The Center for Threat-Informed Defense

A privately funded research and development organization focused on advancing the state of the art and the state of the practice in threat-informed defense.

Serves as the focal point for the Threat-Informed Defense Community, driving applied research and advanced development to improve cyber defense at scale for the global community.

Brings together the best security teams from around the world to identify and solve the most-pressing problems facing cyber defenders.
Collaborating to change the game

Membership is:
- Highly-sophisticated
- Global & cross-sector
- Non-governmental
- Committed to collaborative R&D in the public interest

Members as of October 2021
The center by the numbers

Mission: 1
Members: 29
Months Old: 24

Ideas in Pipeline: 39
Projects Underway: 3
Published Projects: 13
Our Focus: R&D

The outputs of all Center R&D projects are made freely-available globally
Our Values Drive our Research

- Openness
- Flexibility
- Collaboration
- Leadership

Idea Market: Ideas submitted to the idea market
Selection: Based on priorities, insights, and funding
Research: Member-funded projects assigned to dedicated MITRE experts
Completed Project: R&D projects outputs released freely-available
Problem

Defenders struggle to integrate their organization’s local knowledge of adversaries and their TTPs with the public ATT&CK knowledge base.

Solution

Build an 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.

Impact

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

Allow users to explore, create, annotate, and share extensions of MITRE ATT&CK.

© 2021 MITRE Engenuity. Approved for public release.
Demo

① **Annotating a Technique**
I want to take notes on a technique to allow me to collaborate more effectively within my organization's threat intel team.

② **Adding new intel mappings**
I just received a threat report and I want to update my knowledge base to reflect its contents.

③ **Adding a Group not tracked by MITRE ATT&CK**
I want to track a group that is not tracked by MITRE ATT&CK in the same way that I track groups that are included in MITRE ATT&CK.
What do we mean by “Extension?”

New Objects Are Added

Existing objects within ATT&CK are updated

Use Case: Expanded Group Tracking
Fill in gaps in open-source reporting by creating new groups. Map new groups to new and existing techniques.

Use Case: Red Teaming
Create red team techniques and track them using tooling developed for ATT&CK.
• Workbench is the cornerstone for your local infrastructure. You decide which modules you want, and which are irrelevant.
• You can extend your local knowledge base with new or updated techniques, tactics, groups, and software.
Sharing ATT&CK Extensions

The official ATT&CK knowledge base is disseminated as a collection

ISACs may share collections containing their extensions as well

Individual Workbench users can also publish collections

The Workbench provides the means to both import, create, and export collections

MITRE ATT&CK on GitHub
- Enterprise v9.0
- Enterprise v8.2
- Enterprise v8.1

ACME ISAC on GitHub
- ACME Groups v1.0
- ACME Software v1.0

Exampleuser on GitHub
- Hello World v1.0

Exampleuser’s ATT&CK Workbench
- Exporting
- Importing
How do I get the ATT&CK Workbench?

Start here: https://ctid.mitre-engenuity.org/our-work/attack-workbench/

We are interested in your questions and feedback. GitHub Issues are always appreciated or email us ctid@mitre-engenuity.org

Help advance threat-informed defense

Spread the word to help us increase the impact of our work.

Use our work and tell us about it.

Share your ideas and they may become part of the research program.

Advance the research program by joining the Center.