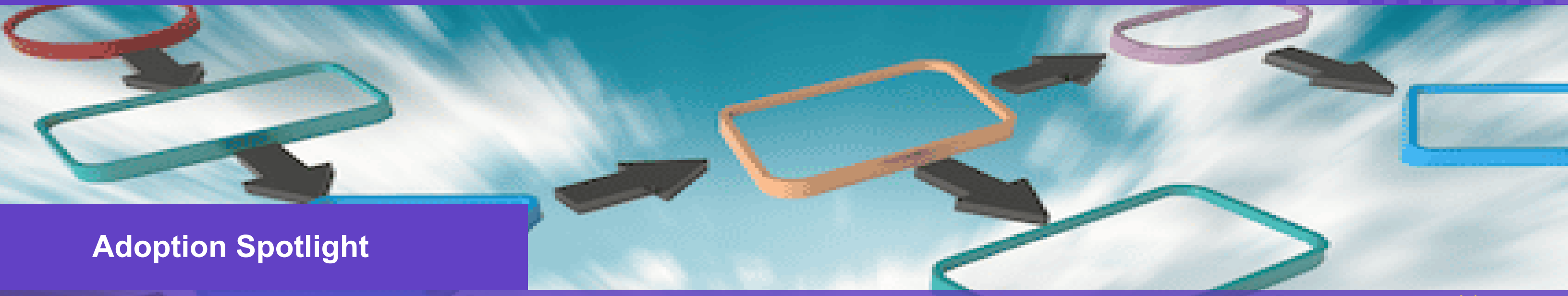
MITRE ENGENUITY. Center for Threat Informed Defense

FORGE ANVILOGIC



Adoption Spotlight

Anvilogic Adopts Attack Flow

GOLD Center for Threat-Informed Defense AFFILIATE MITRE ENGENUITY

R&D Project Introduction

Attack Flow enables defenders to move from tracking individual adversary behaviors to tracking the sequences of behaviors that adversaries employ in an attack. By looking at combinations of behaviors, defenders learn the relationships between them: how some techniques set up other techniques, or how adversaries handle uncertainty and recover from failure. The project supports a wide variety of use cases: from blue team to red team, from manual analysis to autonomous response, and from front-line worker to the C-suite. Attack Flow provides a common language and toolset for describing complex, adversarial behavior.

About Anvilogic

Anvilogic is a Palo Alto-based SaaS cybersecurity company founded by security veterans. Anvilogic's AI-driven SOC Platform has unified the art of low-code/no-code threat detection, investigation and hunting across disparate data lakes without the need to centralize data, replace existing tools or deploy new agents.

Why Anvilogic Adopted Attack Flow

The Anvilogic Forge team's threat detection approach is based on the Pyramid of Pain principles but starts with adversary behaviors. By leveraging the Attack Flow project, Anvilogic has created a behavioral sequencing-based threat library to understand and track adversary actions toward their ultimate goals, allowing for more efficient and high-efficacy threat detection.

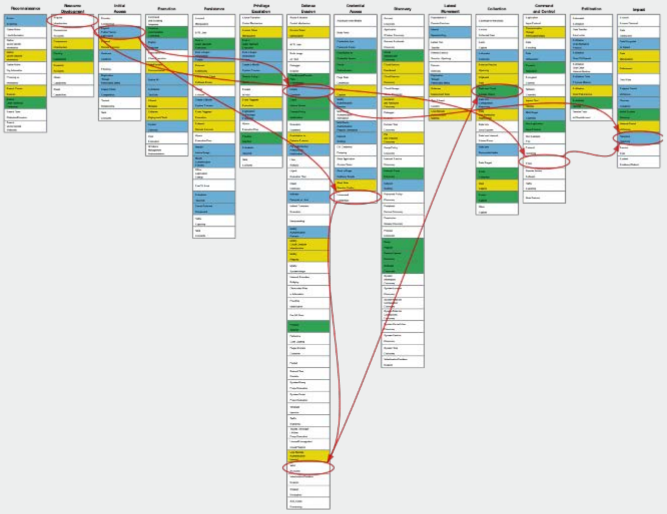
How Anvilogic Uses Attack Flow

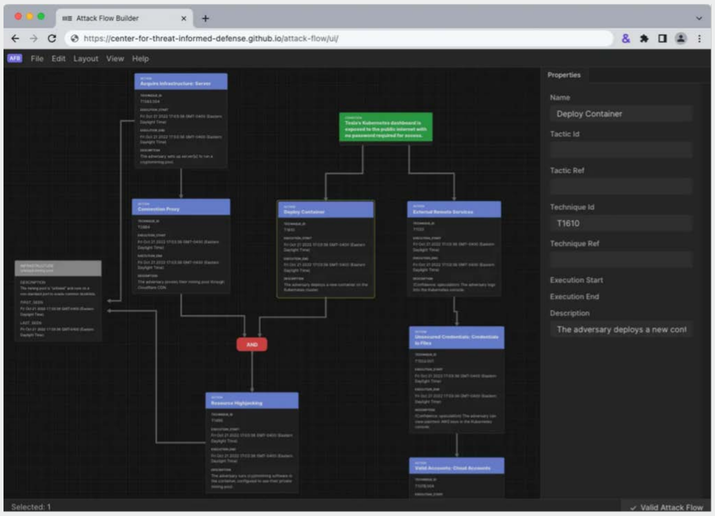
The Anvilogic Forge uses the Attack Flow project to improve its threat detection strategy and provide security operation teams with the ability to easily deploy high-efficacy detections. The focus is to create a comprehensive threat research database that will track adversary campaigns and emulate adversary activity at the technique level. Guided by the Pyramid of Pain, this project will help to show that an effective threat detection strategy needs to be established from the apex and will require an understanding of adversarial behaviors from their tactics, techniques, and procedures. This sequencing will help guide atomic-level identifiers and better determine attack patterns. The intelligence gathered from the research can identify trends in adversary activity and attacks across different verticals. Anvilogic's integration of Attack Flow will help to enhance collaboration between cyber teams and facilitate the prioritization of threat analytics development and detection validation through red team attack simulations.

> “ *At Anvilogic, The Forge is a specialized team dedicated to protecting our trusted clients while contributing to our peers in the security industry by empowering them with actionable threat research and detective capabilities to combat the threats we continue to face. We leverage and extend research and development projects, such as Attack Flow from the MITRE Engenuity Center for Threat-Informed Defense, to more accurately comprehend, track, and simulate threats.*
>
> - Kevin Gonzalez, Head of Security, Anvilogic ”

About the Research: Attack Flow

Attack Flow is a data model with supporting tooling and examples for describing sequences of adversary behaviors. Attack flows help 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, overlayed on ATT&CK Navigator layers to understand defensive coverage, and create a foundation for intel-driven adversary emulation plans.




Attack Flow Builder
https://center-for-threat-informed-defense.github.io/attack-flow/ui/
AFB
File
Edit
Layout
View
Help
Acquire Infrastructure: Server
Tesla's Kubernetes dashboard is exposed to the public internet with no password required for access.
Connection Proxy
Deploy Container
External Remote Services
AND
Resource Hijacking
Unsecured Credentials: Credentials In Files
Valid Accounts: Cloud Accounts
Properties
Name
Deploy Container
Tactic Id
Tactic Ref
Technique Id
T1610
Technique Ref
Execution Start
Execution End
Description
The adversary deploys a new cont
Selected: 1
✓ Valid Attack Flow

Attack Flow enables cybersecurity professionals to better understand how adversaries operate, the impact of threats on their organization, and how to most effectively improve their defensive posture to address those threats. Threat intelligence analysts, security operations, incident response teams, red team members, and risk assessors are some of the groups that can benefit from Attack Flow. This specification facilitates sharing of threat intelligence, communicating about risks, modeling efficacy of security controls, and more. The project includes tools to visualize attacks for the benefit of low-level analysis as well as communicating high-level principles to management.

Data Model

The Attack Flow data model is based on STIX 2.1 and includes the following entities:

- Attack Flow: The attack flow overall, can be a reference from other STIX objects.
- Attack Action: The execution of a particular technique, i.e., a discrete unit of adversary behavior.
- Attack Asset: Any object that is the subject or target of an action, can be technical or non-technical, actions typically either modify or depend upon the state of an asset.
- Attack Operator: The operator joins multiple attack paths together using Boolean logic.
- Attack Condition: This is a possible condition, outcome, or state that could occur, can be used to split flows based on success or failure of an action, or to further describe an action's results.

Use Case	Example
Tracking Threat Intelligence	Users track adversary behavior at the incident level, campaign level, or threat actor level.
Improving Defensive Posture	Determine coverage gaps and choke points to prioritize defenses.
Executive Communications	Assigning resources to attack flow actions and estimating the total financial impact of an attack.
Understanding Lessons Learned From an Incident	Analyzing assets, e.g., looking at how assets interacted with specific actions.
Building Realistic Adversary Emulation Scenarios	With access to Attack Flow specifications users could encode much more information.
Making Threat Hunting Visible	Guided investigative searches showcase the adversary tools & TTPs used, aiding threat hunting

Resources & How to Get Involved

Project resources available on GitHub include:

- Documentation: Resources to help users get the most our of Attack Flow including a getting started guide, example flows, and best practices guide.
- Developers: Guide on how to set up an environment to work on this code and the frequent tasks that you will need to perform if you would like to help create or maintain the code for Attack Flow, including the Attack Flow library (Python) and the Attack Flow builder (ECMAScript/Node.js).
- Attack Flow Builder: A free and open-source tool for creating, viewing, and editing Attack Flows

Here are a few ways for you to learn more and get started with Attack Flow:

1. Look at the corpus of example flows. The corpus is a great place to start learning about Attack Flow. If you're new to the industry, it's also a great way to familiarize yourself with some high-profile breaches!
2. Build your own flow. The Attack Flow Builder is a user-friendly tool that runs in your browser (no download required!) and will let start creating flows in just minutes.
3. Tell us what you think. Find us on LinkedIn or email us and let us know how you're using Attack Flow and what ideas you have to improve it.
4. Spread the word! Our goals is to get members of the community excited about Attack Flow and adopt it in their own work. Attack Flow is open source and royalty-free, so go ahead and share it to your professional network!

MITRE ENGENUITY. Center for Threat Informed Defense

For more information:

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

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.

FORGE ANVILOGIC

For more information:

Anvilogic
info@anvilogic.com
https://www.anvilogic.com/