2022 IMPACT REPORT

MITRE ENGENUITY™ | Center for Threat Informed Defense

RESEARCH PARTNERS

ATTACKIQ
FOUNDER

BANK OF AMERICA
FOUNDER

citi
FOUNDER

CROWDSTRIKE

FORTINET

HCA Healthcare
FOUNDER

IBM Security

JPMorgan Chase & Co.
FOUNDER

verizon

RESEARCH SPONSORS

ANOMALI

BAE SYSTEMS

Booz | Allen | Hamilton
FOUNDER

FUJITSU
FOUNDER

Google Cloud

LLOYDS BANKING GROUP

Microsoft
FOUNDER

nab

red canary
FOUNDER

SIEMENS
FOUNDER

splunk> turn data into doing.

standard chartered

usbank
FOUNDER

NON-PROFIT PARTICIPANTS

Analysis & Resilience Center FOR SYSTEMIC RISK

CIS. Center for Internet Security

CYBER THREAT ALLIANCE
FOUNDER

FIRST Improving Security Together

FS-ISAC

GLOBAL CYBER ALLIANCE.

NRF NATIONAL RETAIL FEDERATION

RETAIL & HOSPITALITY ISAC

MITRE ENGENUITY

Center for Threat Informed Defense

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

PERSPECTIVES FROM OUR MEMBERS

ANOMALI

“Anomali’s goals center around precision, velocity, and impact of intelligence driven insight, decision making, and execution. The collaboration with the Center innovates and enables all three, joining up the dots and creating clear and efficient pathways to success.”

—**STEVE BENTON**, VP Anomali Threat Research & GM Belfast

ATTACKIQ

“AttackIQ is proud to have been a Center member since the founding days, and it’s been a privilege to see how the Center has evolved in democratizing ATT&CK and providing tools and insights to better assist organizations in interdicting threat actors.”

—**CARL WRIGHT**, Chief Commercial Officer

BAE SYSTEMS

“BAE Systems is proud to sponsor the Center, helping push forward cybersecurity by providing network defenders with new tools to mitigate threats. The program promotes co-operation in the industry through coming together to share problems and ideas for how we can better articulate cyber risks. This means we can innovate with other leaders in the industry to push forward the state of the art. We continue to be astonished at the innovations which attackers come up with in order to breach networks. The Center is a great example of industry collaboration with an innovative response to the threats we face.”

—**DR. ADRIAN NISH**, BAE Systems Digital Intelligence

BANK OF AMERICA

“Bank of America is a proud Founding Research Partner of the Center which enables us to collaborate with global cyber security teams bringing value to our customers, stakeholders and a broader cyber community. Our collective investment in research and development of public interest tools empowers cyber defenders worldwide creating both momentum and learning opportunities.”

—**DAVID HARTE**, Head of Technology Innovation & Shared Platforms

BOOZ ALLEN HAMILTON

“Ensuring cyber superiority will require us to see the cyber threat landscape in the same way our adversaries do. As a Founding Research Sponsor, we engage in R&D with the Center focused on examining adversarial TTPs. This research is a crucial step towards staying ahead of threats, hardening critical systems, and defending what matters most.”

—**GARRETTSON BLIGHT**, Director of National Cyber Solutions

CROWDSTRIKE

“CrowdStrike values research that aims to change the defensive game and recognizes that effective defenses necessitate understanding the threat. We’re proud to partner with the Center to advance research in insider threat, cloud security, IaaS, and other critical areas.”

—**JOEL SPURLOCK**, Senior Director

CYBER THREAT ALLIANCE

“The Center develops practical solutions for hard problems in cybersecurity threat analysis and information sharing. As a result, the Center’s projects directly benefit CTA’s members and ultimately make us more effective at what we do. We appreciate the opportunity to shape and to participate in the Center’s work to make the digital ecosystem safer for everyone.”

—**MICHAEL DANIEL**, President and Chief Executive Officer

FORTINET’S FORTIGUARD LABS

“One of the most powerful things you can do when fighting cybercrime is shift the economics of an attack, and the work we are doing with the Center focused on adversary behavior does just that. Fortinet looks forward to our continued work with the Center on important projects as a Research Partner.”

—**DEREK MANKY**, Chief Security Strategist & VP Global Threat Intelligence

FS-ISAC

“FS-ISAC is proud to partner with the Center; collaborating together on common topics of interest, such as insider threats. By working together and sharing insights, we increase the value of each other’s intelligence.”

—**STEVEN SILBERSTEIN**, CEO

HCA HEALTHCARE

“As a Founding Research Partner, HCA Healthcare has found itself in the unique and thrilling position of having been involved in the impressive growth of the Center over the past three years. Being in the same room with some of the world’s most regarded cyber security teams has been a true learning experience for our researchers and our business.”

—**DAVID VASIL**, Consulting Security Threat Architect

MICROSOFT

“The collaboration and innovative work done at the Center benefits everyone in the security community, not only those who use ATT&CK as part of their products and services, but also Microsoft’s valued ecosystem of partners.”

—**KARTHIK SELVARAJ**, Partner Director, Microsoft Defender Security Research

NATIONAL AUSTRALIA BANK

“Given the threat landscape of the financial services industry here in Australia, joining the Center as a Research Sponsor in 2022 was a top priority for National Australia Bank. We have seen great value in the projects already released by the Center and are excited about the ideas being curated to be come running projects in 2023.”

—**ROB SMITH**, Executive, Cyber Security

STANDARD CHARTERED

“Sharing ideas and problems around understanding the adversary, assessing their capabilities, and applying this to defense efforts has been the greatest benefit for us. The Center’s collaborative approach helps the whole community. Its research can enable understanding and focus across the community.”

—**GRZEGORZ MOLSKI**, Intelligence Enablement Lead Cyber, Threat Intelligence & Countermeasures

SIEMENS AG

“When we joined the Center as a founding member 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. Three 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

VERIZON

“We need a better way to understand what we do, so we can get better at measuring what we do, and someday, hopefully, optimizing what we do. Its possibility of achieving this has never been more clear to me or how in reach this idea is since working in the Center.”

—**ALEX PINTO**, DBIR Team Manager

IBM SECURITY

“As one of the highest priority challenges of our time, cybersecurity is not an area where one should be doing it alone. We hope to level the playing field for cyber defenders by working together with an open approach. We are proud to support the cause of collective defense by contributing to the important research at the Center.”

—**JASON KEIRSTEAD**, Distinguished Engineer & CTO IBM Security Threat Management, OASIS Board of Directors member

2022 IMPACT REPORT

CONTENTS

MITRE ENGENUITY™ | Center for Threat Informed Defense

LETTER FROM THE DIRECTOR

Welcome to the second annual Center for Threat-Informed Defense Impact Report. Just two years after our first R&D project release, the Center published its 20th R&D project in September, then released two additional projects by the end of 2022. Closing out the year with 22 published R&D projects is a truly remarkable achievement that can only be accomplished with the hard work and dedication of the Center's 30 Participants. I invite you to explore the projects in this report and welcome your insight and feedback.

In this 2022 Impact Report, you will find evidence of the most successful year in the Center since our launch in 2019. Throughout the report we highlight an active innovation pipeline, the consistent, methodical release of open-sourced research projects, the addition of sophisticated cyber teams to the Center's Participant roster, and the organic adoption of the Center's work.

The single most rewarding outcome of 2022 has been the organic adoption of the Center's work. Not only are security teams using our work in creative ways, but our work is reaching small businesses, academia, and non-profit organizations that lack the resources to develop and conduct this research on their own. Thanks to the support of our Participants and the community, the Center's R&D program makes a difference. ATT&CK Powered Suit—a freely available browser extension that puts MITRE ATT&CK® at your fingertips—was downloaded over 5,000 times. The Center's Adversary Emulation Library has become the go-to source for cyber defenders in need of research for FIN6, MenuPass, and Micro Emulation Plans. Cyber defenders use Attack Flow to go beyond a technique-by-technique focus to understanding and defending against attacks. Our work creates a community that shares the Center's mission: **Changing the Game on the Adversary.**

In the coming year, we will convene the community as the focal point for threat-informed defense. Together with Center Participants, we will engage with the community to foster collaboration, ensure that the Center has broad awareness of pressing challenges, and develop timely solutions that enable cyber defenders to be more efficient and effective.

Our challenge is to improve cyber defense globally, fundamentally shift the economics of cyber-attacks in favor of the defenders, and to change the game on the adversary.

Thank you for your continued support,

JONATHAN BAKER
Director, Center for Threat-Informed Defense

Published November 17, 2022

DEFENDING IAAS WITH ATT&CK

PROJECT SUMMARY

Defending Infrastructure-as-a-Service (IaaS) with ATT&CK has developed an ATT&CK matrix that enables users to easily understand and work with the techniques applicable to IaaS environments, regardless of whether the attacks target the cloud management layer, the container technology, or the hosted infrastructure. The project has also developed documentation and tools to simplify creating overlays for other domains like Industrial Control Systems (ICS) or Operational Technology (OT).

Research Participants

ATTACKIQ
CIS Center for Internet Security
citi
CROWDSTRIKE
JPMorgan Chase & Co.
verizon

Problem

Organizations using IaaS need to understand the techniques adversaries can use against them regardless of whether they occur at the cloud management layer, the container technology, or the hosted infrastructure itself (primarily Linux servers).

Solution

Provide a straightforward approach to understanding and working with techniques applicable to IaaS across Cloud, Containers, and Linux.

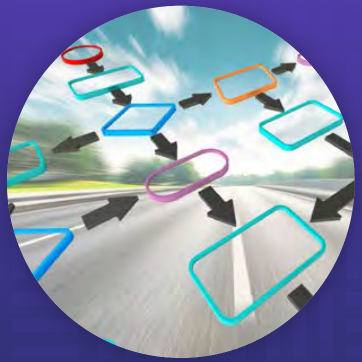
Impact

Organizations that use IaaS can easily understand and defend against the full set of techniques that might be used against that environment.

> *The Defending IaaS project delivered on its promise to provide defenders a complete view of adversary behavior against systems in the cloud and on premise. ATT&CK tools (Workbench and Navigator) make it easy to customize and visualize the collection."*
>
> –JOEL SPURLOCK, SENIOR DIRECTOR, CROWDSTRIKE

Published October 27, 2022

ATTACK FLOW



PROJECT SUMMARY

Attack Flow is a data model with supporting tooling and examples for describing sequences of adversary behaviors. Attack Flow helps defenders understand, share, and make threat-informed decisions based on the sequence of actions in a cyber-attack. Flows can be analyzed to identify common patterns in adversary behavior, then overlayed on ATT&CK Navigator layers to understand defensive coverage and create a foundation for intel-driven adversary.

Research Participants

Analysis & Resilience Center FOR SYSTEMIC RISK
ANOMALI
ATTACKIQ
citi
CROWDSTRIKE
cybereason
CYBER THREAT ALLIANCE
FORTINET
FUJITSU
GLOBAL CYBER ALLIANCE
HCA Healthcare
IBM Security
JPMorgan Chase & Co.
Microsoft
verizon

Problem

Defenders often track adversary behaviors atomically, focusing on one specific action at a time. This makes it harder to understand adversary attacks and to build effective defenses against those attacks.

Solution

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

Impact

Help defenders and leaders understand how adversaries operate and compose atomic techniques into attacks to better understand defensive posture.

> *For many years, operationalization of ATT&CK has focused on atomic adversary TTPs. That's important, but it's not how adversaries think. They think in graphs, and the ability to chain together TTPs to achieve their objectives. Attack Flow was an incredibly important project and a big step that enables defenders to chain together TTPS and graph them."*
>
> – **CARL WRIGHT**, CHIEF COMMERCIAL OFFICER, ATTACKIQ

> *Building on ATT&CK's foundation, Attack Flow enables us to better understand the big picture of cyber attacks by letting us create, share, store, and visualize the steps in cyber attacks. I cannot wait to see where Attack Flow will lead us in a few years."*
>
> –**RYUSUKE MASUOKA**, TECHNICAL ADVISOR, FUJITSU SYSTEM INTEGRATION LABORATORIES

Published September 15, 2022

MICRO EMULATION PLANS

PROJECT SUMMARY

Micro Emulation Plans help organizations validate their defenses quickly and easily by building smaller scale adversary emulation plans that are fully automated using compatible tools and focused on common threats. The Micro Emulation Plans help scale the impact of the Adversary Emulation Library beyond those with sophisticated red teams to allow even those without a red team to run scenarios in compatible breach and attack simulation or automated adversary emulation tools. They can also make improvements and validate the improvements.

Research Participants

ATTACKIQ® Booz | Allen | Hamilton® citi EY Building a better working world FUJITSU

HCA Healthcare™ IBM Security Microsoft verizon✓

Problem

Long and complicated emulation plans can be complex and costly for organizations to implement and then rapidly iterate based on results.

Solution

Create light-weight emulation plans that focus on key attack techniques for important threats.

Impact

Red teams and others can quickly perform emulations for relevant threats that lead to positive changes in defensive posture.

> *“Micro Emulation Plans help bring adversary emulation to any security team by decreasing the time and complexity it takes to validate defensive measures. The plans are diverse in adversary techniques and require little effort to execute which aids in our ability to perform continuous security testing.”*
>
> –TJ BEAN, DIRECTOR OF CYBERSECURITY, HCA HEALTHCARE

Published July 28, 2022

CLOUD ANALYTICS

PROJECT SUMMARY

The Cloud Analytics project advances the state of the practice by developing a blueprint for writing analytics for cloud platforms. To create the blueprint, the team “learned by doing”—exercising adversary behaviors, developing corresponding analytics, and refining them. Lessons learned were gathered along the way and incorporated into the analytics blueprint that we shared with the community.

Research Participants

citi CROWDSTRIKE FUJITSU Google Cloud HCA Healthcare Microsoft SIEMENS splunk> turn data into doing. verizon

Problem

Defenders achieve sufficient visibility of adversary behaviors in on-premises environments, but they struggle to achieve comparable adversary visibility in cloud environments.

Solution

Develop a foundational set of cloud analytics for key TTPs and capture best practices and lessons learned in an analytics blueprint document.

Impact

Improves defenders’ ability to develop analytics to detect adversary behaviors in cloud environments.

> *Our customers use multiple cloud services for which cyber analytics are becoming increasingly important. Prior to the Center’s Cloud Analytics Project the industry lacked a unified approach to cyber analytics and this project is a great first step toward addressing that void.”*
>
> –KOJI YAMADA, RESEARCH MANAGER, FUJITSU SYSTEM INTEGRATION LABORATORIES

Published June 28, 2022

SECURITY STACK MAPPINGS—GOOGLE CLOUD PLATFORM

PROJECT SUMMARY

This project identified and mapped security capabilities available as part of Google Cloud Platform (GCP) to the ATT&CK techniques to which they can detect, protect, or respond. This allows cyber defenders of cloud platforms to make threat-informed decisions about which capabilities to use and how to use them.

Research Participants

ATTACKIQ · citi · Google Cloud · HCA Healthcare · JPMorgan Chase & Co. · usbank

Problem

Administrators and defenders of GCP lack a comprehensive view of how native GCP security controls defend against real-world adversary TTPs.

Solution

Map the effectiveness of native security capabilities available in GCP to specific ATT&CK techniques.

Impact

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

> *I've been able to use the GCP security control mappings as both a training method for those who are not aware of ATT&CK, and as a guiding tool when creating new security use cases, which has been fantastic."*
>
> –IVAN NINICHUCK, SOLUTIONS ARCHITECT, GOOGLE CLOUD

Published May 10, 2022

TOP ATT&CK TECHNIQUES

PROJECT SUMMARY

Top ATT&CK Techniques provides defenders with a systematic approach to prioritizing ATT&CK techniques. Our open methodology considers technique prevalence, common attack choke points, and actionability to enable defenders to focus on the ATT&CK techniques that are most relevant to their organization. The Top ATT&CK Techniques Calculator makes building customized top technique lists easy. Users can create a top ten technique list tailored to their organization. The Top Ransomware Technique List provides a starting point for defending against ransomware attacks and demonstrates how the Top ATT&CK Techniques methodology can be tailored to different use cases.

Research Participants

ATTACKIQ CIS Center for Internet Security citi CROWDSTRIKE HCA Healthcare

JPMorgan Chase & Co. Microsoft red canary splunk> turn data into doing.

Problem

Defending against all ATT&CK techniques is simply not practical and, without guidance, determining which techniques to focus on is overwhelming.

Solution

Publish a methodology and tools to help defenders systematically prioritize ATT&CK techniques.

Impact

Defenders focus on adversary behaviors that are most relevant to their organization and will have the greatest effect on their security posture.

> *Organizations struggle to understand what they should focus on first. With Top ATT&CK Techniques, the Center produced a calculator to assist in prioritizing. We pioneered chokepoint analysis in that project and built a scoring rubric based on customer input so they could focus on TTPs in their organization to create a much better prevention and detection practice."*
>
> – CARL WRIGHT, CHIEF COMMERCIAL OFFICER, ATTACKIQ

> *CIS is proud of our participation in the Top ATT&CK Techniques project, which leveraged our Community Defense Model to select ransomware variants in the creation of a ransomware top technique list. Collaborative research projects like this provide important resources to help defenders focus on finding and stopping adversaries in their tracks."*
>
> –CURTIS DUKES, EXECUTIVE VICE PRESIDENT AND GENERAL MANAGER, SECURITY BEST PRACTICES, CENTER FOR INTERNET SECURITY

Published February 23, 2022

SIGHTINGS ECOSYSTEM

PROJECT SUMMARY

The Sightings Ecosystem project provides cybersecurity defenders and researchers with critical insight into real-world, in the wild adversary behaviors mapped to ATT&CK. The ecosystem aims to fundamentally advance the collective ability to see threat activity across organizational, platform, vendor and geographical boundaries. Voluntarily contributed raw “sightings”, or observations of specific adversary TTPs that are mapped to ATT&CK, anonymized, and then aggregated to produce intelligence describing insights from that data.

Research Participants

ATTACKIQ · CYBER THREAT ALLIANCE · FORTINET · GLOBAL CYBER ALLIANCE · verizon

Problem

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

Solution

Build and operate a way for organizations to safely contribute sightings of specific ATT&CK TTPs which powers analytics that create a picture of where and when TTPs are used.

Impact

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.

> *“One of the most powerful things you can do when fighting cybercrime is shift the economics of an attack, and the work we are doing with the Center focused on adversary behavior does just that. Fortinet is committed to new projects that extend the work invested into Sightings, with the intent to help build corpus, develop tools for visualization, and add further contextual insight into the data. Fortinet looks forward to our continued work with the Center on important projects as a Research Partner.”*
>
> –**DEREK MANKY**, CHIEF OF SECURITY INSIGHTS AND GLOBAL THREAT ALLIANCES, FORTINET’S FORTIGUARD LABS

Published February 17, 2022

INSIDER THREAT TTP KNOWLEDGE BASE

PROJECT SUMMARY

The Insider Threat TTP (Tactics, Techniques, and Procedures) Knowledge Base aims to advance our collective understanding of the technical mechanisms that insider threats have used. With this knowledge, Insider Threat Programs and Security Operations Centers can stop insider threats by detecting, mitigating, and emulating insider actions on IT systems. Utilizing the Knowledge Base, cyber defenders across organizations will identify insider threat activity on IT systems and limit damage. Capturing and sharing the Design Principles and Methodology for developing the Knowledge Base is a foundational step to establishing this community resource and also enabling its broad adoption and ongoing development.

Research Participants

citi CROWDSTRIKE HCA Healthcare JPMorgan Chase & Co. Microsoft verizon

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.

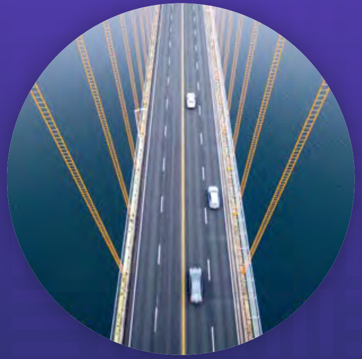
Impact

Defenders limit damage by detecting, mitigating, and emulating insider actions on IT systems.

> *The Center brought together companies with deep knowledge and experience of Insider Threat detection and response and delivered a Knowledge Base for the benefit of the broader community built on real world case data and observed TTPs."*
>
> –**JOHN STRINGER**, DIRECTOR OF PRODUCT MANAGEMENT, CROWDSTRIKE

Updated January 13, 2022

NIST 800-53 CONTROLS TO ATT&CK MAPPINGS



PROJECT SUMMARY

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

Research Participants

ATTACKIQ

CIS. Center for Internet Security

JPMorgan Chase & Co.

Problem

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

Solution

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

Impact

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

> *“In ground-breaking research, the Center aligned the world’s two most important threat and risk management frameworks: ATT&CK and NIST 800-53. Why is this important? Compliance in and of itself does not equal security. With this research, you can now use ATT&CK to validate your compliance controls. The result: a revolutionary increase in security readiness.”*
>
> –**CARL WRIGHT**, CHIEF COMMERCIAL OFFICER, ATTACKIQ

BROWSER EXTENSION

ATT&CK POWERED SUIT

MITRE ATT&CK® AT YOUR FINGERTIPS

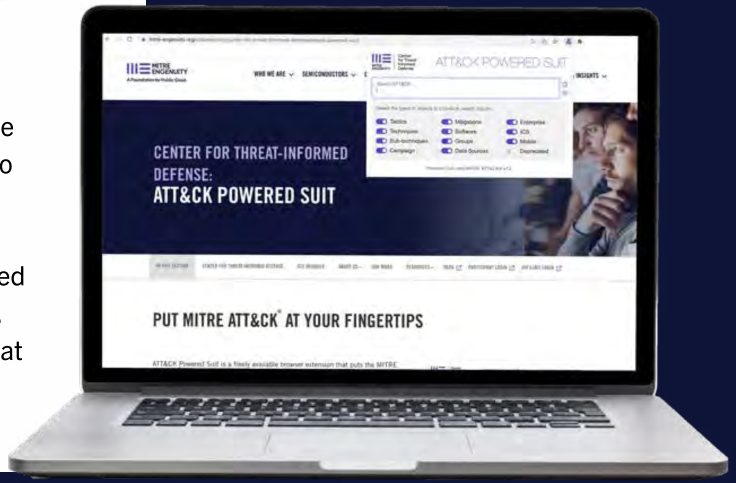
ATT&CK Powered Suit is a freely available Chrome and Edge Extension that puts the ATT&CK knowledge base at users' fingertips. This extension enables quick searches for TTP without disrupting workflow. Users can streamline research by easily copying snippets and exporting selected techniques to ATT&CK navigator. The extension supports context menus, omnibar, and more. This project would not have been possible without our valued partnership with Fujitsu. We are especially grateful to Mr. Toshitaka Satomi for proposing the original concept and for his hard work providing the initial source code.

Our Most Heartfelt Thanks

FUJITSU

CREATED WITH CYBER THREAT INTEL ANALYSTS AND DEFENDERS IN MIND

The ATT&CK community spends too much time copying and pasting text from one place to another to achieve simple tasks like looking up ATT&CK technique IDs, linking to a software page, or just finding a term from the latest threat intel report in the ATT&CK knowledge base. Now, with ATT&CK Powered Suit, they can quickly find ATT&CK objects. This extension creates a browser overlay that enables copying information with a single click to paste.



CENTER FOR THREAT-INFORMED DEFENSE:
ATT&CK POWERED SUIT

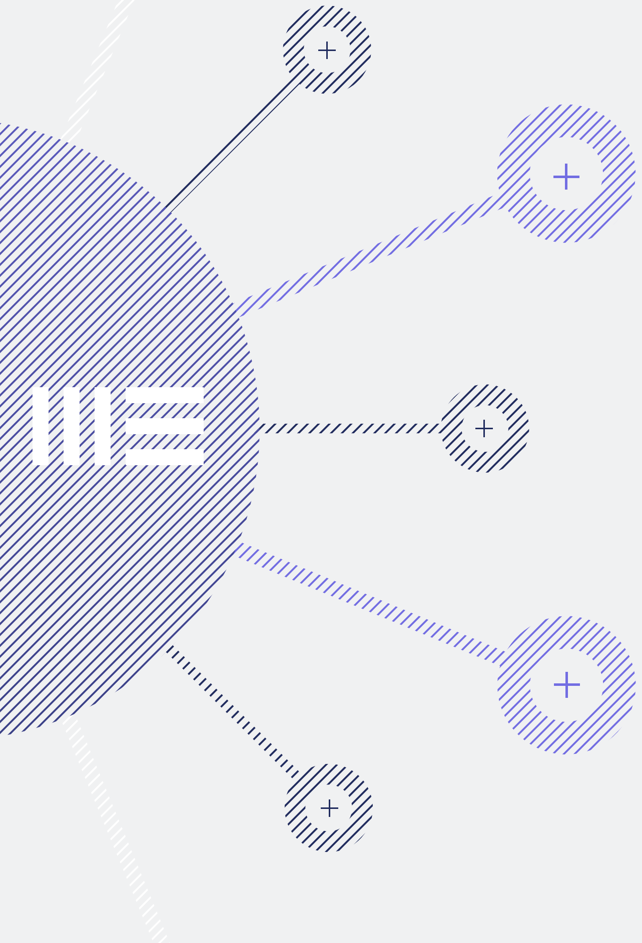
PUT MITRE ATT&CK® AT YOUR FINGERTIPS

ATT&CK Powered Suit is a freely available browser extension that puts the MITRE

> *"ATT&CK Powered Suit (APS) was born from my efforts to simplify using ATT&CK. The Center refined and published my prototype, creating a capability for the whole community. The global use and impact of APS is amazing and I am grateful for the Center making this happen."*
>
> –TOSHITAKA SATOMI, RESEARCHER, FUJITSU SYSTEM INTEGRATION LABORATORIES

CELEBRATING THE CONTRIBUTOR COMMUNITY

Community drives the advancement of threat-informed defense. Advancing threat-informed defense globally is only possible with community support and contributions.



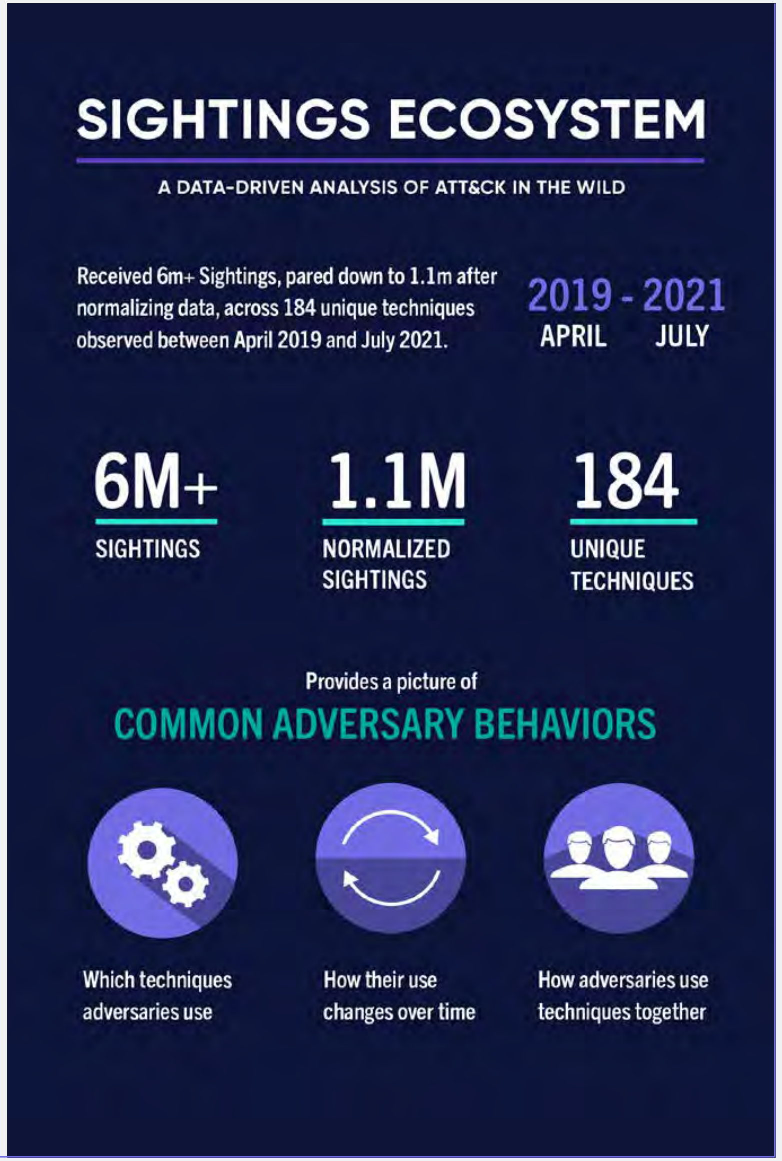
STOPPING INSIDER THREATS

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

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.



SIGHTINGS ECOSYSTEM

A DATA-DRIVEN ANALYSIS OF ATT&CK IN THE WILD

Received 6m+ Sightings, pared down to 1.1m after normalizing data, across 184 unique techniques observed between April 2019 and July 2021.

2019 - 2021
APRIL JULY

6M+ SIGHTINGS

1.1M NORMALIZED SIGHTINGS

184 UNIQUE TECHNIQUES

Provides a picture of

COMMON ADVERSARY BEHAVIORS

Which techniques adversaries use

How their use changes over time

How adversaries use techniques together

Community adoption and feedback accelerates innovation and advances threat-informed defense. Defenders' work, ideas, and hard problems are inputs into the Center's innovation pipeline. They directly influence the projects that we launch and the approaches that we take.

Feedback and applications of Center research and development impact what we do and guide others as they adopt a threat-informed defense.

Changing the game on the adversary takes community support.

ADVISORY COUNCIL

STRATEGIC GUIDANCE AND EXECUTIVE ADVOCACY IN SUPPORT OF THE CENTER'S MISSION

Our Advisors apply their executive experience to guide the Center as we evolve our strategy, model, and approach to advancing threat-informed defense. They increase the Center's impact and support the Center's growth by leveraging their connections and influence.

COUNCIL GOALS

IMPACT

Focus on visibility, accessibility, and applicability of projects

GROWTH

Advise on growth strategy and membership goals

MODEL

Evolve the business model and shape new programs

FOCUS

Recommend and evaluate new focus areas

Advisors

Advisors from the Center's Founding Participant organizations and Research Partner organizations invest their time to strategically advance threat-informed defense.

CARL WRIGHT

Chief Commercial Officer
AttackIQ
Founding Research Partner

ALEXIS LAVI

Chief Security Architect, Cyber Security Technology
Bank of America
Founding Research Partner

GARRETTSON BLIGHT

Director of National Cyber Solutions
Booz Allen Hamilton
Founding Research Sponsor

ELVIS VELIZ

Global Head of Cloud Security Operations
Citigroup
Founding Research Partner

ELIA ZAITSEV

SVP/CTO of the Americas
CrowdStrike
Research Partner

MICHAEL DANIEL

President & Chief Executive Officer
Cyber Threat Alliance
Founding Non-Profit Participant

DEREK MANKY

Chief Security Strategist & VP Global Threat Intelligence
Fortinet's Fortiguard Labs
Research Partner

SYOICHI KANZAKI

President
Fujitsu System Integration Laboratories
Founding Research Sponsor

TJ BEAN

Director of CyberSecurity
HCA Healthcare
Founding Research Partner

SRIDHAR MUPPIDI

IBM Fellow, VP & CTO
IBM Security
Research Partner

SHAHAN SUDUSINGHE

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

KARTHIK SELVARAJ

Partner Director/Principal Security Research
Microsoft
Founding Research Sponsor

DR. MARTIN OTTO

Head of Cybersecurity Research Group
Siemens AG
Founding Research Sponsor

ALEX PINTO

Security Research Lead
Verizon
Research Partner

HOW TO 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, the most highly 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

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 be more impactful. Be the first to know about R&D project releases by signing up.

JOIN THE AFFILIATE PROGRAM—SHOWCASE OUR R&D IN USE

Affiliates are early adopters of the Center's work that incorporate our R&D into their product or service offerings and educate consumers about threat-informed defense. Through co-branded use cases, Affiliates exponentially expand the reach of the Center's R&D, highlight adoption best practices, and provide solutions that leverage our work. Learn more about becoming an Affiliate.

LEARN MORE ABOUT GETTING INVOLVED →

YOU CHOOSE HOW TO GET INVOLVED

BECOME A CENTER PARTICIPANT—GUIDE THE R&D PROGRAM

As a highly 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 the Center's R&D projects 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.

Openess
Members propose ideas

Flexibility
Members choose projects

Collaboration
Members share ideas, research, and funding

Leadership
Members gain key expertise

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.

PROJECT ROSTER 2020–2021

FIN6 ADVERSARY EMULATION PLAN

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

CALDERA PATHFINDER

This open-source CALDERA plugin helps you understand what a vulnerability exposes to an adversary and what potential destructive paths an adversary could take within the network due to those vulnerabilities. Pathfinder aims to push the boundaries on vulnerability scanning, moving them to the next generation by integrating vulnerability scan data with the CALDERA automated adversary emulation platform.

ATT&CK FOR CLOUD

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

MENUPASS ADVERSARY EMULATION PLAN

menuPass is a threat group with members known to have acted in association with the Chinese Ministry of State Security's (MSS) Tianjin State Security Bureau and also worked for Huaying Haitai. menuPass has targeted healthcare, defense, aerospace, finance, maritime, biotech, energy, and government sectors globally, with emphasis on Japanese organizations. This project developed an adversary emulation plan for menuPass.

ATT&CK FOR CONTAINERS

This project investigated the viability of adding container-related techniques into ATT&CK, leading to an ATT&CK for Containers matrix. It covers both orchestration-level and container-level adversary behaviors in a single Containers platform and was incorporated into version 9 of ATT&CK. The team worked with a global set of contributors to identify and refine both existing ATT&CK techniques and completely new container-specific ones.

ATT&CK WORKBENCH

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

SECURITY STACK MAPPINGS AZURE

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

ATOMIC DATA SOURCES

Cyber threat detection starts with understanding the data sources and sensors used to detect a given adversary TTP. Motivated by a lack of detailed data source definitions in ATT&CK to support defensive cyber operations use cases, we wanted to greatly expand the set of data sources in ATT&CK and research creating an open data model for data sources that would enable defenders to quickly determine if they have the data.

ATT&CK INTEGRATION INTO VERIS

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

SECURITY STACK MAPPINGS—AMAZON WEB SERVICES

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

THREAT REPORT ATT&CK MAPPER (TRAM)

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

MAPPING ATT&CK TO CVE FOR IMPACT

This research defines a methodology for using ATT&CK to characterize the potential impacts of vulnerabilities, as ATT&CK's tactics and techniques enable defenders to understand the impacts of vulnerabilities. Vulnerability reporters and researchers use the methodology to describe the impact, enabling defenders to easily integrate vulnerability information into their risk models and identify appropriate compensating security controls.

NIST 800-53 CONTROLS TO ATT&CK MAPPINGS

This project created a comprehensive set of mappings between ATT&CK and NIST Special Publication 800-53 with supporting documentation and resources. The mappings provide a critically important resource for organizations to assess their security control coverage against real-world threats as described in the ATT&CK knowledge base. They also provide a foundation for integrating ATT&CK-based threat information into the risk management process.

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.

EXPLORE THE CENTER FOR THREAT-INFORMED DEFENSE →

About MITRE Engenuity

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