

Attack Flow Training: 1 – Introduction to Attack Flow

May 14, 2025 • Brussels



Agenda

- 1 – Introduction to Attack Flow
- 2 – Tagging Techniques in Narrative Reports

Break

- 3 – Using Attack Flow Builder
- *Lightning Talk*
- 4 – Building An Attack Flow

Break

- *Lightning Talk*
- 5 – Attack Flow 3 Preview
- *Lightning Talk*
- 6 – Visualization



Mark Haase

Chief Engineer

MITRE Center for
Threat-Informed Defense

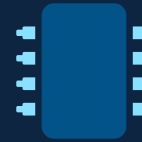
Background



Software Engineering



Cybersecurity



Machine Learning

Experience



MITRE: Threat-Informed Defense



Microsoft: Sovereign Clouds



DARPA: Dark Web & Internet Crime

System Owner/User Discovery (T1033)

```
adamp$ whoami
```

- He/him/his
- Lead of MITRE ATT&CK
- 16 years with MITRE
- Focused on threat intel and deception
- Past defender and CTI analyst
- Involved with ATT&CK since it was a spreadsheet with no &



Together, we are changing the rules of the game



+ MITRE

Membership is:

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

IT TAKES A VILLAGE



MITRE | Center for Threat
Informed Defense



<https://ctid.mitre.org>



<https://ctid.mitre.org>

Attack Flow – Motivation



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

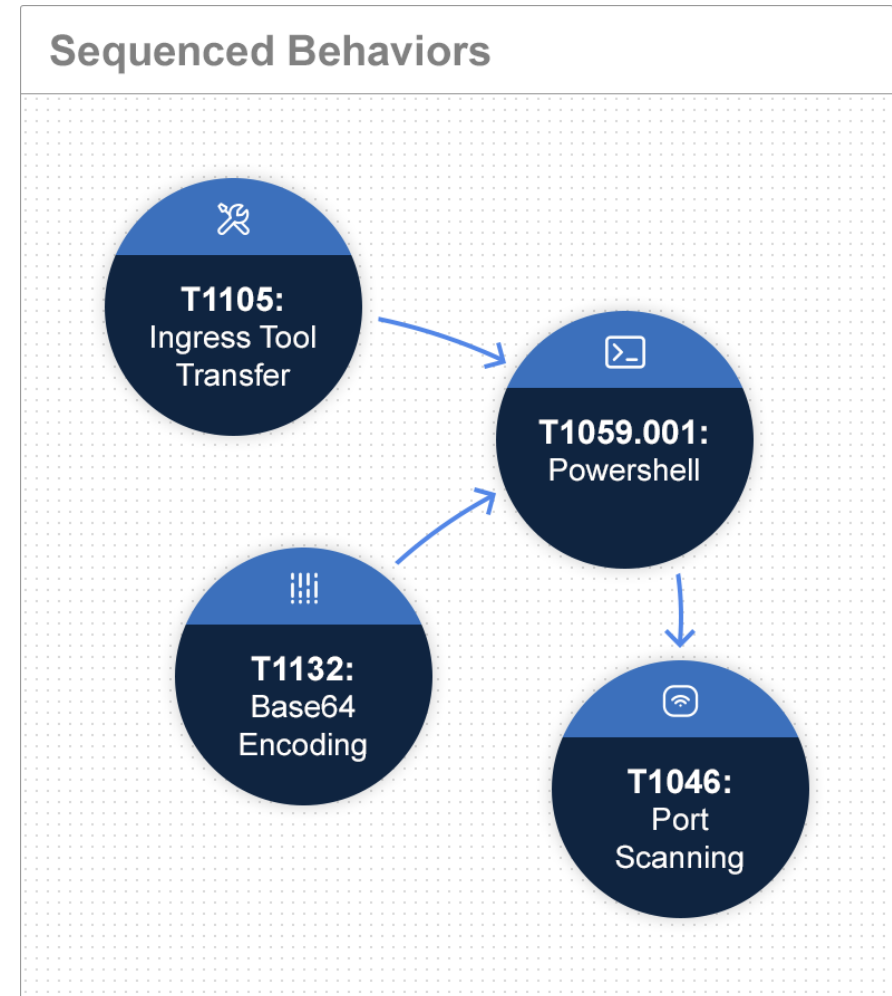
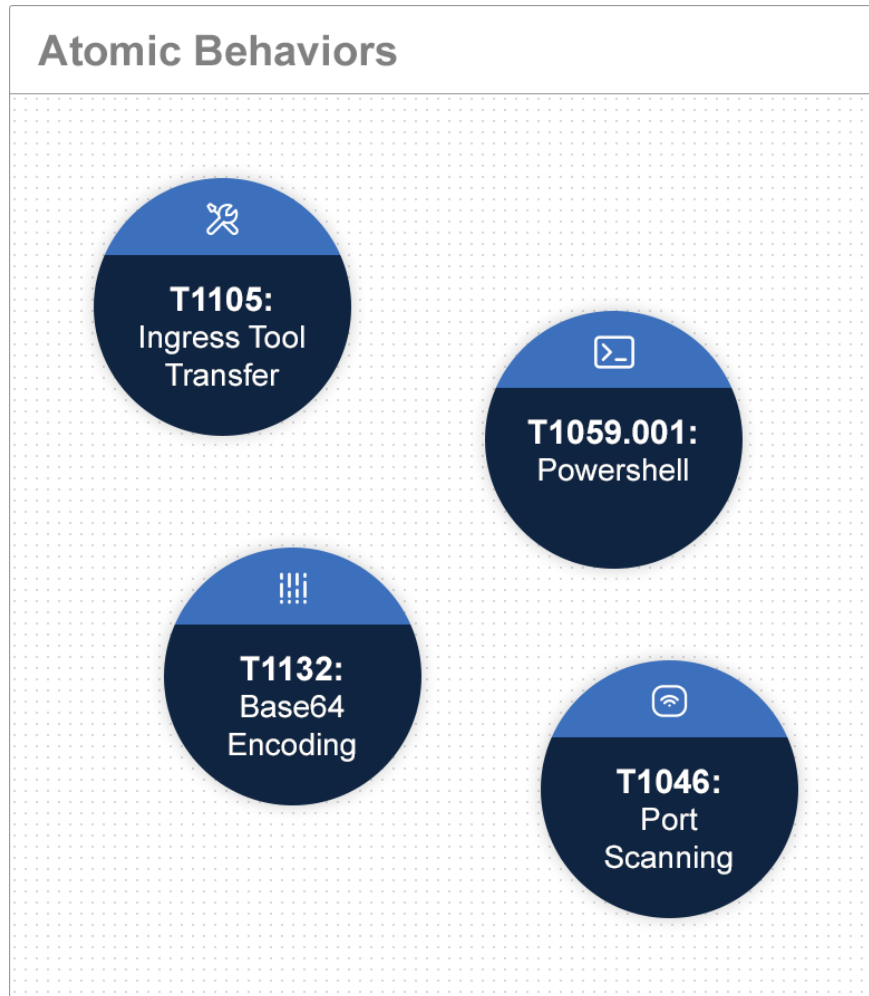
Create a language, and associated tooling, to describe flows of ATT&CK techniques and combine those flows into patterns of behavior.



IMPACT

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

Describing Adversary Behavior




Tesla Incident: Atomic Behaviors

Tesla cloud systems exploited by hackers to mine cryptocurrency

Updated: Researchers have discovered that Tesla's AWS cloud systems were compromised for the purpose of cryptojacking.

Written by **Charlie Osborne**, Contributor
Posted in Zero Day on February 20, 2018 | Topic: Security



Tesla

Tesla's cloud environment has been exploited by threat actors to mine cryptocurrencies, researchers have discovered.

On Tuesday, cloud security firm **RedLock** released the firm's **2018 Cloud Security Trends** report which documents the discovery of an unprotected Kubernetes console belonging to automaker Tesla.

The Kubernetes console is used to automate the deployment,

SECURITY

Hackers spent months inside a network and nobody noticed. Then a ransomware gang turned up

RELATED

- Best Java bootcamps: Where to learn Java (and why you should!)
- The 9 best cloud storage services: Cost, free storage, and features compared
- The best smart speakers: Should you go with Alexa, Siri, or Google Assistant?

Ad

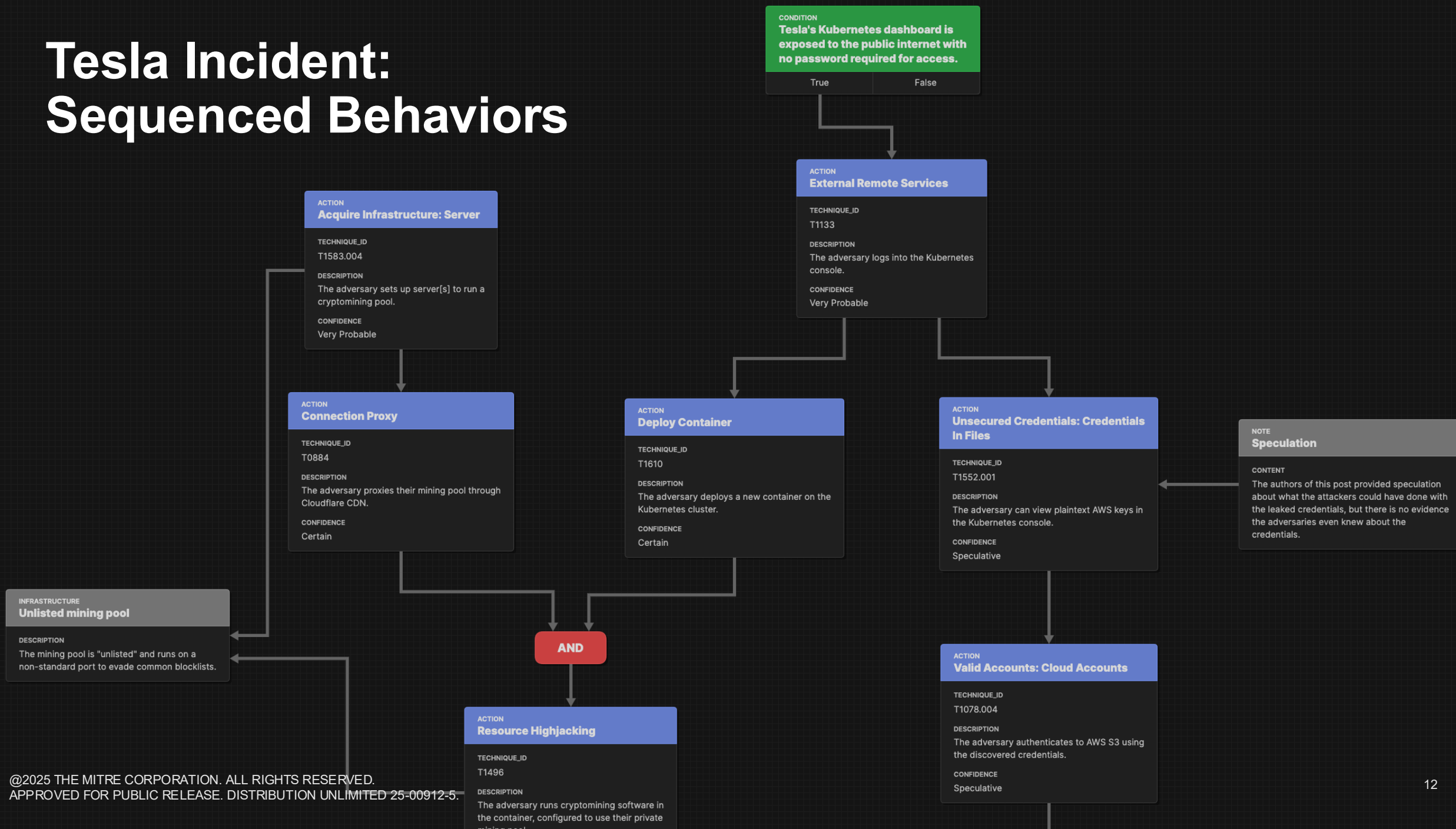
Secure employees at scale
Say goodbye to password spreadsheets

1Password [Learn More](#)



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques
Active Scanning (S)(3)	Acquire Infrastructure (O)(4)	Drive-by Compromise	Command and Scripting Interpreter (O)(8)	Account Manipulation (O)(5)	Abuse Elevation Control Mechanism (S)(4)	Abuse Elevation Control Mechanism (S)(4)	Adversary-in-the-Middle (O)(3)
Gather Victim Host Information (S)(4)	Compromise Accounts (O)(2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (S)(5)	Access Token Manipulation (S)(5)	Brute Force (O)(4)
Gather Victim Identity Information (S)(3)	Compromise Infrastructure (O)(4)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (O)(14)	Boot or Logon Autostart Execution (S)(14)	Boot or Logon Autostart Execution (S)(14)	Credentials from Password Stores (O)(5)
Gather Victim Network Information (S)(4)	Develop Capabilities (S)(4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (S)(5)	Boot or Logon Initialization Scripts (S)(5)	Build Image on Host	Exploitation for Credential Access
Gather Victim Org Information (S)(4)	Establish Accounts (O)(2)	Phishing (S)(8)	Inter-Process Communication (O)(3)	Browser Extensions	Create or Modify System Process (S)(4)	Decfuscate/Decode Files or Information	Forced Authentication
Phishing for Information (S)(2)	Obtain Capabilities (O)(4)	Replication Through Removable Media	Native API	Compromise Client Native API (T)(10)	Domain Policy Modification (S)(2)	Deploy Container	Forge Web Credentials (O)(2)
Search Closed Sources (S)(2)	Stage Capabilities (S)(5)	Supply Chain Compromise (O)(3)	Scheduled Task/Job (S)(4)	Create Account (S)(2)	Escape to Host	Direct Volume Access	Input Capture (O)(4)
Search Open Technical Databases (O)(4)		Trusted Relationship	Shared Modules	Create or Modify System Process (O)(4)	Event Triggered Execution (S)(15)	Domain Policy Modification (S)(2)	Modify Authentication Process (S)(5)
Search Open Websites/Domains (O)(2)		Valid Accounts (T)(4)	Software Deployment Tools	Event Triggered Execution (S)(15)	Exploitation for Privilege Escalation	Execution Guardrails (S)(1)	Multi-Factor Authentication Interception
Search Victim-Owned Websites			System Services (S)(2)	External Remote Services	Hijack Execution Flow (O)(12)	Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation
			User Execution (O)(3)	Hijack Execution Flow (S)(12)	Process Injection (S)(13)	File and Directory Permissions Modification (O)(2)	Network Sniffing
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (S)(5)	Hide Artifacts (S)(18)	OS Credential Dumping (S)(8)
				Modify Authentication Process (S)(5)	Valid Accounts (T)(4)	Hijack Execution Flow (O)(12)	Steal Application Access Token
				Office Application Startup (O)(4)		Impair Defenses (O)(9)	Steal or Forge Kerberos Tickets (S)(4)
				Pre-OS Boot (S)(5)		Indicator Removal on Host (S)(4)	Steal Web Session Cookie
				Scheduled Task/Job (O)(5)		Indirect Command Execution	Unsecured Credentials (O)(7)
				Server Software Component (S)(5)		Masquerading (S)(7)	
				Traffic Signaling (S)(1)		Modify Authentication Process (S)(5)	
				Valid Accounts (T)(4)		Modify Cloud Compute Infrastructure (S)(4)	

Tesla Incident: Sequenced Behaviors



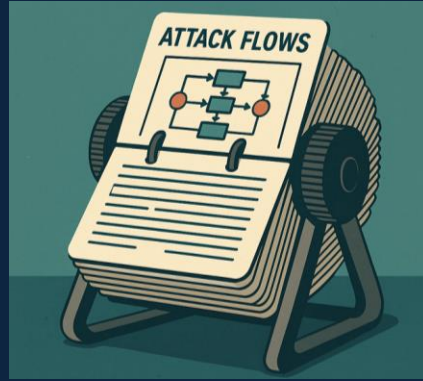
Attack Flow – What It Is

What's Included?



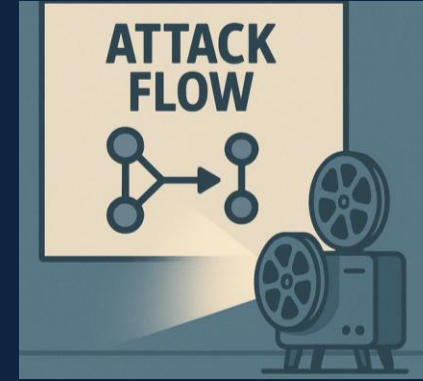
Attack Flow Builder

Web-based tool for creating, editing, and presenting flows.



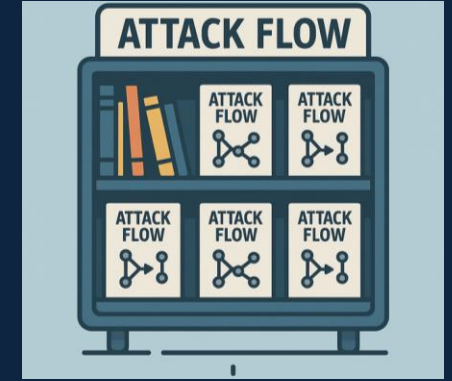
Flow Library

A collection of 34 example flows, useful for learning about Attack Flow, learning about breaches, and data mining.



Visualization

Tools for visualizing flows for different audiences and purposes.



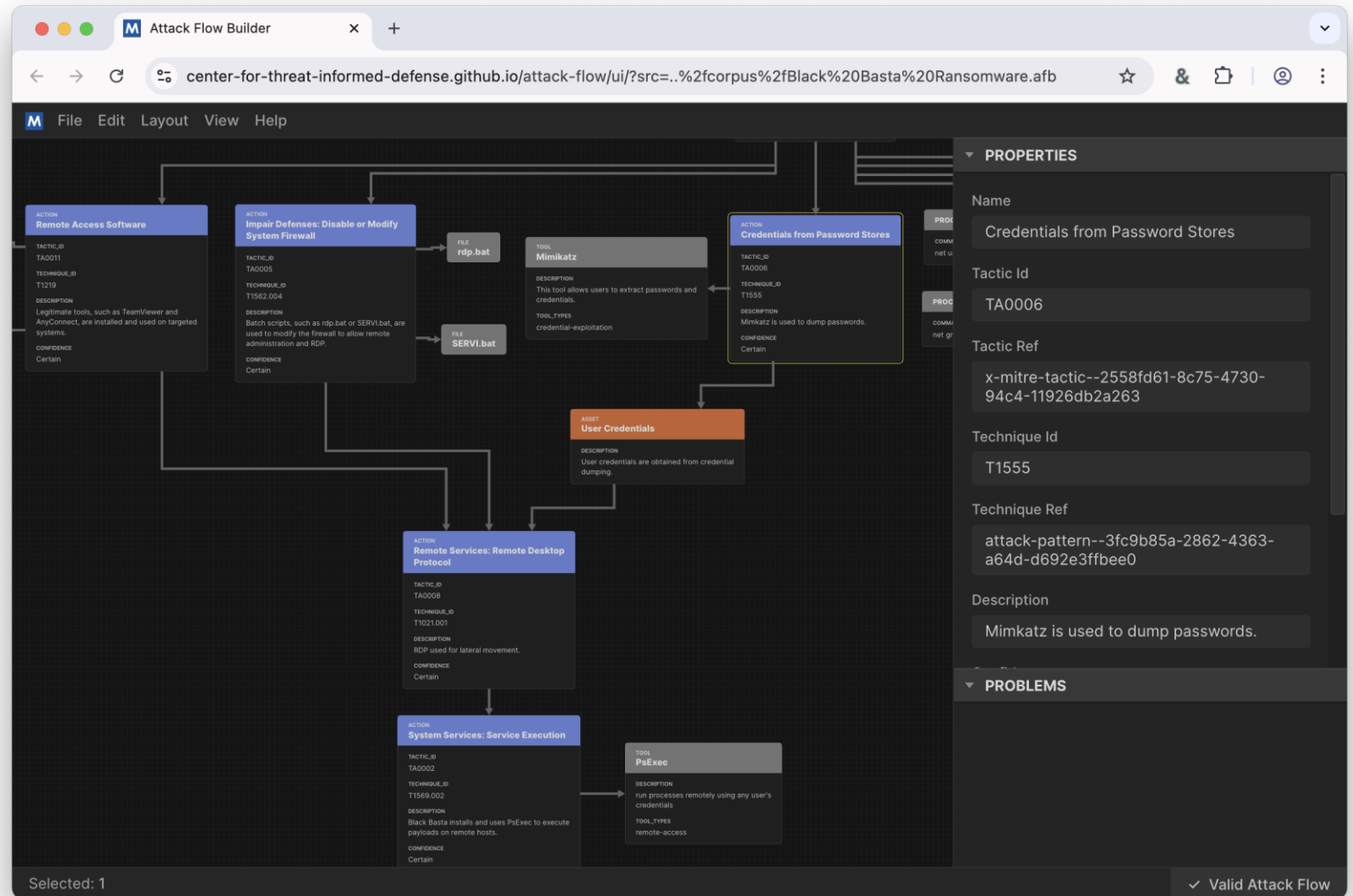
Documentation

User-friendly introduction to flow, easy access to the library and tools.

← Machine Readable (STIX) Data →

Attack Flow Builder

- Web-based tool for creating, editing, and presenting flows.
- Totally private: your flow data stays in the browser; we do not collect it or share it.



Flow Library

Example Flows — Attack Flow

center-for-threat-informed-defense.github.io/attack-flow/example_flows/

ATTACK FLOW V2.3.2

MITRE | Center for Threat Informed Defense

Search docs

CONTENTS

- Overview
- Introduction
- Example Flows
- Builder
- Visualization
- Language
- Best Practices Guide
- Developers
- Translation to OWL/RDF

List of Examples

Report	Authors	Description
Black Basta Ransomware Open: Attack Flow Builder Download: JSON GraphViz (PNG) Mermaid	Lauren Parker	Black Basta is a RaaS (Ransomware as a Service), written in C++, that has been in development since February 2022 and in active use since April 2022. Operators using Black Basta employ a double-extortion technique where they encrypt files on the target systems and demand payment for the decryption key while also threatening to leak the information if they are not paid.
CISA AA22-138B VMWare Workspace (Alt) Open: Attack Flow Builder	Lauren Parker	Alternative method used to exploit VMWare Workspace ONE Access

ON THIS PAGE

- Example Flows
- List of Examples

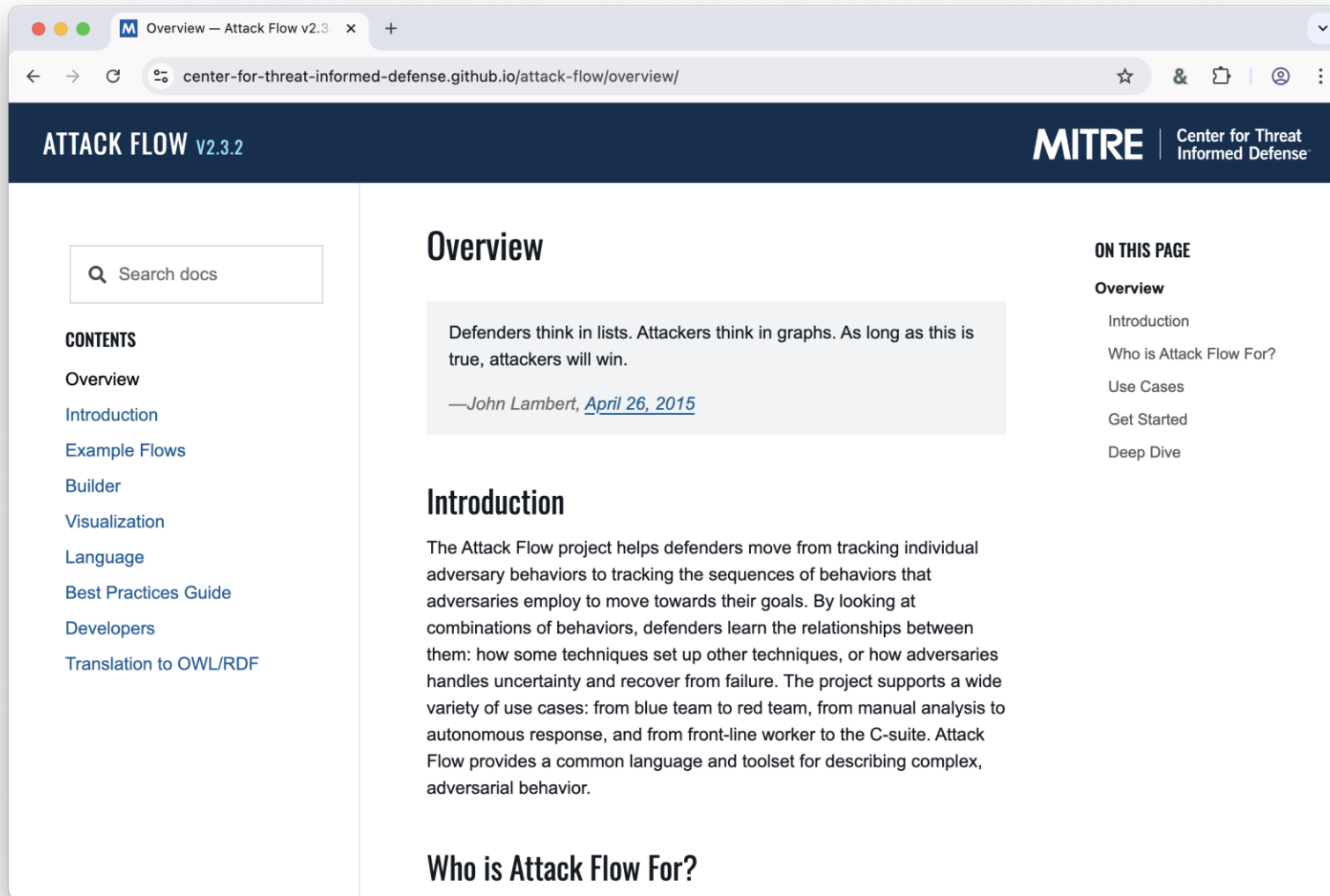
- A collection of 39 example flows, based mostly on real-world CTI.
- Each example contains references to source material.
- Open each example in Attack Flow Builder or download as image.

Visualization

- Extract data from an Attack Flow and generate insight by visualizing it in new ways.
- Automatically generate TTP tables or timeline views – a huge time saver.

The screenshot shows a web browser window with the URL `center-for-threat-informed-defense.github.io/attack-flow/visualization/`. The page header includes the MITRE logo and the text "Center for Threat Informed Defense". The main content area is titled "ATT&CK Navigator" and contains a description: "On this page, you can visualize an Attack Flow drawn on top of an ATT&CK Navigator matrix. First, choose a Navigator base layer or supply your own. Then upload an Attack Flow. Finally, preview and download the resulting visualization." Below the text is a large, complex matrix visualization. The matrix has columns for "about", "domain", and "platforms". The "domain" column is labeled "Enterprise ATT&CK v15". The "platforms" column lists various operating systems and environments: "Windows, Linux, macOS, Network, PaaS, Containers, Office 365, SaaS, Google Workspace, IaaS, Azure AD". The matrix itself is a grid of colored cells (blue, green, yellow, orange, red) representing different attack techniques. Red lines connect various cells across the matrix, illustrating an attack flow. On the left side of the page, there is a "CONTENTS" section with links to "Overview", "Introduction", "Example Flows", "Builder", "Visualization", "Language", "Best Practices Guide", "Developers", and "Translation to OWL/RDF". On the right side, there is a "ON THIS PAGE" section with links to "Visualization" and "ATT&CK Navigator". A "Full Screen" button is located at the bottom right of the matrix visualization.

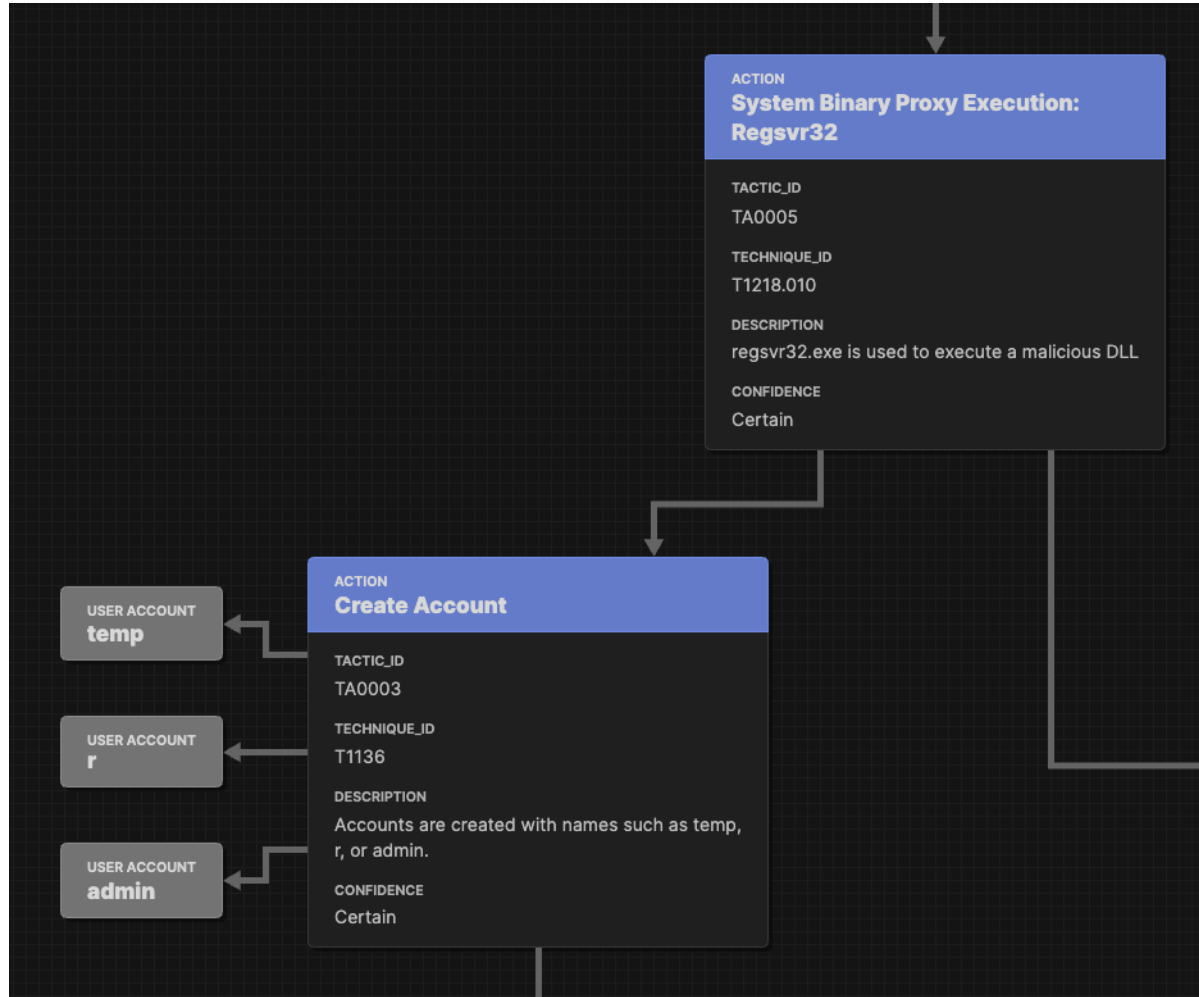
Documentation



- A complete guide to learning Attack Flow, starting from the ground up.
- Links to builder tool and visualizations.
- Usage guides for applying Attack Flow to specific job roles.

Attack Flow – Why It Matters

Less Ambiguous



- Prose reports contains lots of ambiguities, especially around the order of events, dependencies, and confidence levels.
- Attack Flow clarifies how an adversary works through a sequence of behaviors to reach their desired impact.
- Models how adversaries handle failure and recovery.

Visualize & Present

- Visualize attack paths and chokepoints.
- High quality presentations for a variety of audiences, including execs.
- Combine with other data to generate insights.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Phishing for Information	Acquire Access	Exploit Public-Facing Application	Software Deployment Tools	Valid Accounts	Valid Accounts	Valid Accounts	Harvested Credentials
Active Scanning	Acquire Infrastructure	Valid Accounts	Command and Scripting Interpreter	Server Software Component	Abuse Elevation Control Mechanism	Modify System Image	Harvesting in the Memory
Gather Victim Host Information	Compromise Accounts	Supply Chain Compromise	Inter-Process Communication	Create or Modify System Process	Exploitation for Privilege Escalation	Abuse Elevation Control Mechanism	Exploitation for Credential Access
Gather Victim Identity Information	Compromise Infrastructure	Drive-by Compromise	Windows Management Instrumentation	Pre-OS Boot	Create or Modify System Process	Exploitation for Defense Evasion	OS Credential Dumping
Gather Victim Network Information	Develop Capabilities	External Remote Services	Export/Import for Client Execution	Hijack Execution Flow	Escape to Host	Indicator Removal	Steal Application Access Token
Gather Victim Organization Information	Establish Accounts	Phishing	Scheduled Task/Job	External Remote Services	Hijack Execution Flow	Subvert Trust Controls	Steal or Forge Kerberos Tickets
Search Based Sources	Obtain Capabilities	Replication Through Removable Media	System Services	Modify Authentication Process	Scheduled Task/Job	System Binary Proxy Execution	Modify Authentication Process
Search Open Technical Databases	Stage Capabilities	Trusted Relationships	User Execution	Create Account	Domain or Tenant Policy Modification	Pre-OS Boot	Brute Force
Search Victim-Owned Web Sites		Hardware Additions	Container Administration Command	Implement Container Image	Process Injection	Hijack Execution Flow	Network Sniffing
Search Open Web Sites/Domains		Content Injection	Deploy Container	PaaS Jobs	Account Manipulation	Network Boundary Bridging	Force Authentication
			Serverless Execution	Browser Extensions	Boot or Logon Initialization Scripts	Modify Authentication Process	Steal Web Session Cookie
			Native API	Scheduled Task/Job	Event Triggered Execution	Impair Defenses	Multi-Factor Authentication Interception
			Cloud Administration Command	Office Application Startup	Access Token Manipulation	Debugger Evasion	Credentials from Password Stores
			Shared	Account	Boot or Logon	Plist File	Forge Web

Increase Automation

- Machine readable format is compatible with STIX; import and export IOCs easily.
- Visualization tools automatically create artifacts such as TTP tables or attack timelines.
- Open source: coders can build custom tooling.

```
{
  "type": "bundle",
  "id": "bundle--c4b15246-0bb4-49ca-8ec4-1cb8f3f1d451",
  "spec_version": "2.1",
  "created": "2025-04-25T15:41:36.746Z",
  "modified": "2025-04-25T15:41:36.746Z",
  "objects": [
    {
      "type": "extension-definition",
      "id": "extension-definition--fb9c968a-745b-4ade-9b25-c324172197f4",
      "spec_version": "2.1",
      "created": "2022-08-02T19:34:35.143Z",
      "modified": "2022-08-02T19:34:35.143Z",
      "name": "Attack Flow",
      "description": "Extends STIX 2.1 with features to create Attack Flows.",
      "created_by_ref": "identity--fb9c968a-745b-4ade-9b25-c324172197f4",
      "schema": "https://center-for-threat-informed-defense.github.io/attack-flow/",
      "version": "2.0.0",
      "extension_types": [
        "new-sdo"
      ],
      "external_references": [
        {
          "source_name": "Documentation",
          "description": "Documentation for Attack Flow",
          "url": "https://center-for-threat-informed-defense.github.io/attack-flow/"
        }
      ]
    }
  ]
}
```


Users and Use Cases

- **Cyber Threat Intelligence Analysts**

- Use Attack Flow to augment CTI reporting.
- Automatically generate generating artifacts, e.g. export STIX IOCs, generate timeline view, create TTP table, etc.

- **Incident Response**

- Use Attack Flow to document incident investigations as they develop.
- Confidence and notes feature to highlight what's known vs unknown and where to focus next.

- **Red Team**

- Plan red team scenarios based on known threat actors; start at high level and work down to procedure level.
- Record execution notes and use the flow to debrief blue team.

Who is using Attack Flow?

- Global community from US to EU to APAC.
- Multinational corporations and small business.
- Threat modelers, red teamers, CTI analysts, defenders.

Dave Johnson · 1st
Threat Intelligence Advisor @Feedly | Former FBI Analyst | Entrepren...
1mo · Edited · 🌐

I've been working on a secret ATT&CK Flow visualization tool 🤖

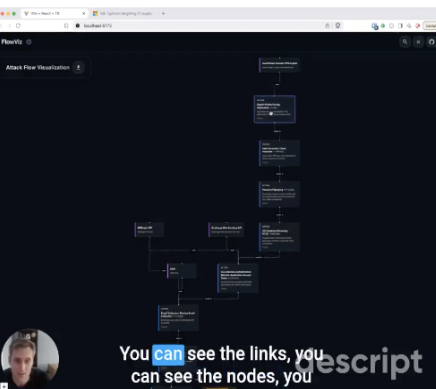
Why? Because it's winter in Wisconsin. 🌨️

What does it do? It generates a graph of attack procedures in a threat intelligence report automatically, so you get the gist of detailed reports much faster.

It will also generate STIX bundles so you can do adversary emulation in tools like MITRE Caldera. Or, you can export into an image file to use in a custom report or presentation.

Drop a comment down below if your interested! 🙌

#ThreatIntelligence #AdversaryEmulation #ATTACKFlow
#CyberSecurity



You can see the links, you can see the nodes, you can see the flow

You and 421 others · 112 comments · 19 reposts

Like · Comment · Repost · Send

Dewank Pant · 1st
Security@Amazon (Alexa AI Security Research) | Lea...
(edited) 1mo · ...

Dave Johnson This is great! would love to collaborate on this. Some thoughts: these attack flow details could also be linked to an exploit crafting agent to generate new attack variants, speeding up security testing. This would also be valuable for prompt testing tools (like Garak, and Pyrit), as jailbreak research papers come out every other day, this way we could feed in new papers and generate multiple attack variants to expand the test sets!

David Greenwood · 1st
I build products that make threat intelligence analysts go; "Wow! That's wh...
2mo · 🌐

txt2stix now supports automated Attack Flow extraction for MITRE ATT&CK references in reports.

I've update the last part of my blog post (linked in the post below) with some examples.

dogesec
1,765 followers
2mo · Edited · 🌐

For a long time, I, like many of you, have been tagging detection content with ATT&CK Techniques.

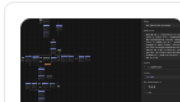
Sometimes, ashamedly, I tout full detection coverage for a particular threat. I show off the ATT&CK Navigator highlighting how all the detections cover the ATT&CK Techniques an intel team has discovered an adversary to use

The reality is, although this captures a lot of information, and is often better-than-nothing, it still lacks a key component – time (or flow!) of techniques.

Many people incorrectly read the ATT&CK Matrix as a flow. They assume the flow of an attack moves from left to right. This is incorrect in many instances where an attacker jumps backwards and forwards in their attempts to achieve an objective.

The point is this; the ATT&CK Matrix alone does not provide enough to describe how an adversary might work and that's where Attack Flows come in.

<https://lnkd.in/ezaPN4rB>



Beyond the ATT&CK Matrix: How to Build Dynamic Attack Flows with STIX
dogesec.com

Gert-Jan Bruggink · 1st
Founder & CEO, Venation | Proven Systems for Smarter Decisions.
Visit my website
2mo · Edited · 🌐

I've been successfully modeling threat scenarios for over 7 years. Here's how I recently updated my 'system' with Attack Flow:

I believe that cybersecurity needs a support function that helps understand variables (threats) that drive risk + support explicit decision making on what to do about it.

To do this right, you need a system.

Most teams understand WHY you need to do this. Some even have figured out HOW. Today, I'll show you WHAT you can do right now to integrate this in your daily workflow using Attack Flow.

Copy it into your internal procedures and create your own!

Let's make this week count!

Gert-Jan

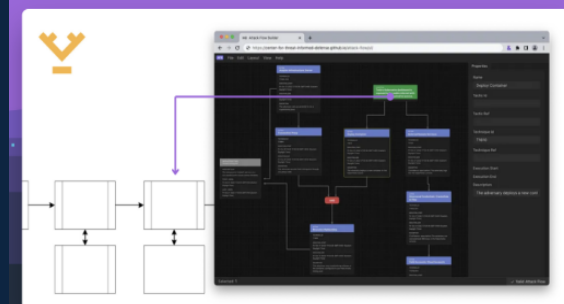
If you want systems directly in your mailbox, join our newsletter for the complete ones:

GO here: <https://lnkd.in/eWwxc5bQ>

Found my content useful?

Share it with your network & follow [Gert-Jan Bruggink](#) and [Venation](#) for more. 💜

#CyberSecurity #RiskManagement #ThreatModeling #ThreatScenarios



End of Section 1