mappings—Azure](#)
- [Mapping ATT&CK to CVE for Impact](#)

OUR WORK →



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.

For more information contact:

ctid@mitre-engenuity.org