MITRE ENGENUITY | Center for Threat Informed Defense

THREAT-INFORMED DEFENSE ADOPTION HANDBOOK

September 2021 Edition, Volume 1

8 MITRE ATT&CK®-based Resources

To learn more about the Affiliates community or how to become an Affiliate, we're happy to contact you.

In just two short years since we launched the Center for Threat-Informed Defense, we've released a wide array of innovative research and development projects that are freely available to the entire community. This accomplishment is the direct result of our unique model – bringing together some of the best security teams from organizations from around the world to focus on collaborative R&D in the public interest. The substantial investments that our participant organizations make in our R&D program is the fuel that powers the Center.

This handbook documents the first eight R&D projects that the Center has released to date. These projects are the embodiment of the Center's mission to advance the state of the art and the state of the practice in threat-informed defense, globally. We've organized these projects in three categories: foundational work that enables threat-informed defense, projects that help you connect ATT&CK to the rest of your defensive toolkit and projects that help you validate that your defenses are working. Taken together, this work represents a significant expansion in the resources that are available to the cybersecurity community. But they also represent just the beginning as the Center and our participants are hard at work on even more practical and innovative resources that we'll be releasing in the months to come.

With the launch of the Center's Affiliate program, we are expanding the opportunities for cybersecurity companies to be at the forefront of our innovation. As the Center releases new R&D projects, our Affiliates will be well-positioned to put our work into practice and communicate their capabilities to the threat-informed defense community. I hope you will consider joining us as we change the game on the adversary.

RICHARD STRUSE
Director, Center for Threat-Informed Defense

TABLE OF CONTENTS

Project summaries

4 Brief abstracts of freely available Center for Threat-Informed Defense projects.

Projects that enable threat-informed defense

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

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

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

Projects that connect ATT&CK to the frameworks and capabilities that you use

17 **NIST 800-53 Controls to ATT&CK Mappings**: Allows defenders to quickly focus on understanding how the controls in use in their environment relate to adversary TTPs of interest to them.

21 **Security Stack Mappings – Azure:** Empowers defenders with independent data on which Azure controls are most useful in defending against the adversary TTPs they care about.

Projects that help you validate your defenses

27 **Adversary Emulation Library:** Enables cyber defenders to see their defenses from the perspective of the adversary.

- 30 FIN6
- 33 menuPass
- 35 All Available Plans

36 **CALDERA Pathfinder:** Shows defenders what a vulnerability exposes to an adversary and what potential destructive paths an adversary could take within the network as a result of those vulnerabilities.

Adopting Projects with the Center COMING SOON

39 **The Affiliates Program:** Affiliates lead the charge in driving global adoption of the latest R&D projects built by the Center for Threat-Informed defense.

About the Center for Threat-Informed Defense

43 **Contact information**

SUMMARIES

Projects that enable threat-informed defense

ATT&CK FOR CLOUD

The ATT&CK for Cloud project is addressing the problem of defenders lacking the visibility into adversary behaviors in cloud technologies. This ultimately leads organizations exposed to emerging threats. ATT&CK for Cloud is an expansion of MITRE ATT&CK that focuses on describing adversary behaviors in, and against, Cloud technologies. These efforts will allow for a simplified defenders use of ATT&CK. This is accomplished by aligning ATT&CK's coverage for Cloud TTPs with how organizations are using Cloud in their operations.

Read more

ATT&CK FOR CONTAINERS

The ATT&CK for Containers project is geared towards solving the issue of the scarcity of defenders visibility into emerging threats against container technologies. There is a need for knowledge into adversary behavior in, and against, container technologies. The ATT&CK for Containers is a solution to that by expanding MITRE ATT&CK to describe adversary behaviors within a container technology, such as Docker or Kubernetes, as well as against. These efforts will bring a focus to adversary behaviors in an emergent domain leveraging the well-understood, and widely adopted, ATT&CK methodology.

Read more

ATT&CK WORKBENCH

The ATT&CK Workbench project's focus is finding a solution for the problem of defenders struggling to integrate their organization's local knowledge of adversaries and their TTPs with the public ATT&CK knowledge base. This solution is building an easy-to-use open-source software tool that allows organizations to manage and extend their own local version of ATT&CK and keep it in sync with MITRE's knowledge base. These efforts will drastically reduce the barriers for defenders to ensure that their threat intelligence is aligned with the public ATT&CK knowledge base.

Read more

Projects that connect ATT&CK to the frameworks and capabilities that you use

NIST 800-53 CONTROLS TO ATT&CK MAPPINGS

The NIST 800-53 Controls to ATT&CK Mappings project address the issue of large and complex security control frameworks, such as NIST 800-53, not relating to actionable TTPs in ATT&CK. This project creates a comprehensive and open, curated set of mappings between 800-53 controls and ATT&CK techniques. These efforts will allow defenders to quickly focus on understanding how controls in use in their environment relate to adversary TTPs of interest to them.

Read more

SECURITY STACK MAPPINGS – AZURE

The Security Stack Mappings – Azure project focuses on how users of Azure lack a comprehensive view of how native Azure security controls can help defend against real-world adversary TTPs. This is accomplished by building a scoring methodology and using it to create mappings to show how effective native Azure security controls are in defending against specific ATT&CK techniques. This empowers defenders with independent data on which Azure controls are most useful in defending against the adversary TTPs they care about.

Read more

Projects that help you validate your defenses

ADVERSARY EMULATION LIBRARY

The Adversary Emulation Library is a freely available resource to help red teams and other cyber defenders systematically test their defenses based on real-world adversary TTPs. Each adversary emulation plan is rooted in intelligence reports and other artifacts that capture and describe breaches and campaigns publicly attributed to a specific named threat actor. We research and model each threat actor, focusing not only on what they do but also how and when. We then develop emulation content that mimics the underlying behaviors utilized by the threat actor. This approach results in nuanced emulation plans, each capturing unique scenarios and perspectives that we can leverage as threat-informed defenders.

Read more

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.

Read more

menuPass ADVERSARY EMULATION PLAN

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

Read more

CALDERA PATHFINDER

The CALDERA Pathfinder project is intended to address the common absence of adversary perspective in traditional vulnerability scanning. Often this doesn't effectively convey the true impact of a given vulnerability in an organization. This project pushes the boundaries on vulnerability scanning, moving them to the next generation by integrating vulnerability scan data with the CALDERA automated adversary emulation platform. The impact of this project will show defenders what a vulnerability exposes to an adversary and what potential destructive paths an adversary could take within the network due to those vulnerabilities.

Read more

ATT&CK FOR CLOUD

ATT&CK FOR CLOUD

This Center for Threat-Informed Defense project refines and expands MITRE ATT&CK's coverage of adversary behaviors in cloud environments.

Cloud Platforms

- When beginning the refinement of ATT&CK for Cloud in consideration of different platforms such as AWS, Azure, and GCP, it was deemed necessary to determine the correct abstraction level for ATT&CK moving forward.

- Following abstraction level measurements, AWS, Azure, and GCP platforms were consolidated into a single Infrastructure as a Service (IaaS) platform in the coming ATT&CK update. An IaaS platform was determined to make for a more inclusive ATT&CK for Cloud because it will represent Cloud Service offerings beyond AWS, Azure, and GCP platforms.

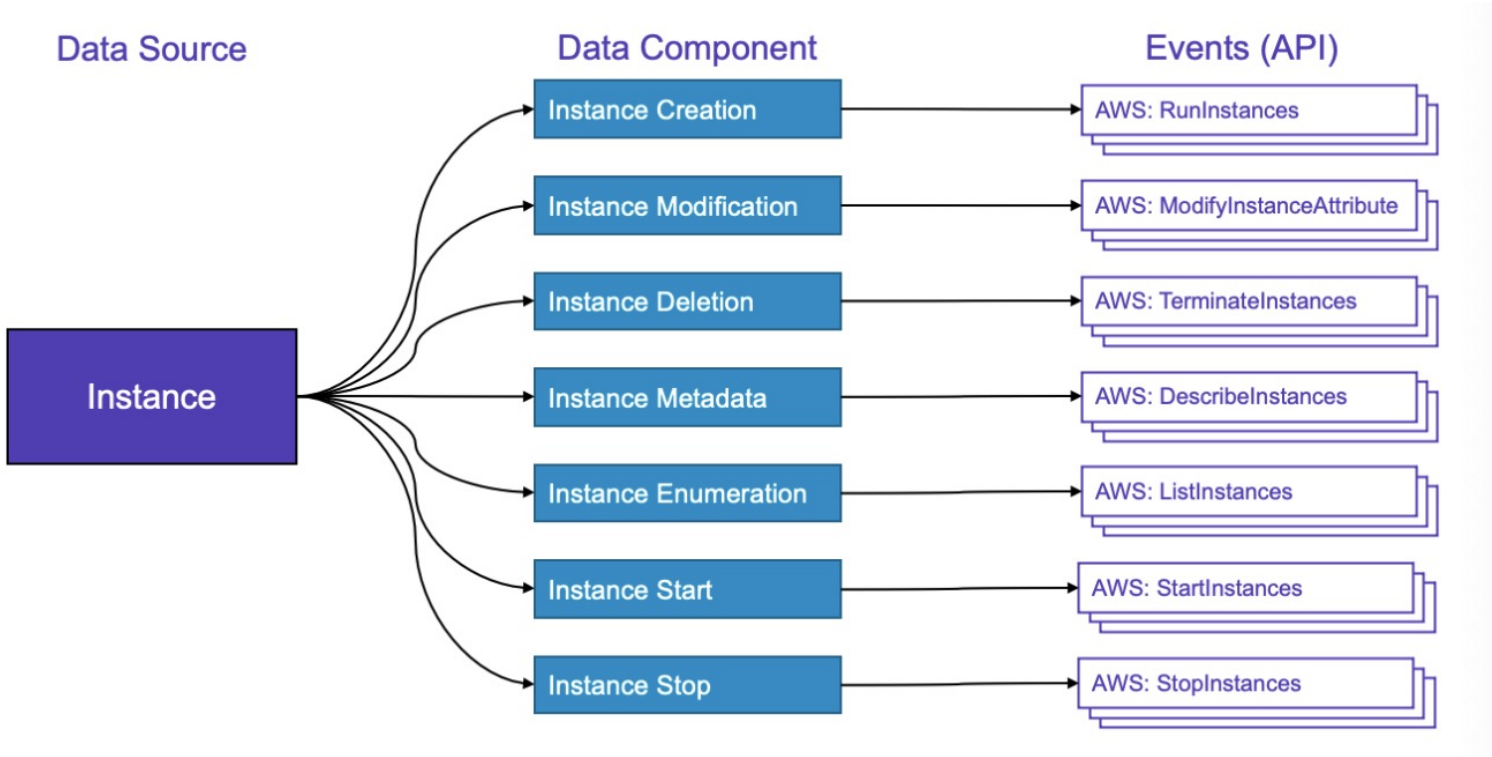
- Additionally, Cloud platforms such as SaaS (Software as a Service), PaaS (Platform as a Service), and FaaS (Function as a Service) were evaluated for future progression. SaaS kept the current breakout of SaaS, Azure AD, and Office 365. PaaS and FaaS were represented in the future IaaS platform with the plan to expand into individual platforms if adversarial behavior warrants a breakout.

Current and future ATT&CK for Cloud platforms

Cloud Data Sources

- The establishment of a set of data sources that aligned with Cloud platforms and is consistent with the future of other Enterprise ATT&CK data sources was relevant when drafting an initial set of Cloud data sources that align with events and APIs within IaaS environments.
- As refactoring of Cloud data sources began, several challenges arose. This included determining how to normalize the name and structure of data sources across multiple Cloud vendors, and which APIs and events involved in detections across multiple vendors are relevant to a particular data source.

Draft of an Att&ck for Cloud data source



Cloud Technique Coverage

- Cloud content in the October 2020 release of ATT&CK was developed from this Center partnership, including the creation of the new sub-technique Impair Defenses: Disable Cloud Logs (T1562.008) and the major update to Account Manipulation: Additional Cloud Credentials (T1098.001).

- Following deliberation across the ATT&CK team and conversations with the Cloud community, it was decided that IaaS techniques in ATT&CK should focus on adversarial behavior on endpoints, as endpoint behavior is already captured in the Linux, macOS, and Windows platforms. This led to the removal of Network Share Discovery (T1135), Data from Information Repositories (T1213), and Remote System Discovery (T1018) from the AWS, Azure, and GCP matrices.

Access the tactics and techniques representing the MITRE ATT&CK Matrix for Enterprise covering cloud-based techniques contain information for the Azure AD, Office 365, Google Workspace, SaaS, and IaaS platforms.

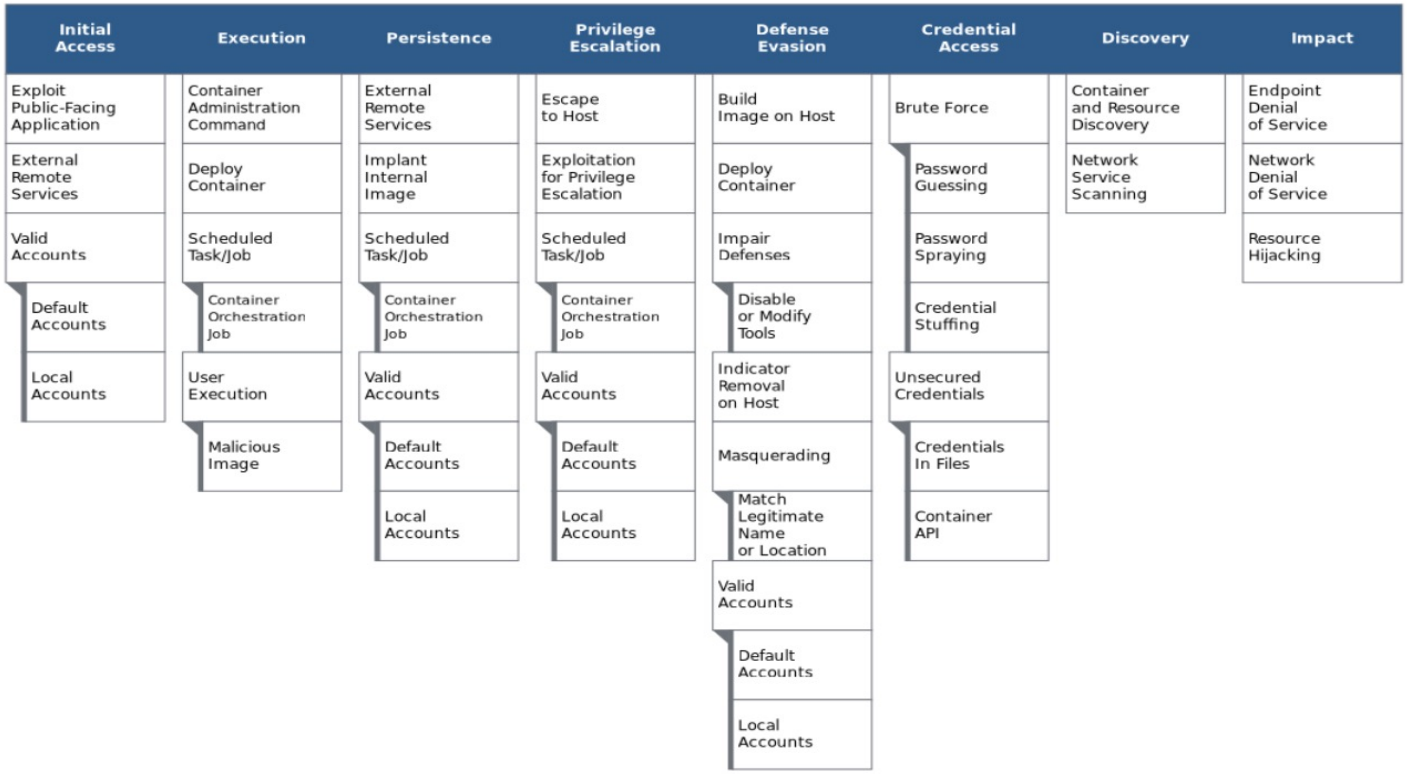
ATT&CK FOR CONTAINERS

ATT&CK FOR CONTAINERS

The Center for Threat-Informed Defense received contributions from the community to help shape ATT&CK for Containers which covers orchestration-level and container-level adversary behaviors. Thanks to contributions and feedback received from the community and Center members, the matrix now includes:

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

ATT&CK for Containers visualized in the ATT&CK Navigator



New from previous iterations?

- **Container Administration Command (T1609):** Per community feedback, the original name, "Container Service", was changed, particularly since Service is overloaded and already a concept used in Kubernetes. Changing the name additionally serves the dual purpose of clarifying what it means in the context of ATT&CK.

- **Valid Accounts:** Default Accounts (T1078.001): It was found that the default service account in Kubernetes fit more cleanly into this technique than Valid Account (T1078), so this sub-technique was added to the containers matrix.

- **Exploitation for Privilege Escalation (T1068):** This technique applies to virtualized environments, such as containers, when adversaries exploit software vulnerabilities to facilitate escaping the underlying host.

- **Impair Defenses (T1562) and Impair Defenses:** Disable or Modify Tools (T1562.001): This sub-technique was added because of a want to include the case where security tools related to a container deployment are disable by an adversary.

- **Indicator Removal on Host (T1070):** This technique may apply to an adversary deleting artifacts at the container orchestration layer.

- **Network Service Scanning (T1046):** This technique was added to map the behavior of adversaries scanning for services like kubelet within Kubernetes network.

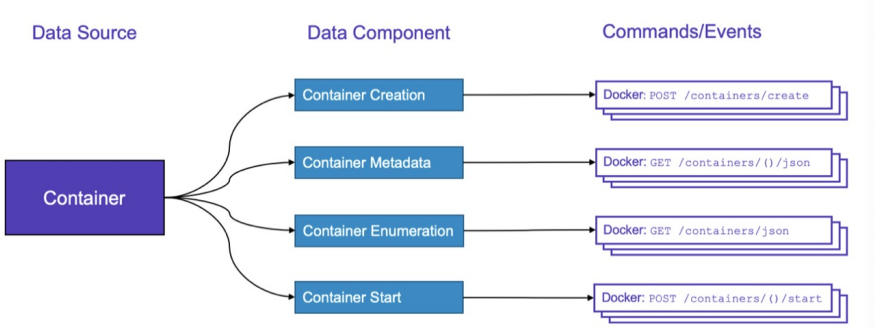
What about malware?

A set of malware related to containers (Kinsing (S0599), Hildegard (S0601)) was mapped into ATT&CK.

Data Sources

To match the refactor of data sources in ATT&CK, a set of data sources was developed that pertains to container techniques. As a result of strong relationships between the Containers, Cloud, and host-based platforms in ATT&CK, there is some overlap on data sources across these platforms. An example of how Containers was translated into a Container data source below.

Visualization of the Container data source



Access the tactics and techniques representing the MITRE ATT&CK Matrix for Enterprise covering techniques against container technologies

ATT&CK WORKBENCH

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. The Workbench was developed with the ATT&CK user community in mind to support practitioners that:

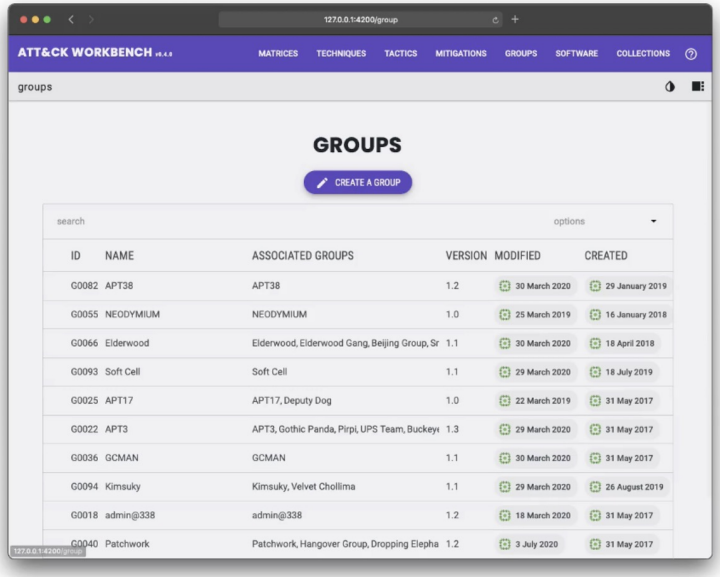
- Have ATT&CK at the core of your organization's security operations.
- Actively track threats against ATT&CK
- Align your defenses to ATT&CK
- Plan security investments based on ATT&CK

Extending one own's copy of ATT&CK

The primary utility of Workbench is the ability to create new objects or extend existing objects with new content. Matrices, techniques, tactics, mitigations, groups, and software can all be created and edited. Users can create an extension of the knowledge base according to own needs, or an entirely new dataset aligned with ATT&CK terminology and usable with ATT&CK tools. Data created within the Workbench can be seamlessly integrated into ATT&CK data - new groups or software can be connected to existing techniques through procedure examples, or new sub-techniques can be created under existing ATT&CK techniques.

Creating or extending ATT&CK data in a local knowledge base enables a number of important use cases, such as:

- Creating red-team techniques that practitioners can track just like existing ATT&CK techniques.
- Documenting groups or software that target sectors or organization but are not presently tracked by the ATT&CK team.
- Updating ATT&CK data to reflect internal, proprietary, or other reporting to which the ATT&CK team does not have access
- Developing one's own matrix with new techniques and tactics outside of the scope of the ATT&CK knowledge base.



To facilitate team collaboration, the Workbench includes features such as the ability to mark objects as "work in progress", "awaiting review", or "reviewed", and the ability to look through the history of an object to determine when a change was made and by whom.

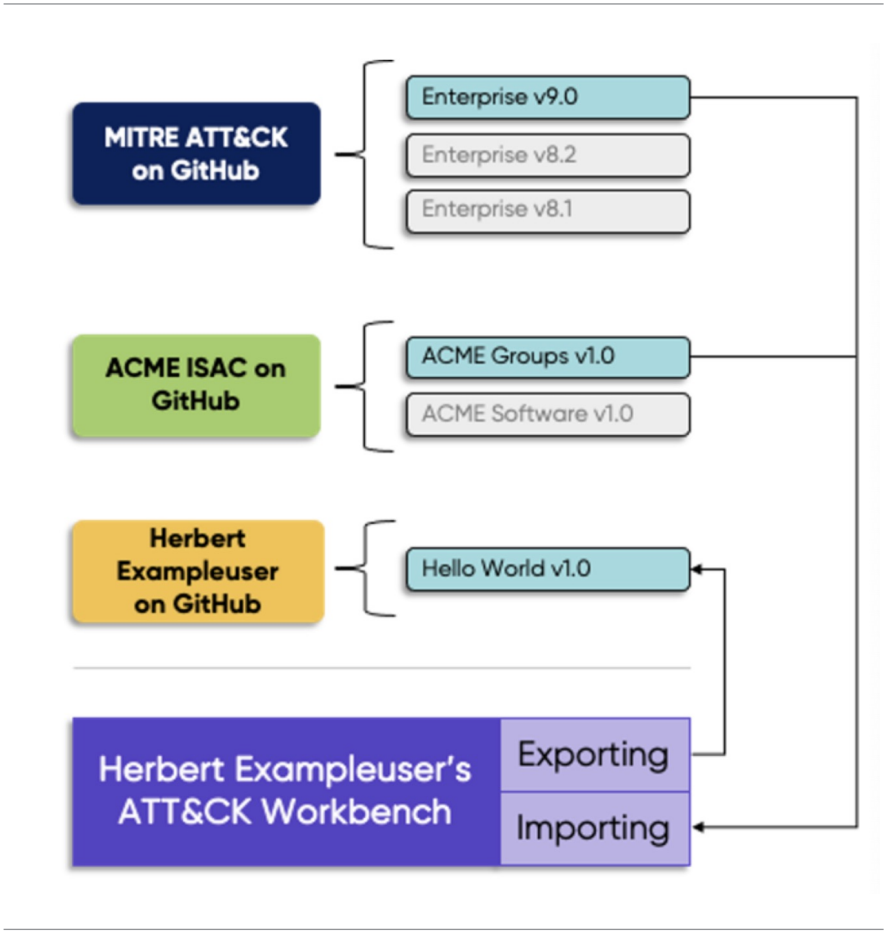
Breaking down silos – updating and sharing your extensions

As teams extend and annotate their ATT&CK data, Workbench will enable them to import updates to that data and provide the option to selectively share their work. Workbench users can subscribe to collections of ATT&CK data and publish their own. Subscriptions allow users to stay up to date with the evolving knowledge base by automatically pulling down updates when they're available. When a collection is imported into the Workbench users can preview exactly what it contains and how the contents relate to a local knowledge base.

Sharing of ATT&CK-related information among organizations as collections will:

- Streamline the process of staying synchronized with ATT&CK when it is updated by enabling automated import and providing detailed change history
- Allow users to integrate the latest from ATT&CK with intelligence extensions from other sources (threat intel vendors, ISACs & ISAOs, and other members of the ATT&CK community) by importing multiple collections
- Create structure and consistency for contributions to ATT&CK

Alongside the release of the Workbench, ATT&CK has made official collections representing current and previous ATT&CK releases available on GitHub. Users can simply subscribe to these collections and import new ATT&CK releases as soon as they are published.



ATT&CK in STIX 2.1

Since collections are represented in STIX 2.1, this is also the first time ATT&CK data is available in that version of the STIX specification. Since many community tools are still reliant on STIX 2.0, we will be maintaining both STIX 2.1 and STIX 2.0 versions of the dataset for the foreseeable future. However, the collection objects will only appear in the STIX 2.1 version of the dataset.

A Hub for Integrations

- **ATT&CK Website Repository:** View your knowledge base through the lens of the ATT&CK website and see notes you created on objects directly on their pages on the website. The ATT&CK Website integration will be useful to users who want to see their customized content in a familiar setting or use the many built-in features of the website such as full ATT&CK matrices, generated Navigator layers, and more.

- **ATT&CK Navigator Repository:** See and annotate your new techniques, tactics, and matrices in the ATT&CK Navigator and view notes you've created on techniques in the matrix view as if they were comments. This integration allows users to create layer files based on customized extensions of the ATT&CK dataset, enabling many of the existing workflows developed within the ATT&CK community which utilize the Navigator.

Supporting Resources

- The ATT&CK Workbench Frontend repository is the entry point for user documentation and installation instructions. In addition to the option of setting up each component individually, we also include a docker-compose (and associated instructions) to ease deployment of the application.

- The usage document explains how to use each feature of the application and many of the potential workflows for developing your extended knowledge base.

- The integrations document provides step-by-step instructions for setting up the ATT&CK Navigator and ATT&CK Website to connect to a local Workbench instance.

Get details on ATT&CK Workbench

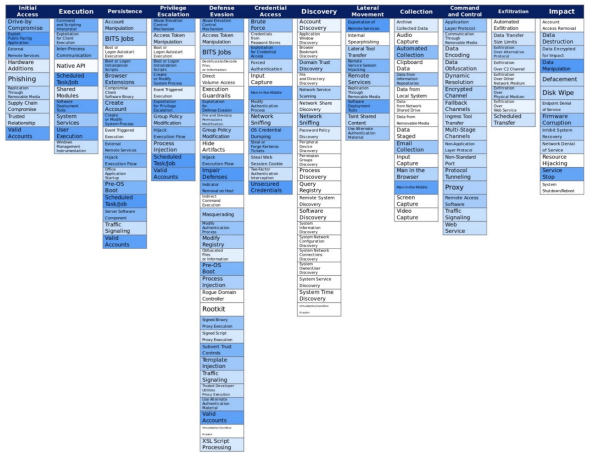
NIST 800-53 CONTROLS TO ATT&CK MAPPINGS

NIST 800-53 CONTROLS TO ATT&CK MAPPINGS

The Center for Threat-Informed Defense, in collaboration with participant organizations, work towards furthering the development of mappings between NIST 800-53 controls and ATT&CK techniques. The goal of the security control framework mappings is to establish a resource of mappings and ATT&CK techniques to empower the community. The repository contains security control framework mappings to MITRE ATT&CK® with supporting documentation and resources. These mappings provide a critically important resource for organizations to assess their security control coverage against real-world threats as described in the ATT&CK knowledge base and provide a foundation for integrating ATT&CK-based threat information into the risk management process.

NIST 800-53 Controls to ATT&CK Mappings

This scalable model can be applied to both refine NIST 800-53 mappings to ATT&CK and to expand coverage to include mappings to other security control frameworks.



Scoping decisions are important to understanding security control coverage and the selection process to develop this repository of mappings. The repository includes several ways to visualize the mappings.

- ATT&CK Navigator layers are provided to display the mappings in the context of the ATT&CK Matrix.

- ATT&CK Navigator layers are based upon a STIX representation of the controls and mappings.

The purpose of open documentation of scoping decisions for NIST 800-53 mappings is to encourage community collaboration. Due to the subjective nature of mapping, differences in perspective on the overall approach are anticipated. Examples of scoping decisions include:

- **ATT&CK Scope:** Work focused on ATT&CK techniques included in the Enterprise domain; Mobile techniques are not covered.

- **Control vs. Control Enhancements:** Mappings are done at the security control level and not to specific control enhancements.

- **Policy & Procedure Controls:** Controls associated solely with policy and procedure are out of scope as the focus is on the technical and operational elements of NIST 800-53

- **Technical in Focus:** Mappings are done for system-specific technical safeguards and countermeasures (e.g., block USB devices) and not for non-technical methods of mitigation (e.g., protection of physical space).

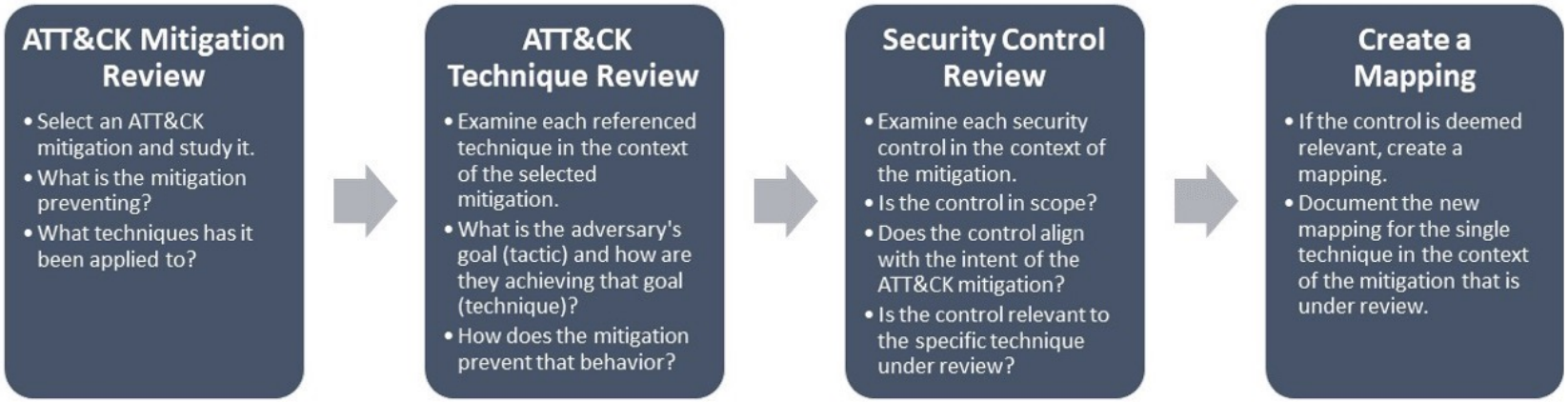
Our Methodology

ATT&CK mitigations act as the bridge connecting adversary behavior (tactics and techniques) to the security controls that may mitigate said behaviors. Each step incrementally builds understanding, allowing the analyst to understand ATT&CK techniques and sub-techniques in the context of a mitigation, then select relevant security controls to map.

1. **ATT&CK Mitigation Review:** Reviewing and analyzing each mitigation.
2. **ATT&CK Technique Review:** Understanding adversary objectives and goals a technique or sub-technique is designed to carry out.
3. **Security Control Review:** Examining security controls in the context of the mitigation and specific techniques.
4. **Create a Mapping:** Identifying and creating security control mappings to ATT&CK techniques and sub-techniques.

Much like an ATT&CK mitigation, a mapping between a security control and an ATT&CK technique or sub-technique means that the security control may prevent the successful execution of the technique or sub-technique. This methodology does not define degrees of mapping or control effectiveness.

Mapping Methodology



Supporting Tools & Resources

- The data model is based on STIX 2.0 JSON. This provides a consistent and machine-readable format for information sharing that allows for our easy integration with ATT&CK and its tool and resources. Basing the data model off of STIX allows for flexibility and extensibility to other security control frameworks.

- A set of Python tools support data manipulation, including the creation of new mappings and the customization of existing mappings. Users can easily refine and extend the mappings for their needs and locally rebuild the full set of supporting artifacts.

- The STIX 2.0 representation allows for the easy generation of different mappings, visualizations, and representations. The build process creates ATT&CK Navigator layers to help users easily understand a given security control framework's coverage of ATT&CK. Excel spreadsheets are also generated, listing the mappings for each framework in a tabular format.

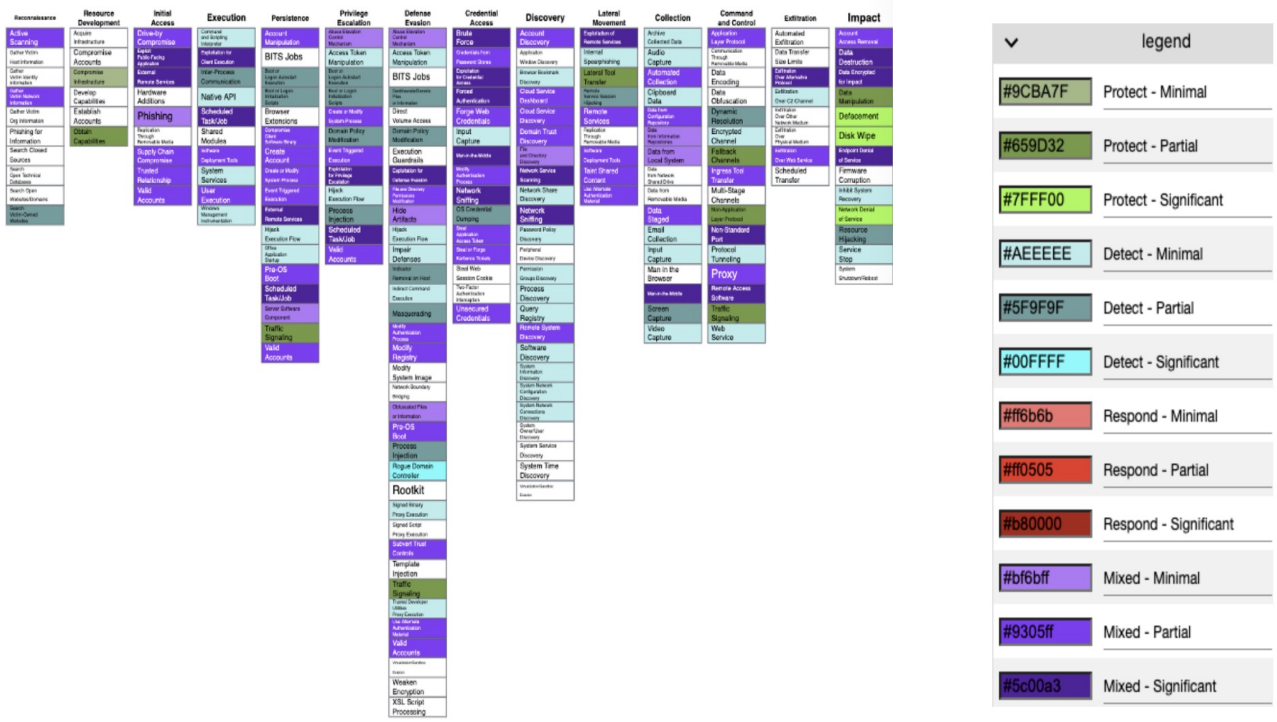
Get details on NIST 800-53 Controls to ATT&CK Mappings

SECURITY STACK MAPPINGS – AZURE

SECURITY STACK MAPPINGS - AZURE

The Center for Threat-Informed Defense's release of mappings between the security controls native to the Azure infrastructure as a Service (IaaS) platform allows organizations to assess their Azure security control coverage against real-world threats as described in the ATT&CK knowledge base.

Azure Security Stack Mappings



Influence Decisions

ATT&CK Scope: This work is focused on ATT&CK sub-techniques included in the Enterprise domain v8 (mobile techniques are not covered). There is a follow-on project that will update the mappings to ATT&CK v9.

Native Security Controls: This work focused on mapping the security controls produced by Microsoft or branded-as-Microsoft products. Third-party security controls available on the platform were excluded from analysis.

Azure Security Benchmark: Most of the controls included in scope were derived from Microsoft's Azure Security Benchmark v2 and the review of Azure security documentation.

Azure Defender for servers: The control was excluded from analysis due to its complexity and its inclusion with recent MITRE ATT&CK Evaluations.

ATT&CK Navigator layers were created for each mapped control, enabling the display of the mappings in the context of the ATT&CK Matrix, as shown above. In addition, a Markdown view is provided that enumerates all controls mapped, along with the list of ATT&CK techniques mitigated by each control.

Methodology

The methodology and its related artifacts (e.g., data format, scoring rubric) serve as a foundation for the Azure project, as well as subsequent projects aimed at mapping the security capabilities of additional platforms (e.g., AWS, Windows, macOS, etc.) to ATT&CK. The methodology consists of five mains steps, with each step incrementally building understanding, and allowing the analyst to understand the security control under analysis and the ATT&CK sub-techniques it mitigates. The five steps are:

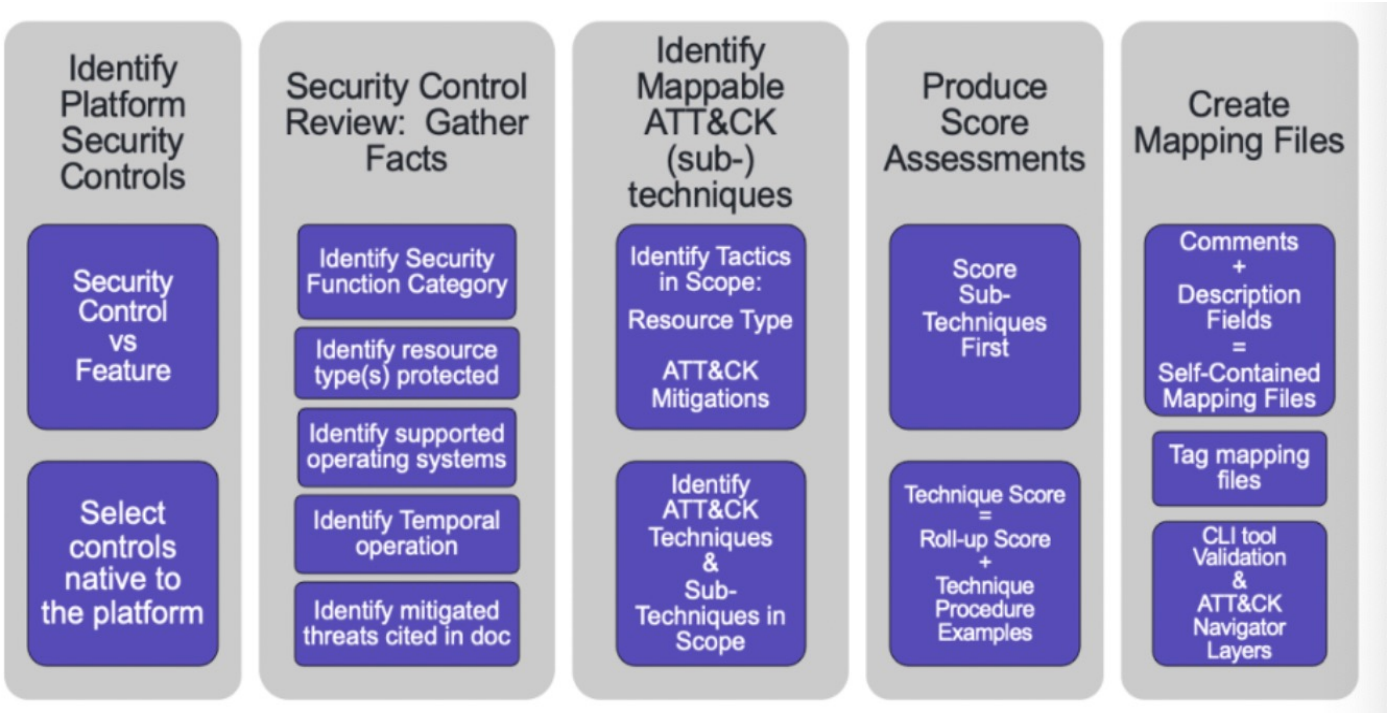
1. **Identify Platform Security Controls:** Research available platform security documentation to identify the set of security controls within scope of analysis.

2. **Security Control Review:** For each control, collect and analyze its documentation, identifying key information on its functionality that will enable selecting the set of ATT&CK sub-techniques that it mitigates. The methodology does not include operational validation of security controls in order to allow for broad coverage of a platform.

3. **Identify Mappable ATT&CK sub-techniques:** The information gathered in the previous step can be used to map the control to the set of ATT&CK sub-techniques it mitigates.

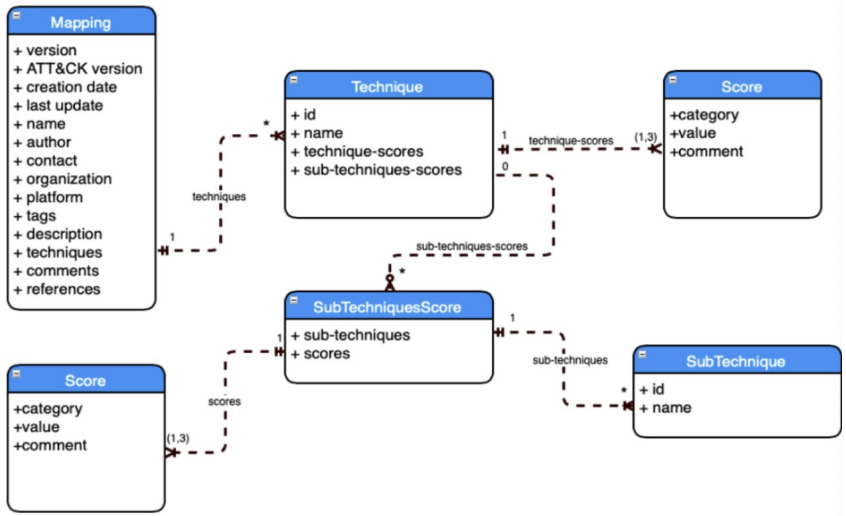
4. **Create Mapping Files:** Record the data gathered in the previous steps in the mapping file as specified in the mapping format.

Mapping Methodology



Data Model and Rubric

A YAML data format was developed to record the mapping information for a particular control.



Salient Properties of the Mapping Format

- **Mapping file per control:** Each mapping file records ATT&CK coverage information for a single security control, resulting in a mapping file per platform security control.

- **Self-contained:** The format supports producing mapping files that provide sufficient information (via its description and reference fields) to enable its reader to understand, at a high-level, the functionality provided by the control being mapped along with references for additional information.

- **Scoring Assessment:** The format provides support for recording a score of the effectiveness of a security control's mitigation of an ATT&CK sub-technique, as well as an optional comment to support the scoring assessment.

In addition to the data format, a scoring rubric enables recording the category of ATT&CK coverage provided by a control (protect, detect, and/or response) along with an assessment of its effectiveness (Minimal, Partial, or Significant). Guidance on the scoring factors considered when assigning a score and additional related documentation is available in the project repository.

Mapping CLI Tool

A forward-looking approach was taken, resulting in the development of a CLI tool that facilitates the mapping process and will allow the Center for Threat-Informed Defense to sustain the Azure platform mappings over time. This will also enable further expanding the mapping of security stacks to other platforms based on the Center's priorities and community collaboration. This Python-based tool provides the following functionality:

- **Syntax Validation:** Supports validating mapping file syntax, ensuring their conformity to the data format specification and accurate references of the sub-techniques from the ATT&CK Enterprise matrix.
- **Visualization:** Supports producing the ATT&CK Navigator layers and Markdown Summary visualizations from mapping files.
- **Querying:** Supports querying the mapping data by various fields, such as ATT&CK tactic or sub-technique, score category (protect, detect, respond), score value (Minimal, Partial, Significant), etc. An example is shown in the figure below:

Get details on Security Stack Mappings – Azure

```
./mapping_cli.py list_scores --category Respond --level Sub-technique --width 50
```

No.	Name	Mapping File	Sub-technique	Score	Comments
1	Azure AD Identity Protection	Azure/IdentityProtection.yaml	T1078.002 Domain Accounts	Partial	Response Type: Containment Supports risk detection responses such as blocking a user's access and enforcing MFA. These responses contain the impact of this sub-technique but do not eradicate it (by forcing a password reset).
2	Azure AD Identity Protection	Azure/IdentityProtection.yaml	T1078.004 Cloud Accounts	Significant	Response Type: Eradication Supports blocking and resetting the user's credentials based on the detection of a risky user/sign-in manually and also supports automation via its user and sign-in risk policies.
3	Azure AD Identity Protection	Azure/IdentityProtection.yaml	T1110.003 Password Spraying	Significant	Response Type: Eradication Supports blocking and resetting the user's credentials based on the detection of a risky user/sign-in (such as Password Spray attack) manually and also supports automation via its user and sign-in risk policies.
4	Azure AD Identity Protection	Azure/IdentityProtection.yaml	T1606.002 SAML Tokens	Significant	Response Type: Eradication Supports blocking and resetting the user's credentials based on the detection of a risky user/sign-in manually and also supports automation via its user and sign-in risk policies.
5	Continuous Access Evaluation	Azure/ContinuousAccessEvaluation.yaml	T1078.004 Cloud Accounts	Partial	Security controls like Azure AD Identity Protection can raise a user's risk level asynchronously after they have used a valid account to access organizational data. This CAE control can respond to this change in the users risky state to terminate the user's access within minutes or enforce an additional authentication method such as MFA. This mitigates the impact of an adversary using a valid account. This is control only forces the user to re-authenticate and doesn't resolve the usage of a valid account (i.e. password change) and is therefore a containment type of response.

Total Rows: 5

ADVERSARY EMULATION LIBRARY

ADVERSARY EMULATION LIBRARY

Philosophy of Adversary Emulation Plans

Adversary emulation plans are based on known-adversary behaviors and designed to empower red teams to manually emulate a specific threat actor in order to test and evaluate defensive capabilities from a threat-informed perspective. This approach empowers defenders to operationalize cyber threat intelligence to better understand and combat real-world adversaries. Rather than focusing on static signatures, these intelligence-driven emulation plans provide a repeatable means to test and tune defensive capabilities and products against the evolving Tactics, Techniques, and Procedures (TTPs) of threat actors and malware.

Adversary Emulation Background

Adversary emulation enables organizations to view their security through the eyes of a cyber adversary with the goal of improving defenses across the adversary's lifecycle. As defenders this expands our attention and focus beyond just the final actions of the adversary achieving their operational objective to rather understand and appreciate every distinct behavior (that could have been detected and/or mitigated) leading up to that point.

- Each emulation plan is rooted in intelligence reports and other artifacts that capture and describe breaches and campaigns publicly attributed to a specific named threat actor.

- To develop each plan, we research and model each threat actor, focusing not only on what they do (ex: gather credentials from victims) but also how (using what specific tools/utilities/commands?) and when (during what stage of a breach?).

- We then develop emulation content that mimics the underlying behaviors utilized by the threat actor (i.e. not an exact representation, rather capturing the pertinent elements that accurately generate appropriate test telemetry for defenders).

This approach results in nuanced emulation plans, each capturing unique scenarios and perspectives that we can leverage as threat-informed defenders.

Getting Started with Adversary Emulation Plans

- As is the case with traditional red teaming and penetration testing, adversary emulation is a specific style of offensive assessment performed to help us test and tune our defenses. In this case, our objective is to operationalize cyber threat intelligence describing behaviors observed in specific campaigns or malware samples. From this intelligence, we select and execute a subset of behaviors (and their variations) to assess our defenses from the perspective of the specific threat.

- As described in the next section, each emulation plan captures specific threat scenarios. These scenarios can be executed end-to-end, or individual behaviors can be tested. Organizations can also choose to further customize the scenarios and/or behaviors within each emulation plan to better fit their specific environment, priorities, or to be shaped by additional intelligence.

- In summary, each emulation plan should be perceived as input to an offensive assessment/red team. The content can be used as strict instructions to follow, or as just a starting point to be built upon and personalized.

Emulation Plan Structure

Detailed documentation for our emulation plan structure can be found in GitHub.

- Each emulation plan focuses on a specific named threat actor. The README of each individual plan provides a curated summary of available cyber threat intelligence, composed of an intelligence overview of the actor (describing who they target, how, and why where possible) as well as the scope of their activity (i.e. breadth of techniques and malware used).

- All presented information is cited back to relevant publicly available cyber threat intelligence and communicated and annotated via ATT&CK.

- Within each emulation plan, the operational flow provides a high-level summary of the captured scenario(s). These scenarios will vary based on the adversary and available intelligence, but typically follow a sequential progression of how the actor breaches then works towards achieving their operational objectives within a victim environment (espionage, data/system destruction, etc.).

- The content to execute the scenario(s) is broken down into step-by-step procedures provided in both human and machine-readable formats. Scenarios can be executed end-to-end or as individual tests. The human-readable formats provide additional relevant background where possible as well as any setup prerequisites, while the machine-readable format is designed to be programmatically parsed (ex: read, reformatted, and ingested into an automated agent, such as CALDERA and/or breach simulation frameworks).

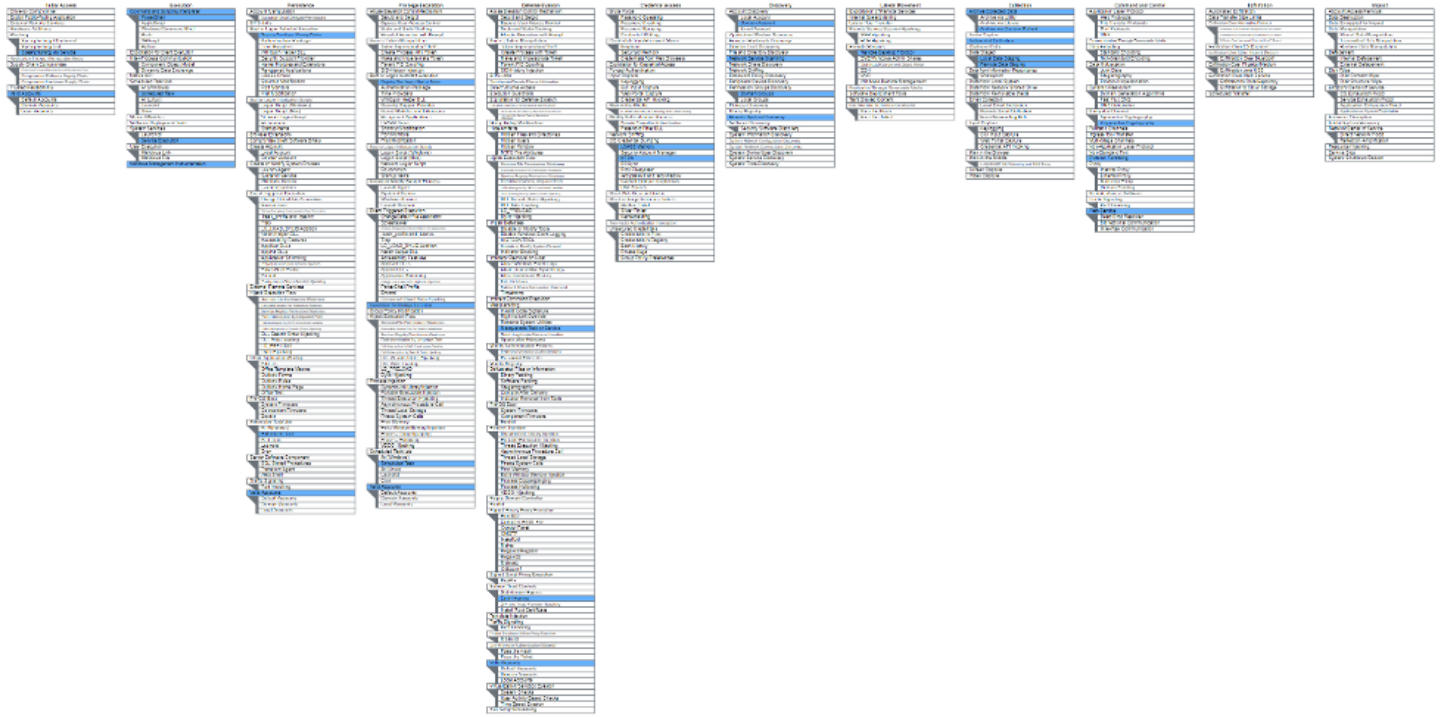
FIN6

The Center for Threat-Informed Defense's addition of FIN6 to the public library of adversary emulation plans is designed to enable red teams and cyber defenders to systematically test their defenders based on real-world FIN6 adversary Tactics, Techniques, and Procedures (TTP's).

- **FIN6** is a cybercrime 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.

Intelligence Summary

The FIN6 intelligence summary outlines 15 publicly available sources to describe FIN6 and motivations, objectives, and observed target industries.



FIN 6 Operations Flow

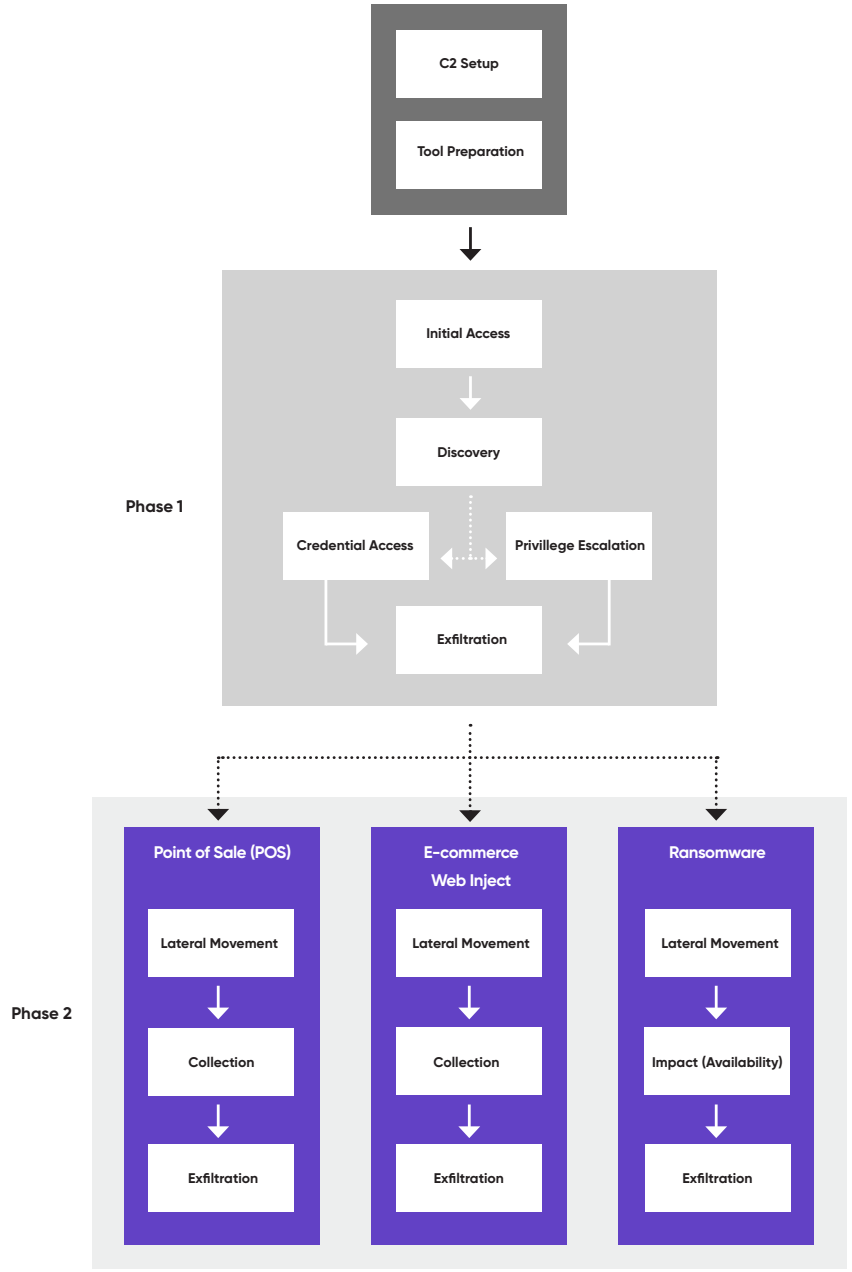
The FIN6 Operations Flow chains techniques together into a logical flow of the major steps that commonly occur across FIN6 operations (two major phases).

Phase 1

This phase consists of the initial access and placement objectives, ensuring that FIN6 is postured for follow-on actions in Phase 2. Specifically Phase 1 includes: Initial Access, Discovery, Privilege, Escalation, and Exfiltration of Phase 1 data.

Phase 2

This phase consists of the specific objectives of a given operation. FIN6 operations have typically been directed against:, Point of Sale (POS) systems, e-commerce web-facing systems, and deploying ransomware to enterprise environments. The emulation plan provides three corresponding scenarios within Phase 2, one for each of these major areas of focus.



FIN6 Emulation Plan

The emulation plan is a human-readable, step-by-step/ command-by-command implementation of the adversary's TTPs organized into phases defined in the Operations Flow. The FIN6 Emulation Plan is organized into two phases.

Phase 1

Described the techniques reported to have been used by FIN6 to achieve initial access but ultimately leaves initial access to the interpretation of the individual analyst. The emulation plan then walks the practitioner through discovery, privilege, escalation, collection, and exfiltration TTPs reported ot have been used by FIN6.

Phase 2

Described lateral movement, persistence, collection, and exfiltration in 3 distinct scenarios as defined in the Operations Flow. The scenarios can be executed end-to-end, or individual behaviors can be tested.

Each Emulation Plan includes a YAML representation, providing a machine-readable version of the overall plan that mirrors the human-readable plan. The FIN6 YAML file includes all steps, commands, and syntax for both Phase 1 and Phase 2.

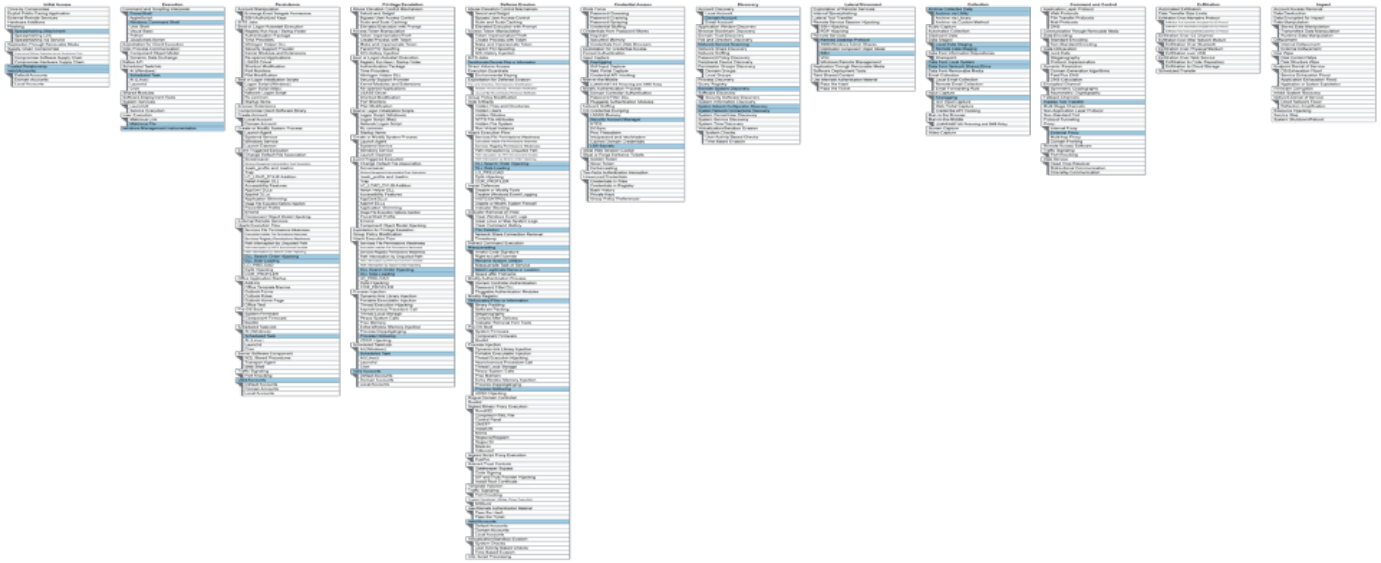
menuPass

The Center for Threat-Informed Defense's addition of menuPass to the public library of adversary emulation plans is designed to enable red teams and cyber defenders to systematically test their defenders based on real-world menuPass adversary Tactics, Techniques, and Procedures (TTP's).

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

Intelligence Summary

The menuPass intelligence summary outlines 32 publicly available sources, motivations, objectives, and observed target industries. The Intelligence Summary describes the typical menuPass operation along with their publicly attributed TTP's and their most often used software, mapped to MITRE ATT&CK. Additionally, the Intelligence Summary provides ATT&CK Navigation Layers, illustrating menuPass interactive TTP's from the TTP's associated with each of their Software platforms.



menuPass Operations Flow

The menuPass Operations Flow chains techniques together into a logical flow of the major steps that commonly occur across menuPass operations (two major scenarios).

Scenario 1: MSP Subscriber Networks

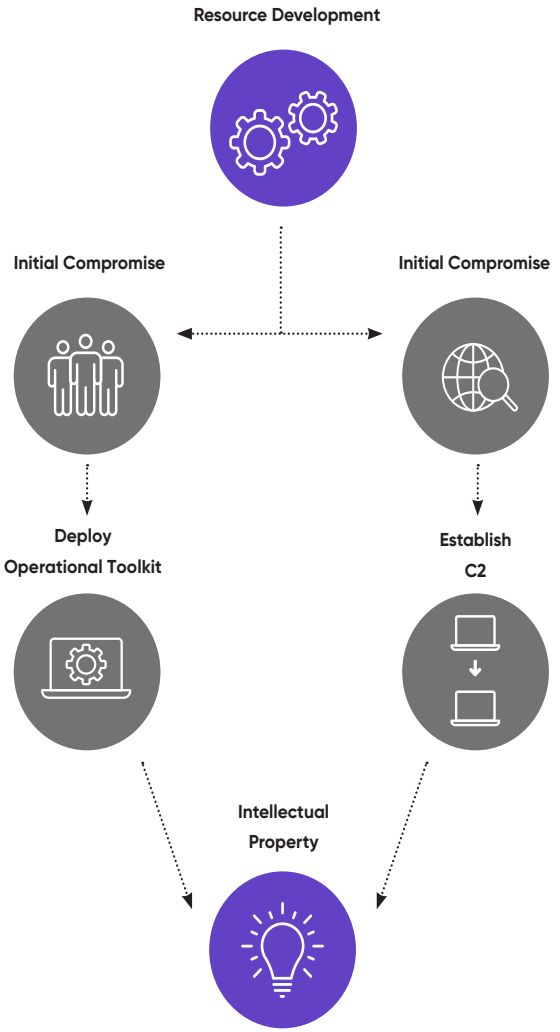
This scenario is designed to emulate activity attributed to menuPass that is specific to the group's efforts targeting MSP subscriber networks. The intent of this scenario is to assess your organization's ability to protect, detect, and defend against execution, tool ingress, discovery, credential access, lateral movement, persistence, collection, and exfiltration.

Scenario 2: IP Theft

This scenario is designed to emulate activity attributed to menuPass that uses a command-and-contol framework in support off the operational goal of intellectual property theft. This scenario is intended to assess your organization's ability to protect, detect, and defend against execution, discovery, privilege escalation, credential access, lateral movement, exfiltration, C2, and persistence using a command-and-control framework.

menuPass Emulation Plan

The menuPass YAML file provides a machine-readable version of the overall plan that mirrors the human-readable plan. The YAML is used to facilitate programmatic use of the plan content, either with custom-developed tools or off-the-shelf breach and attack simulation (BAS) tools. In addition, the CALDERA team has authored a plugin that converts the YAML file to a CALDERA adversary, enabling users to easily emulate the menuPass adversary. The plugin is available with the next CALDERA release.



All Currently Available Plans

All currently available adversary emulation plans are listed below with corresponding links. We thank the MITRE Engenuity ATT&CK Evaluations team for their contributions.

FIN6 is thought to be a financially motivated cyber-crime group. The group has aggressively targeted and compromised high-volume POS systems in the hospitality and retail sectors since at least 2015.

APT29 is thought to be an organized and well-resourced cyber threat actor whose collection objectives appear to align with the interests of the Russian Federation. The group is reported to have been operating as early as 2008 and may have logged operational successes as recently as 2020.

menuPass is thought to be motivated by collection objectives that align with Chinese national interests.4 6 12 14 17 The group's targeting is consistent with China's strategic objectives as stated in the Five-Year Plan (FYP) / Made in China 2025 Plan.4 While most of the group's targets have been located in the United States and Japan, the group has also been linked to intrusions in at least 12 other countries.

Carbanak is a threat group that has been found to target banks. It also refers to malware of the same name (Carbanak). It is sometimes referred to as FIN7, but these appear to be two groups using the same Carbanak malware and are therefore tracked separately.

FIN7 appears to be a financially motivated threat group that has primarily targeted the U.S. retail, restaurant, and hospitality sectors since mid-2015. They often use point-of-sale malware. A portion of FIN7 was operated out of a front company called Combi Security. FIN7 is sometimes referred to as Carbanak Group, but these appear to be two groups using the same Carbanak malware and are therefore tracked separately.

Access to the full library

CALDERA PATHFINDER

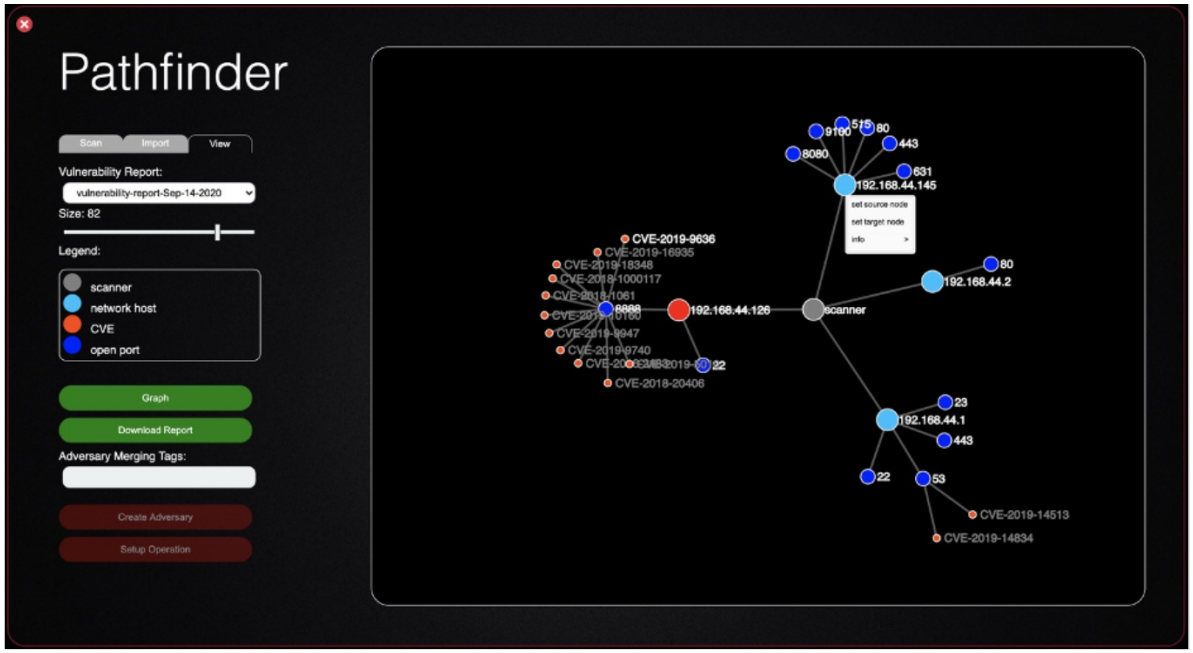
CALDERA PATHFINDER

Pathfinder is a CALDERA plugin developed by the Center for Threat-Informed Defense. This open-source CALDERA plugin helps users understand what a vulnerability exposes to an adversary, and what potential destructive paths an adversary could take within the network as a result of those vulnerabilities.

Functionality

- First, Pathfinder conducts a scan of a targeted network using the default scanner NMAP (additional scanners can be added). Scan results are then ingested into CALDERA's knowledge store, either from the scan initiated through the user interface, or imported separately by a file upload, where it can then map out the network.
- Next, Pathfinder is able to combine the information from the scan with the power of a breach and attack simulation tool in order to map out potential attack paths within the target network. These paths can be acted upon, and the user can run an operation on the target network exploiting the vulnerabilities to discover even more information about the state of the network.

Pathfinder contains two parsers for network scan results: one for NMAP and one for SIEMENS AG's SiESTA. Additional parsers can also be added.



Using CALDERA Pathfinder

1. Install CALDERA https://github.com/mitre/caldera
2. Clone down the pathfinder repo into the caldera/plugins folder with this command:
    a. git clone https://github.com/center-for-threat-informed-defense/caldera_pathfinder.git pathfinder —recursive
3. Add pathfinder to enabled plugins list in the caldera conf file for own environment.

Get details on Pathfinder plug in

ADOPTING PROJECTS WITH THE CENTER: AFFILIATES PROGRAM

COMING SOON

COMING SOON

ADOPTING PROJECTS WITH THE CENTER: AFFILIATES PROGRAM

Organizations that belong to the Affiliates Program showcase the latest R&D resources developed by the Center for Threat-Informed Defense. It's a community-driven program for organizations that strive to support the advancement of the state of the art, and the state of the practice in threat-informed defense. Affiliates are recognized as industry leaders that proactively move the community forward towards a safer world.
The Affiliates program offers:

- Publication of case studies on their adoption experience and lessons learned
- Participation in educational events that facilitate the ability for the community to adopt a threat-informed defense approach to security
- Leadership in promoting the value and impact of the freely available Center projects available to the community

The Affiliate Program offers a mix of communication and networking opportunities to showcase leadership in the threat-informed defense community. Depending on the Affiliate tier, as outlined in the Affiliate Program Benefits Matrix on page 42, Affiliates are entitled to access the following benefits:

R&D Adoption Spotlights

Custom, co-branded case studies showcase leadership in threat-informed defense approach to security.

A package of marketing initiatives: Co-promote the case studies to the community:

- Dedicated email to our data base of ATT&CK practitioners (25,000+)
- Banner ad in our bi-weekly Quick ATT&CK Facts Newsletter
- One ATT&CK Subject Matter Expert video interview

Shareable Digital Badge

Identify that your organization is an Affiliate of the Center for Threat Informed Defense

- Leverage the power of social media to promote your leadership in the community
- Share this badge to inform prospects and customers that your company is plugged into the Center – the global focal–point for threat-informed defense

To learn more about the Affiliates community or how to become an Affiliate, we're happy to contact you.

COMING SOON

Corporate logo featured on the Center's website

The Center's website is quickly becoming a go-to resource for the global cyber defense community

- Highlight your company's active role in threat-informed defense
- https://ctid.mitre-engenuity.org/

Virtual Booth at Threat-Informed Defense Summit

Showcase your company and your solutions to attendees that are all prequalified as practitioners of ATT&CK and threat-informed defense

Pre-release access to Center R&D with gold tier

Gives Affiliates a critical head-start to incorporate Center R&D into your product or service offerings

- Receive access approximately two weeks prior to the public release
- Incorporate cutting-edge R&D solutions before your competition
- Be poised to announce your adoption of R&D the day we release it to the world

Annual Affiliates Technical Workshop

Receive complimentary tickets to our annual technical workshop

- Hear directly from MITRE subject matter experts responsible for the cutting-edge R&D about the latest advances in ATT&CK and threat-informed defense
- Use this benefit to ensure that your team has the latest insights on ATT&CK, threat-informed defense and the Center's R&D program

MITRE ATT&CK Defender™ (MAD) Subscriptions

Access training and certification subscriptions at no cost

- Earn any of the badges and certifications offered
- Ensure that your key team members have the latest and greatest insights provided by our MAD professors

To learn more about the Affiliates community or how to become an Affiliate, we're happy to contact you.

COMING SOON

Affiliate Program Benefit (12 months)	Affiliate Tier	
	Gold	Silver
Affiliates technical workshop (seats)	4	2
MAD training & certification (bundle)	5	3
Pre-release access to Center R&D projects	✓	
Digital Badges (social media – ready)	✓	✓
Logo promotion on Center website	✓	✓
R&D Adoption Spotlight	5	3
Two-page PDF (co-branded use case w. custom quote)	✓	✓
Corporate logo on website project page	✓	✓
One dedicated email to ATT&CK users (25,000 +/-)	✓	
One ad in newsletter in top or bottom banner (25,000 +/- ATT&CK users)	✓	
One ATT&CK subject matter expert video interview (5min.)	✓	✓
"Booth" at virtual Threat-Informed Defense Summit in December 2021	✓	
COST in USD	$50,000	$30,000

MITRE ENGENUITY | Center for Threat Informed Defense

About the Center for Threat-Informed Defense

The Center is a non-profit, privately funded research and development organization operated by MITRE Engenuity. The Center's mission is to advance the state of the art and the state of the practice in threat informed defense globally. Comprised of participant organizations from around the globe with highly sophisticated security teams, the Center builds on MITRE ATT&CK , an important foundation for threat-informed defense used by security teams and vendors in their enterprise security operations. Because the Center operates for the public good, outputs of its research and development are available publicly and for the benefit of all.

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

For more information:

Center for Threat-Informed Defense
ctid@mitre-engenuity.org