

Attack Flow Training: 3 – Using Attack Flow Builder

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

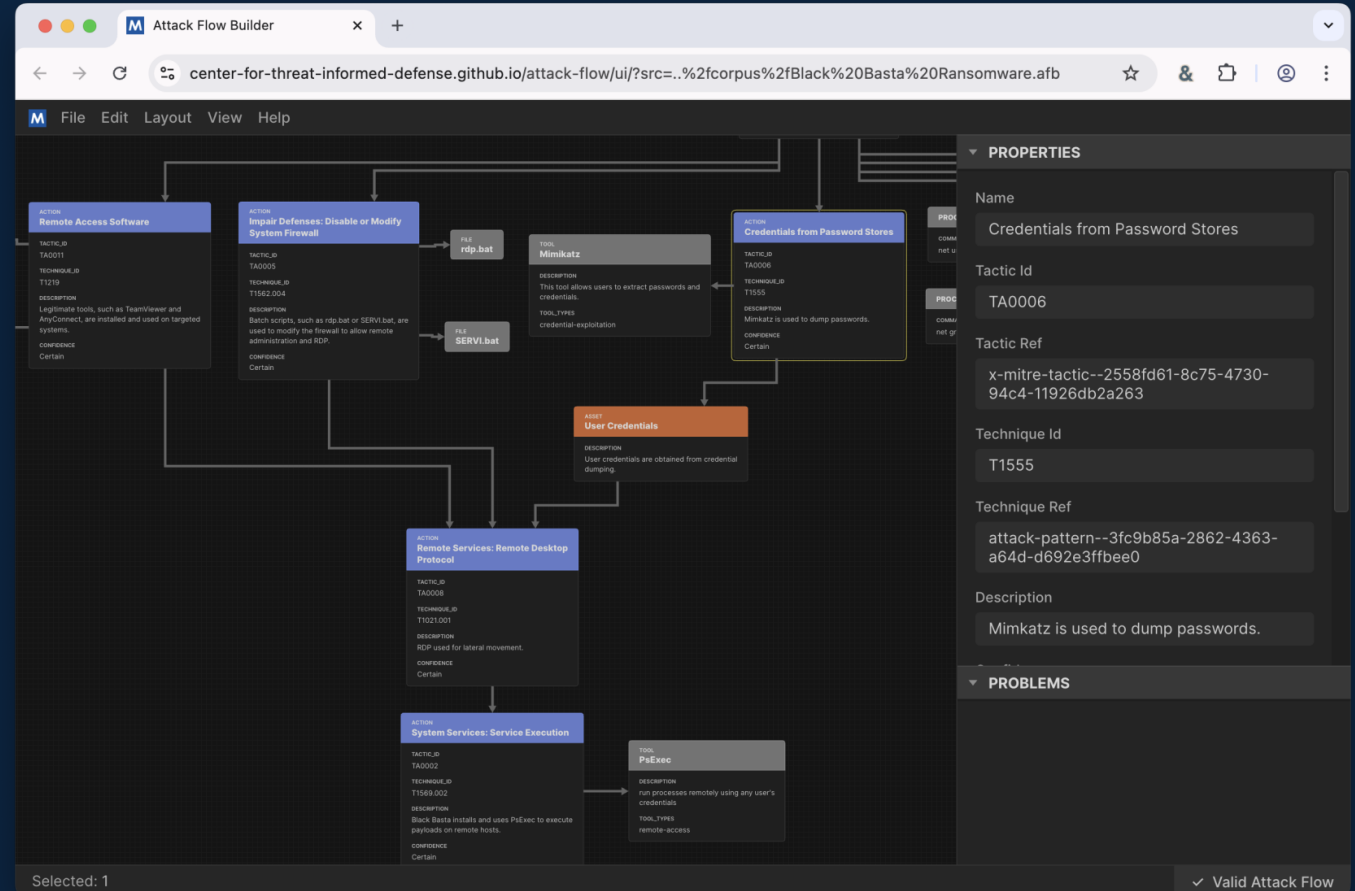
Break

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

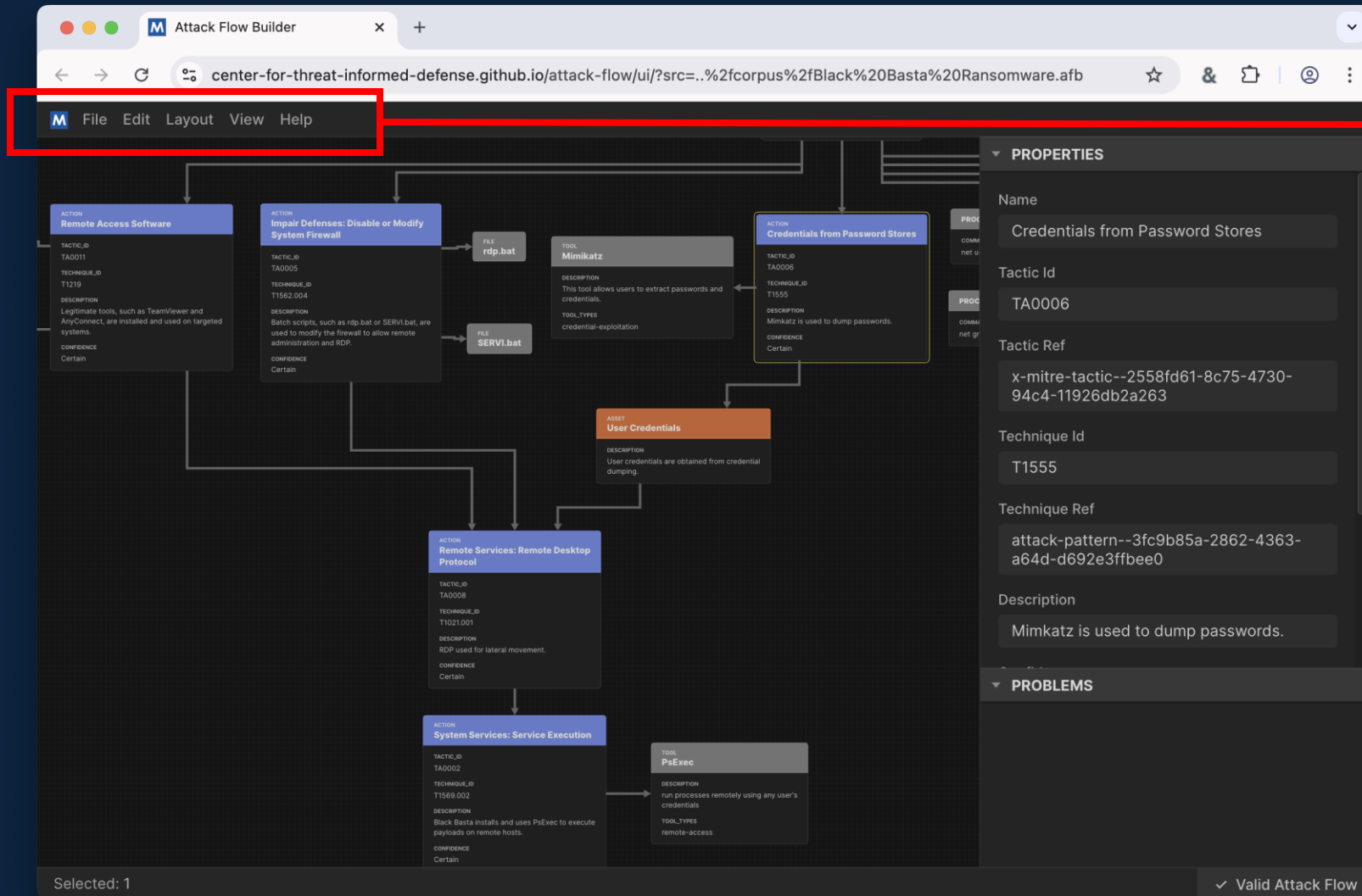
Overview of Attack Flow Builder

Web App for Diagramming Attacks

- Open source, web-based tool.
- Similar to Visio: create nodes (boxes) and connect with edges (lines).
- Create, edit, export, and present flows.
- Private: flow data stays in the browser. We do not collect or share it.
- Can be hosted at your organization for additional privacy & assurance.



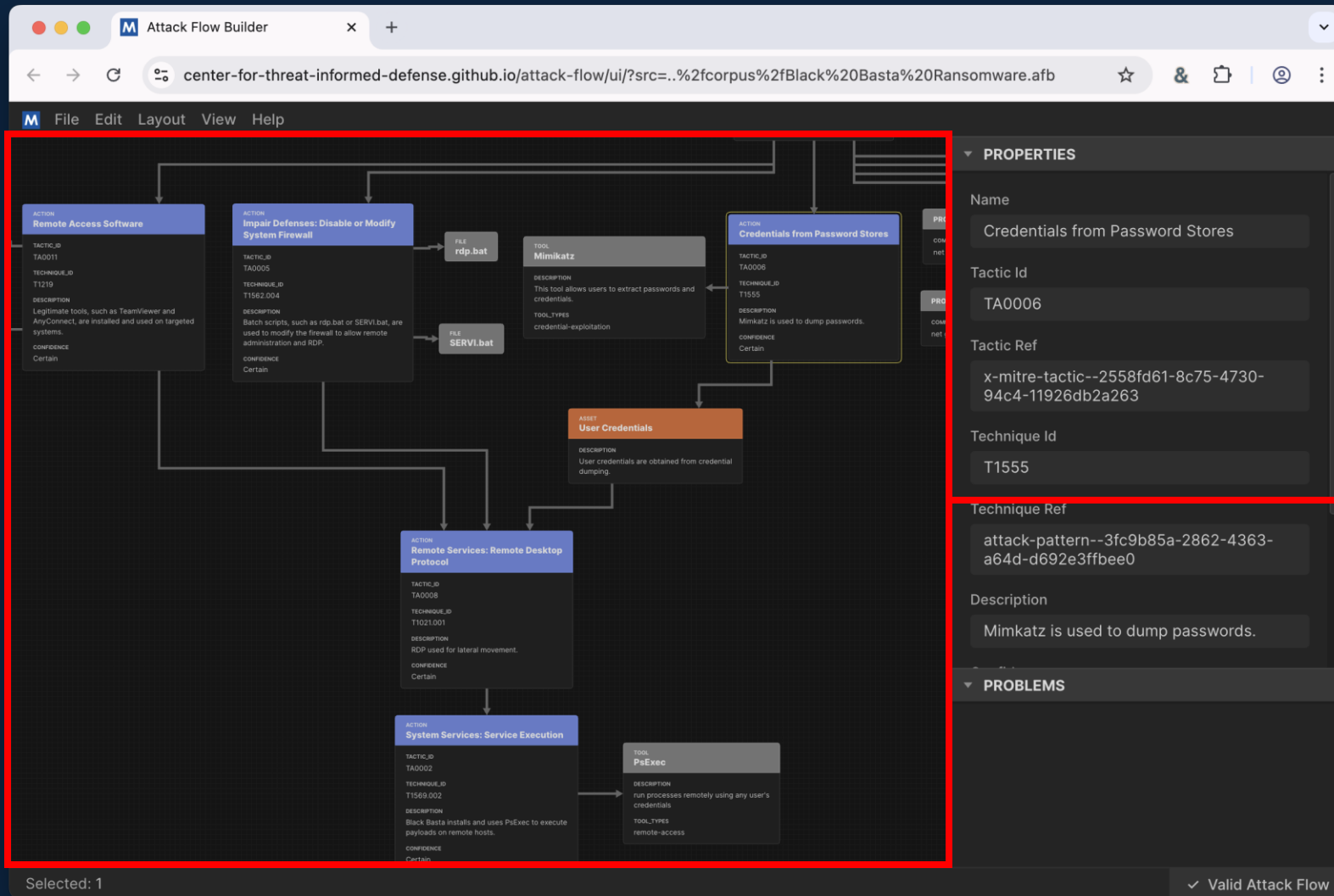
Web App for Diagramming Attacks



Menu bar: new flow, open flow, export, copy/paste, etc.

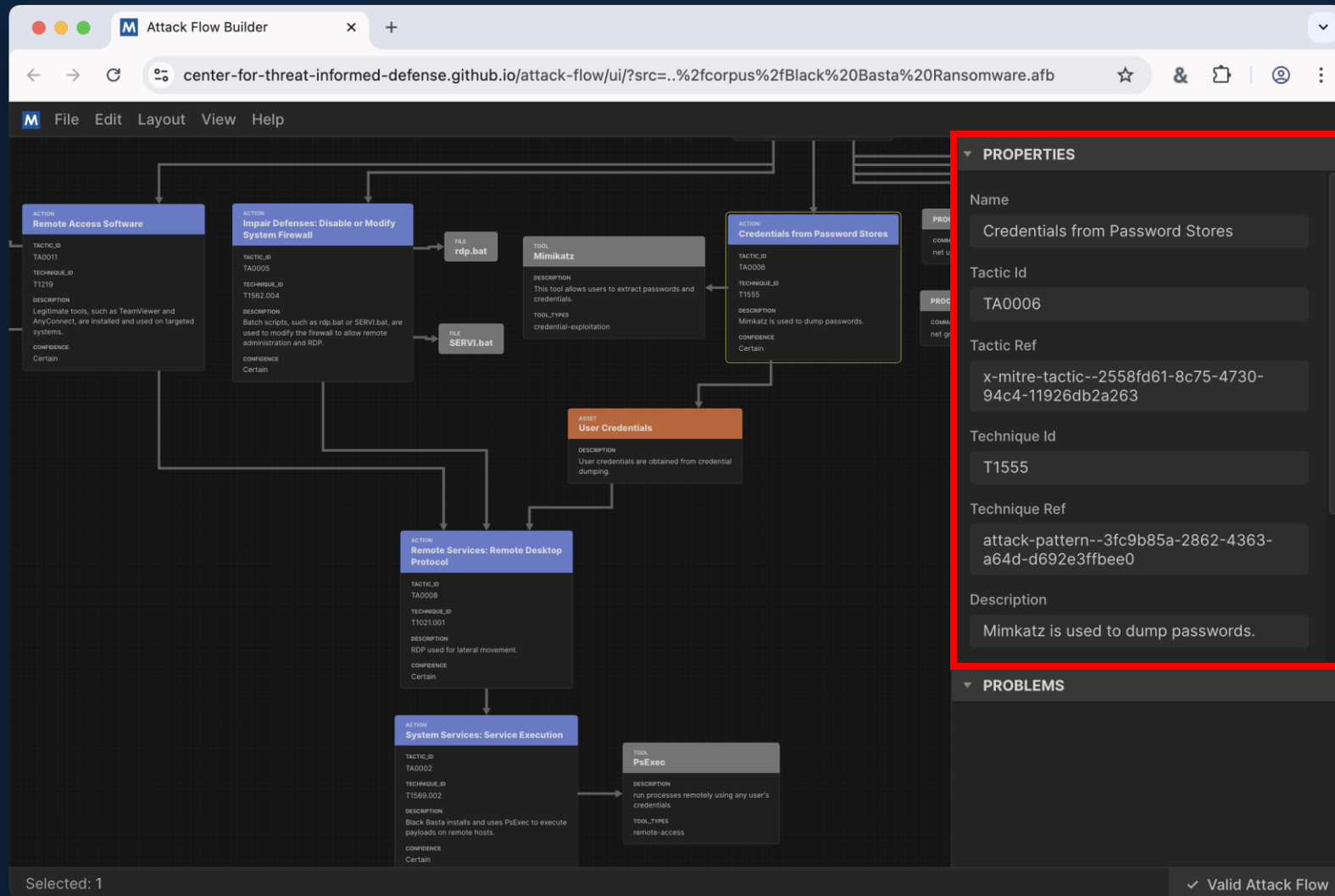
Select: Menu bar → Edit → Create → ... to get started with adding items

Web App for Diagramming Attacks



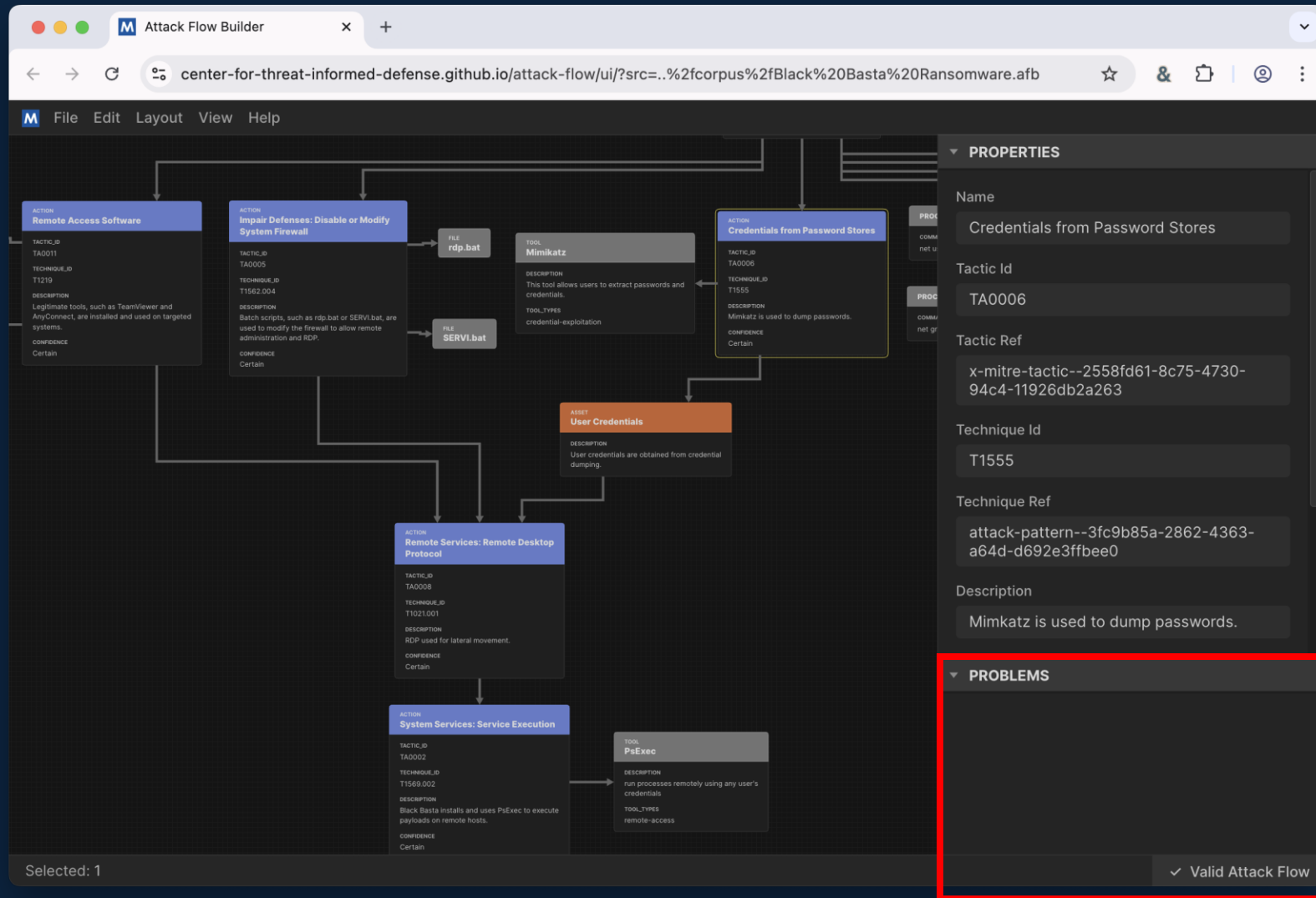
Canvas: this is where you draw the diagram, the nodes, and the edges.

Web App for Diagramming Attacks



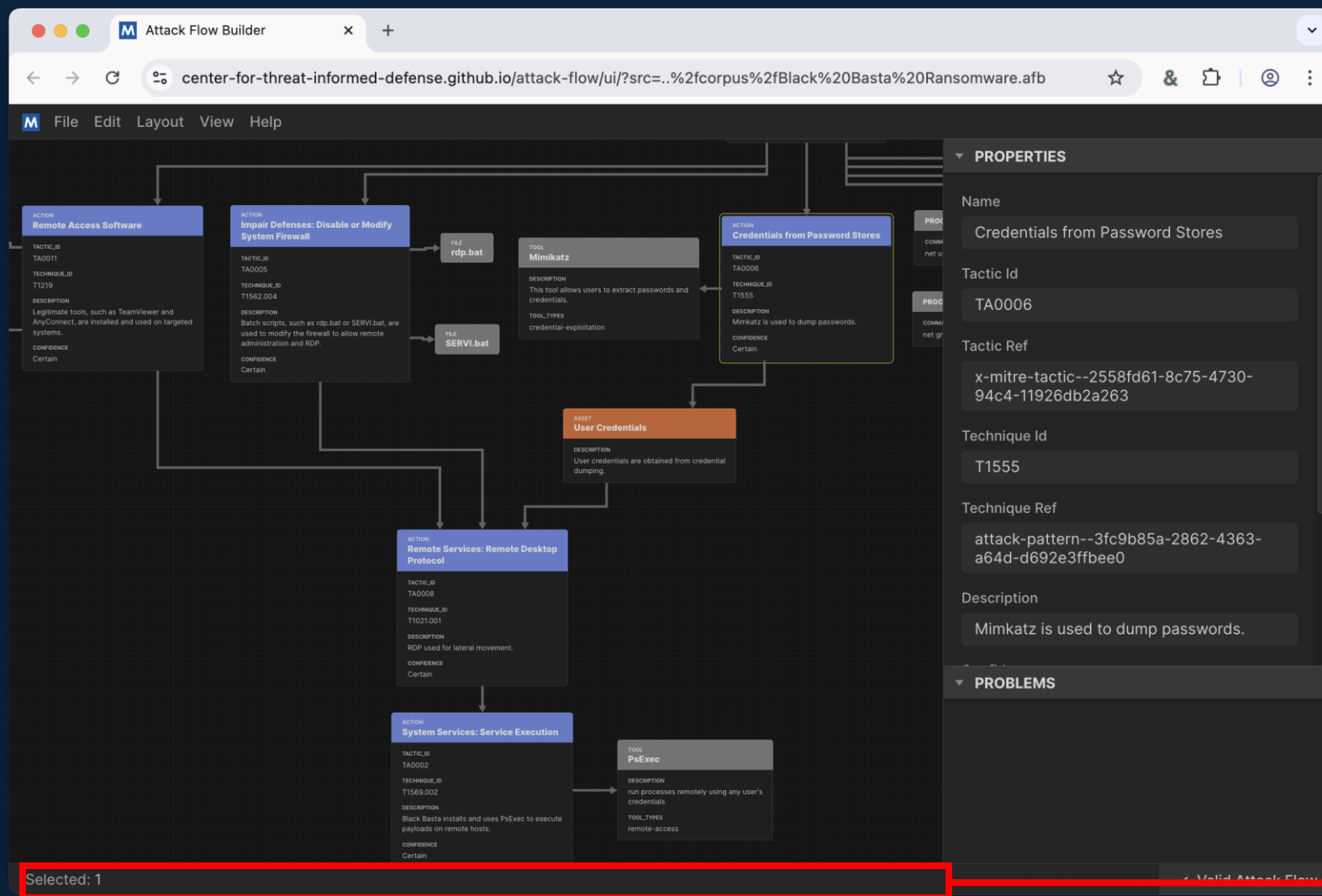
Properties: when you select an item in the diagram, its properties appear here and you may edit them

Web App for Diagramming Attacks



Validation: displays any problems with the flow. click on an issue to zoom to the affected item

Web App for Diagramming Attacks



Attack Flow Building Blocks

Building Blocks: Action

ACTION	
Phishing: Spearphishing Attachment	
TACTIC_ID	TA0001
TECHNIQUE_ID	T1566.001
DESCRIPTION	Victims receive spear phishing emails with malicious zip files attached.
CONFIDENCE	Certain

- Actions are the backbone of Attack Flow. They describe what the adversary is doing at the TTP level (tactic, technique, procedure).
- A action should at least have a name and description. The name is displayed in the blue header, the description is displayed underneath.
- Each action may be mapped to ATT&CK but not required to do so. (It is called “*Attack Flow*”, not “ATT&CK Flow”.)

Building Blocks: Action Properties

ACTION

Phishing: Spearphishing Attachment

TACTIC_ID

TA0001

TECHNIQUE_ID

T1566.001

DESCRIPTION

Victims receive spear phishing emails with malicious zip files attached.

CONFIDENCE

Certain

▼ PROPERTIES

Name

Phishing: Spearphishing Attachment

Tactic Id

TA0001

Tactic Ref

x-mitre-tactic--ffd5bcee-6e16-4dd2-8eca-7b3beedf33ca

Technique Id

T1566.001

Technique Ref

attack-pattern--2e34237d-8574-43f6-aace-ae2915de8597

Description

Victims receive spear phishing emails with malicious zip files attached.

Confidence

Certain ▼

Execution Start

Null

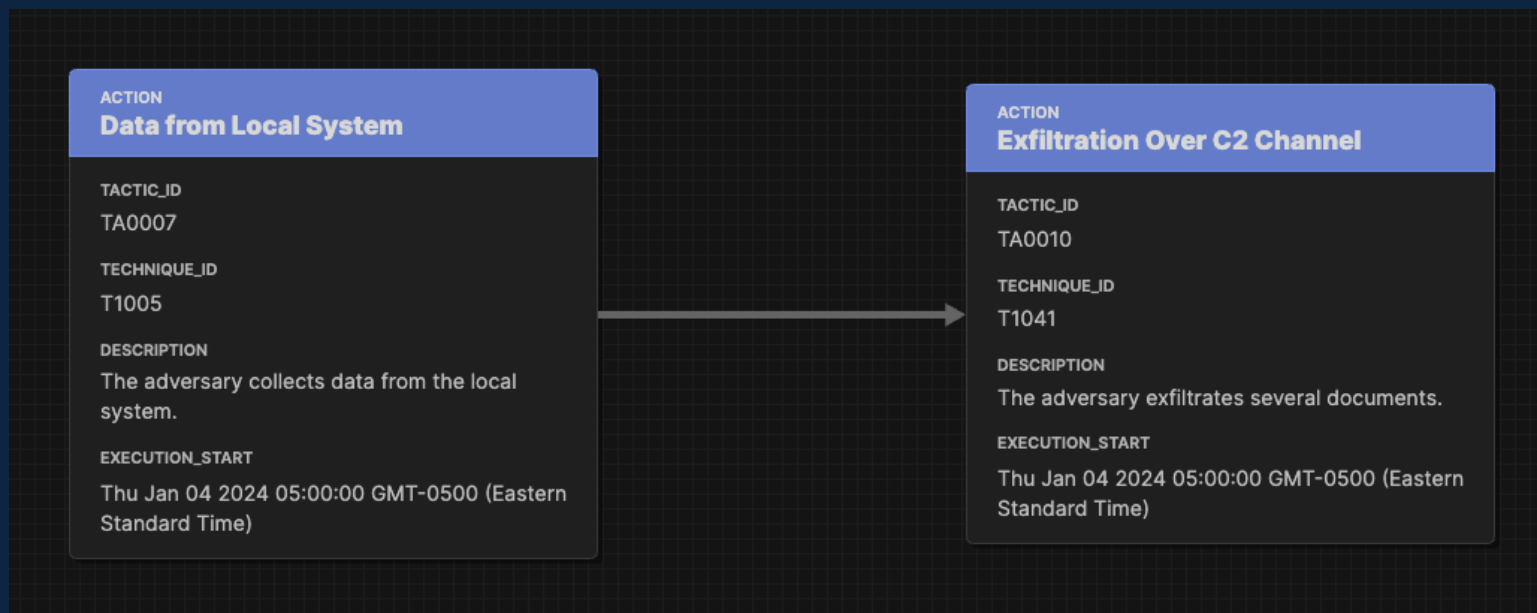
Execution End

Null

Building Blocks: Action Confidence

Term	Description	Confidence Value	Confidence Range
Speculation	Information that is purely speculative or hypothetical, e.g. the author imagines a what-if scenario.	0	0-0
Very Doubtful	Information that is very unlikely to be true. All of the available evidence is against it, or it may have bias in its reporting, e.g. an adversary providing attribution information.	10	1-20
Doubtful	Information that is unlikely to be true. Most of the available evidence is against it.	30	21-40
Even Odds	Information that is equally like to be true as not true; a coin flip. The available evidence is equally weighted in support and against.	50	41-60
Probable	Information that is likely to be true. Most of the available evidence supports it.	70	61-80
Very Probable	Information that is very likely to be true. All of the available evidence supports it.	90	81-99
Certainty	Information that is unquestionably true.	100	100-100

Building Blocks: Action Connections

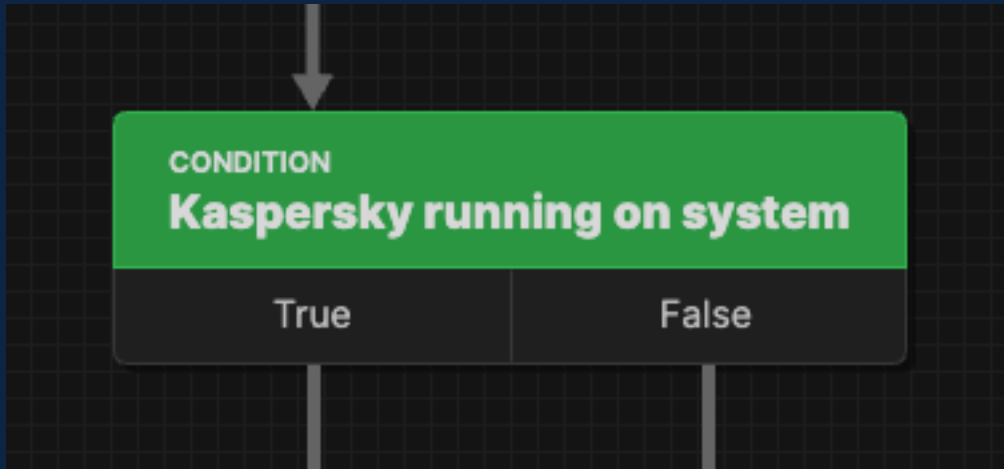


When an action is connected to another action, it represents an *effectual* relationship.

The first action produces an effect that positions the adversary to take the next step.

Reminder: the arrows are not chronological!

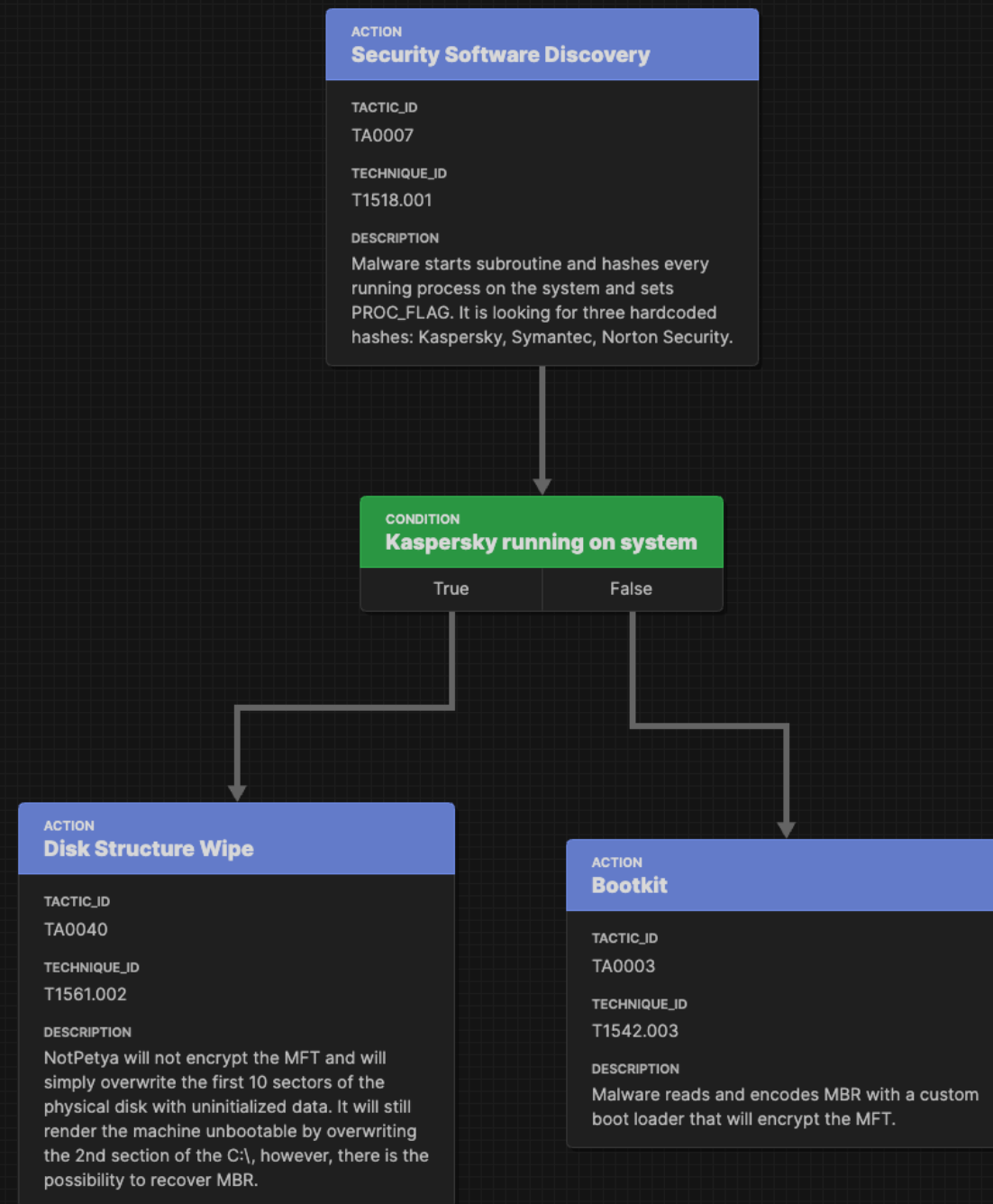
Building Blocks: Condition



- Conditions are used to model decision points in the attack flow, show how the adversary responds to failed attempts, or to represent the state of an asset.
- The description is a human-readable text that is displayed in the green header.
- Can optionally use the STIX Pattern language for machine-readable condition evaluation.
- Unlike other nodes, conditions have two types of ports (true, false).

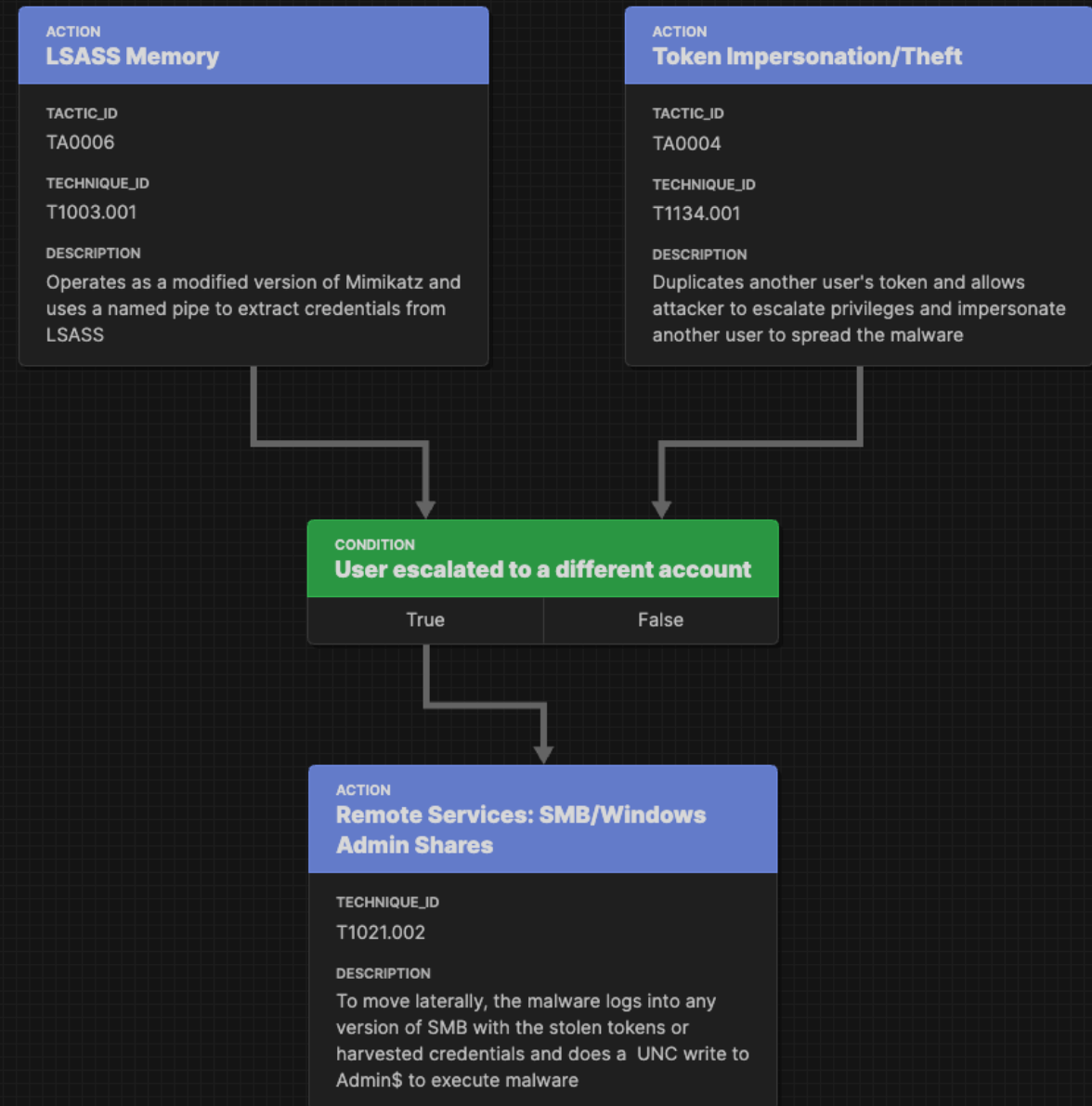
Building Blocks: Condition

- NotPetya checks if Kaspersky is running on the system.
- If yes: corrupts the Master Boot Record.
- If no: installs a malicious bootloader.

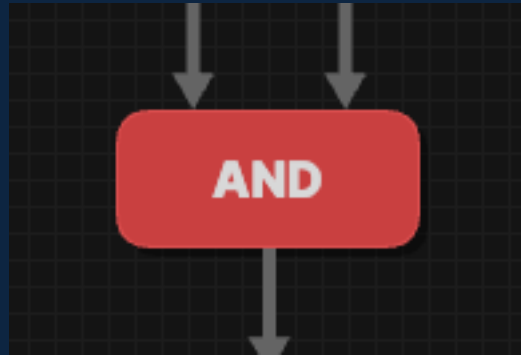
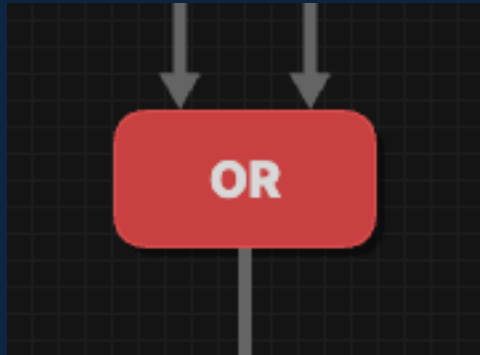


Building Blocks: Condition

- Helpful for easing understanding of complex topics.
- E.g. in NotPetya, the privilege elevation is complex and requires knowledge of Windows internals.
- The condition object makes the flow easier to read.



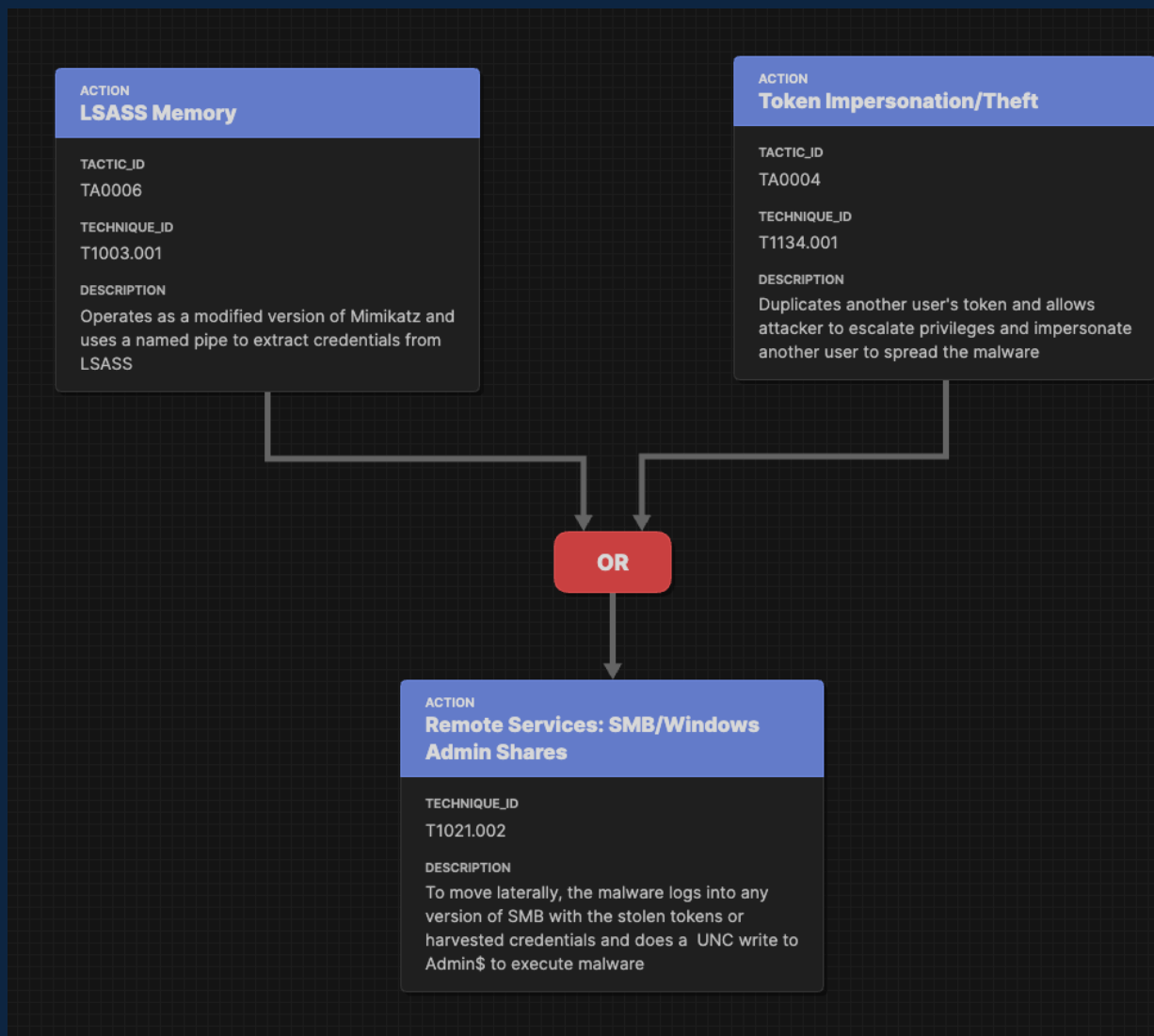
Building Blocks: Operator



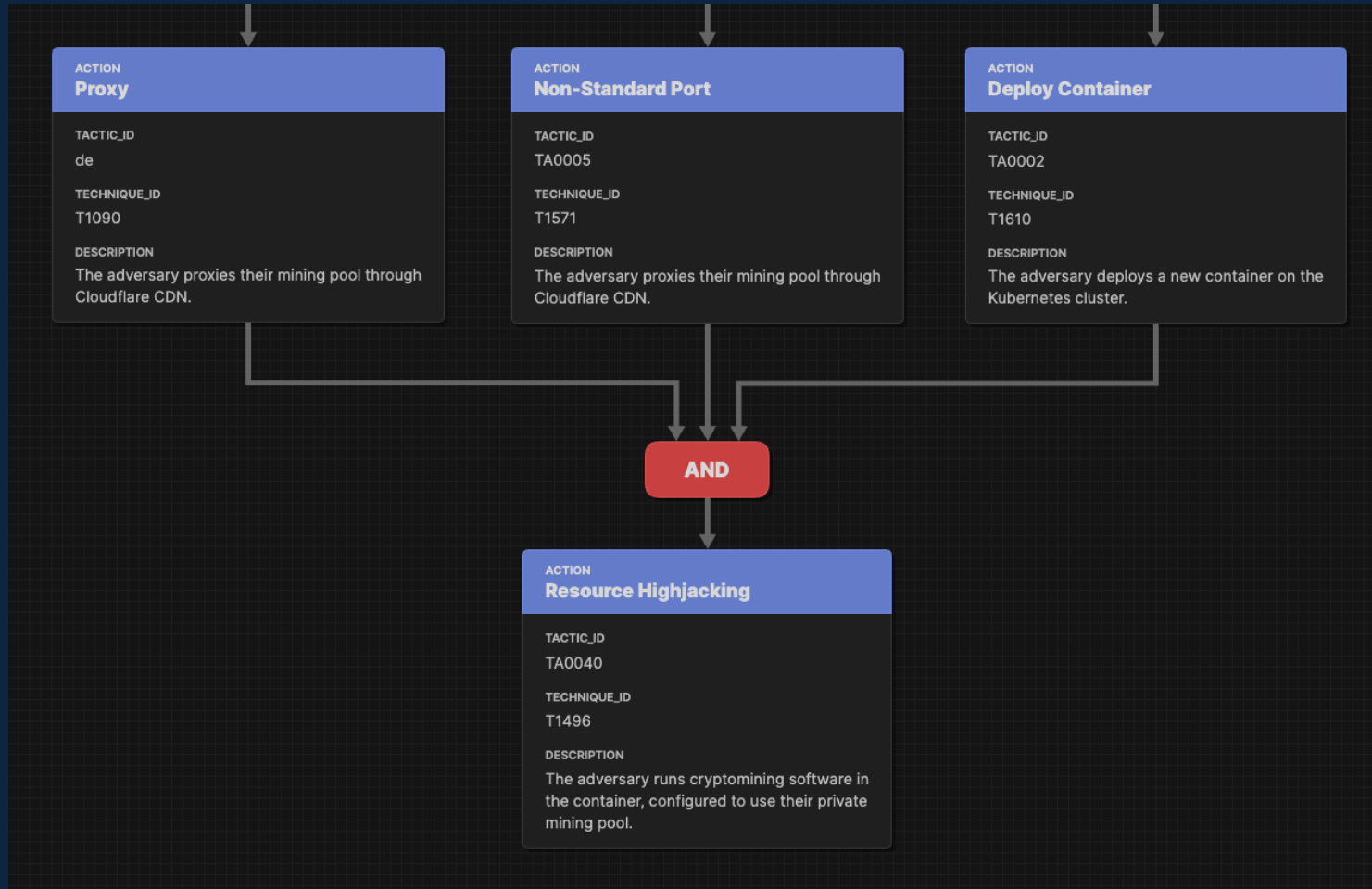
- Operators allow multiple attack paths to converge.
- The OR operator requires *any* of its inputs to succeed before execution continues.
- The AND operator requires *all* its inputs to succeed before execution continues.

Building Blocks: OR Operator

- NotPetya has two privilege escalation techniques.
- If *either one* succeeds, then it can execute its lateral movement technique.

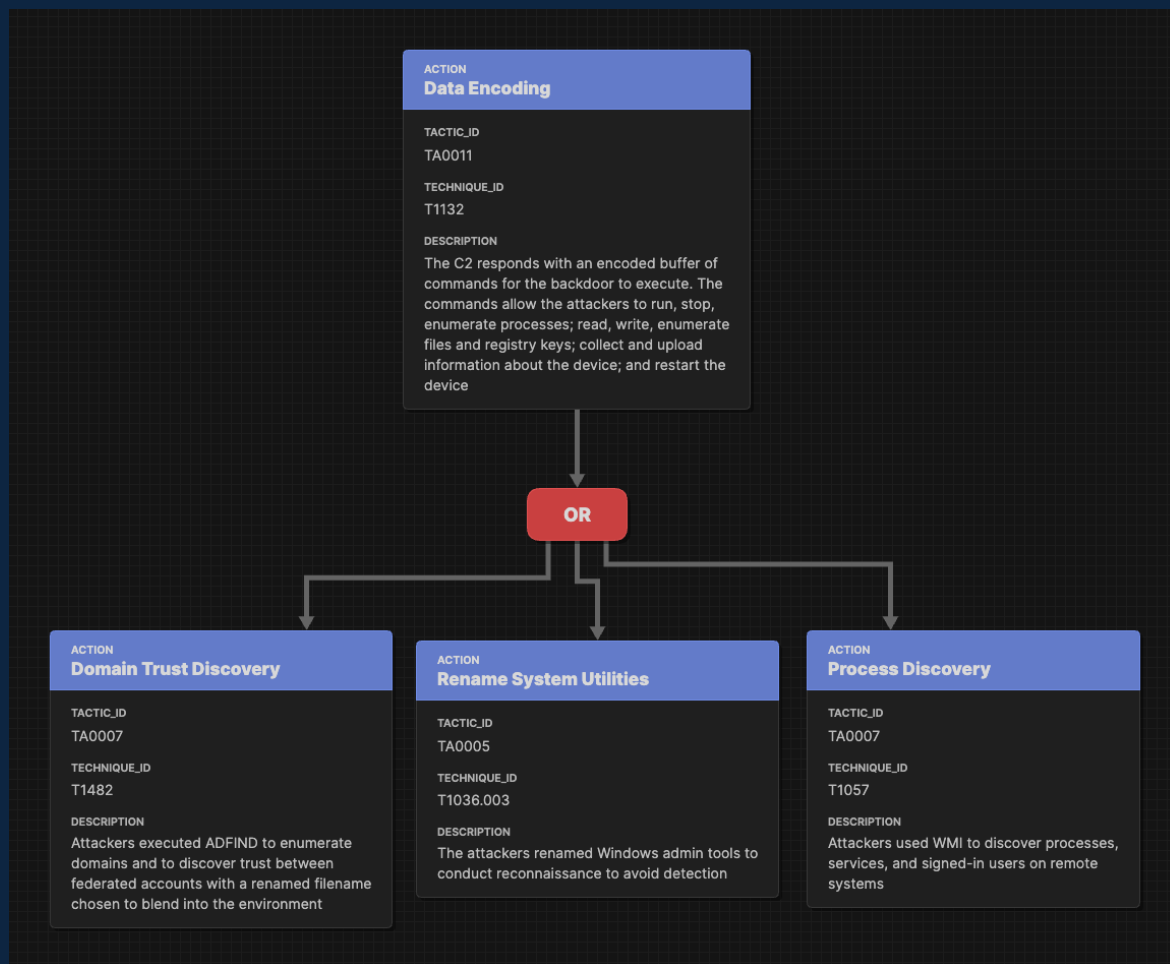


Building Blocks: AND Operator



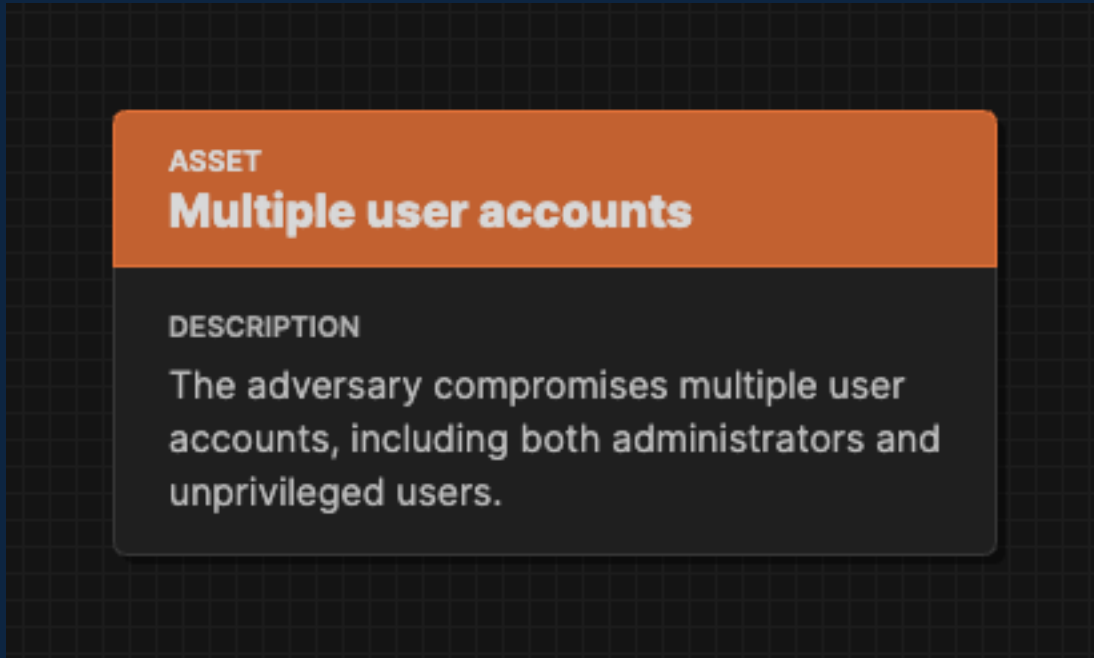
- In the Tesla flow, the adversary must position infrastructure, configure a non-standard port, and deploy a Kubernetes container.
- If they succeed in all three, then they can execute resource hijacking.

Building Blocks: Operator Anti-pattern



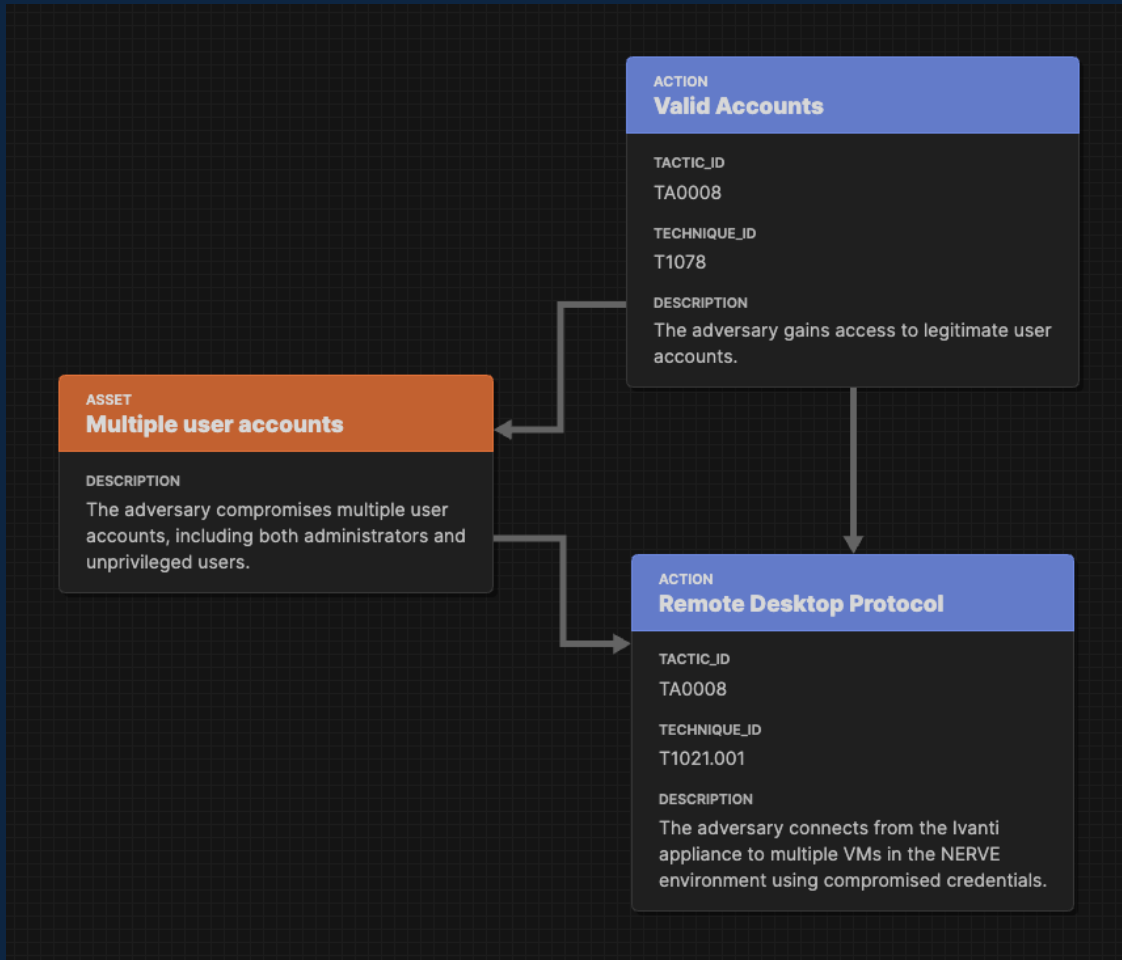
- An operator with a single input doesn't do anything.
- *This is not recommended.*
- We see this in some flows due to a misunderstanding about how to use operators.

Building Blocks: Assets



- Assets represent information systems, data, or users involved in an attack.
- Very generalized: it contains only a name and a description.
- You can add additional structured data using STIX.

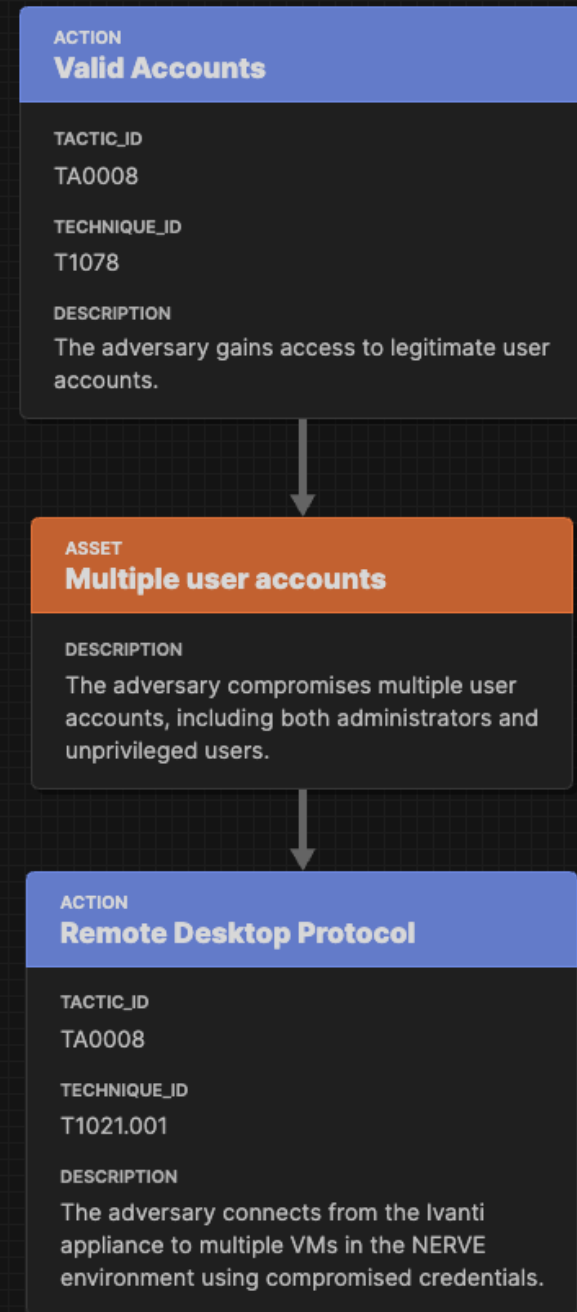
Building Blocks: Asset Connections



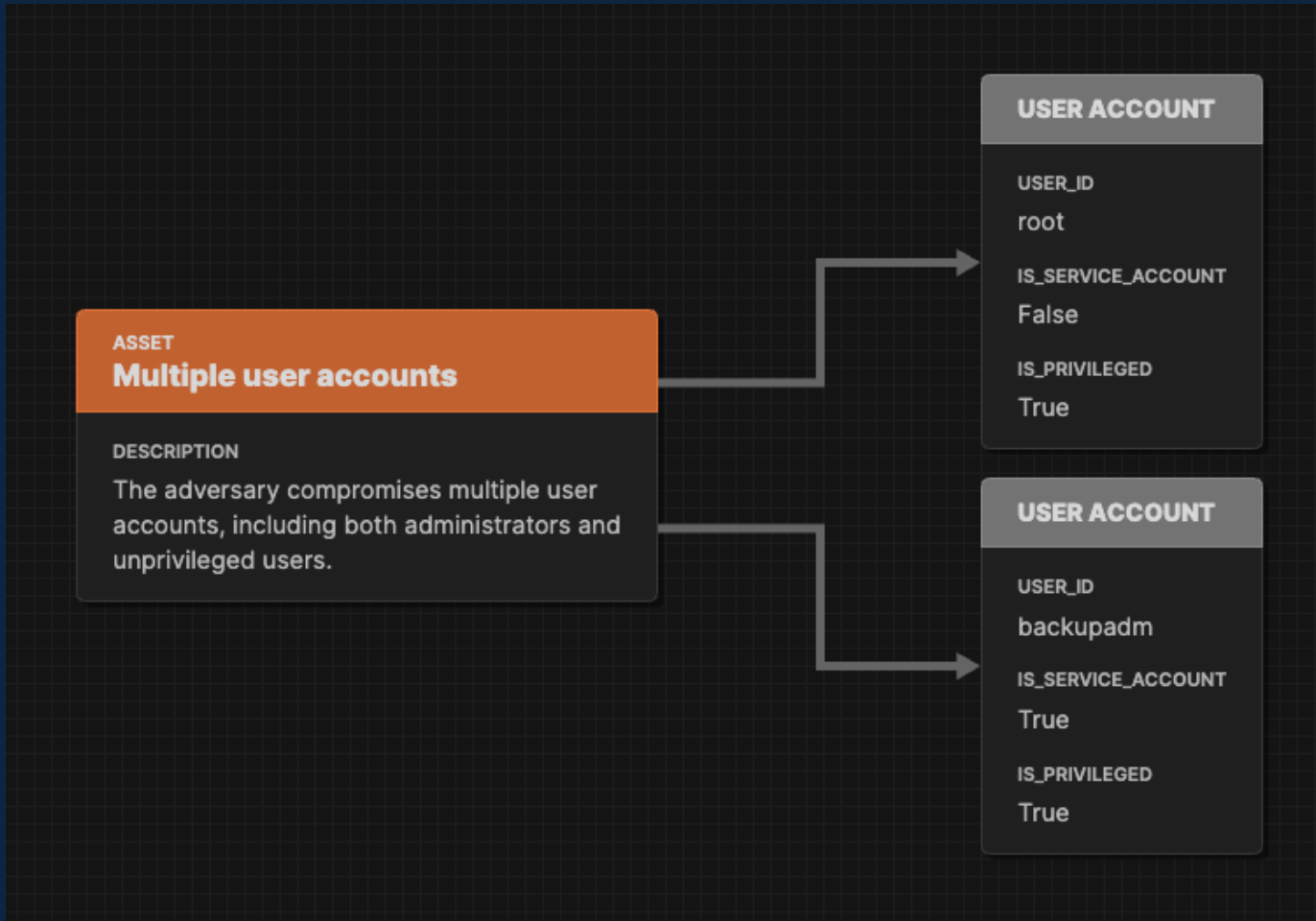
- An edge from an action to an asset indicates that the action modifies the state of that asset.
- An edge from an asset to an action indicates that the action depends on the state of that asset.

Building Blocks: Asset Anti-pattern

- Inserting an asset in between actions is allowed but not recommended.
- Actions should connect to other or operators in a continuous chain. No other nodes should come between actions.



Building Blocks: Asset Structured Data



- While assets are very simple on their own (just name and description) they can be enriched using STIX objects.
- For example, add “User Account” nodes to an asset; this creates structured data about the impacted accounts.

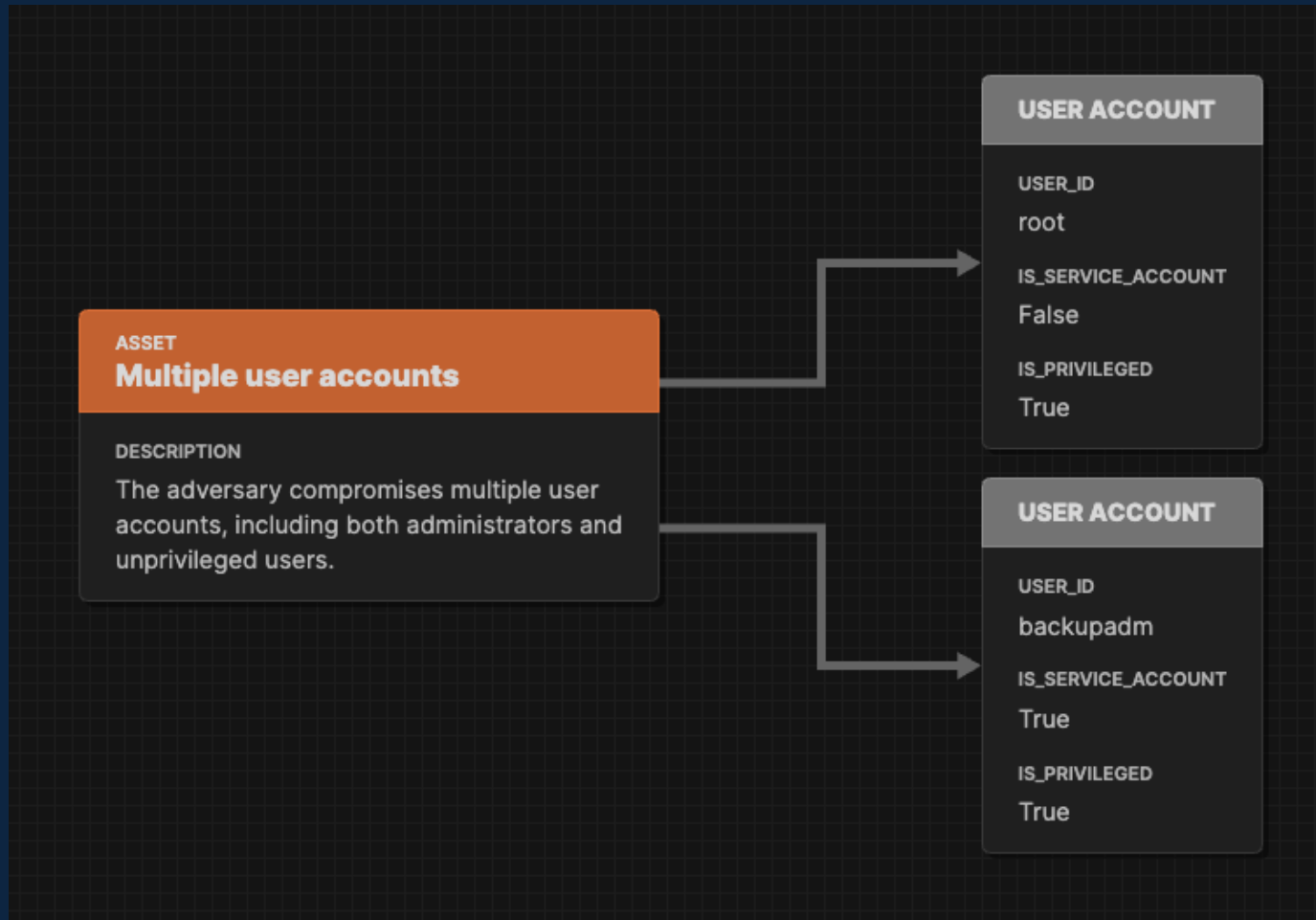
Attack Flow STIX Nodes

STIX Nodes

FILE
afb.exe
SIZE
2048
HASHES
912ec803b2ce49e4a541068d495ab570, 3da541559918a808c2402bba5012f6c60b2766 1c
CTIME
Wed Jan 01 2025 07:00:00 GMT-0500 (Eastern Standard Time)

- Attack flow supports all STIX 2.0 types:
 - 18 STIX Domain Object (SDO) Types
 - 18 STIX Cyber Observable (SCO) Types
- These types are defined in the STIX specification; we adhere to that.
- STIX nodes can be connected with edges just like any other node.
- You can export an Attack Flow to a STIX bundle and import it into any tool that can process STIX (e.g., OpenCTI, etc.)

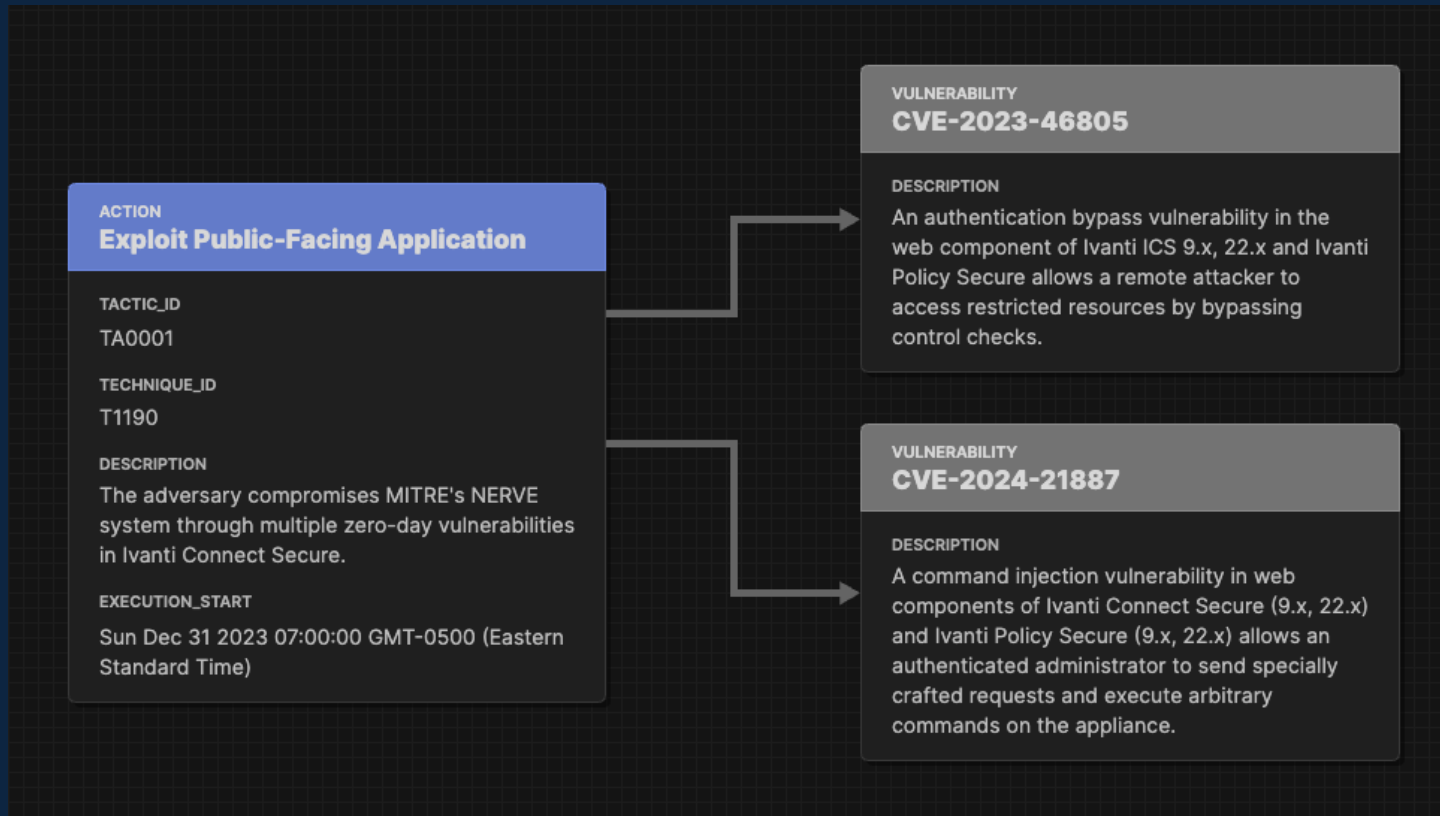
STIX Nodes



This example (that we saw a few slides ago) shows the “User Account” STIX enriching an Asset node.

In STIX this is represented by the "user-account--" observable type.

STIX Nodes



This example shows the "Vulnerability" STIX type used to enrich an Action node.

STIX Nodes

- All of the properties defined in STIX are settable and viewable in Attack Flow Builder.
- For example, “File” is a STIX Observable with 9 property fields. Below is the JSON representation of a File Object (how the data will look exported from Flow)

Examples

Basic file with file system properties without observed encoding

```
{
  "type": "file",
  "spec_version": "2.1",
  "id": "file--e277603e-1060-5ad4-9937-c26c97f1ca68",
  "hashes": {
    "SHA-256": "fe90a7e910cb3a4739bed9180e807e93fa70c90f25a8915476f5e4bfbac681db"
  },
  "size": 25536,
  "name": "foo.dll"
}
```

Basic file with file system properties with observed encoding

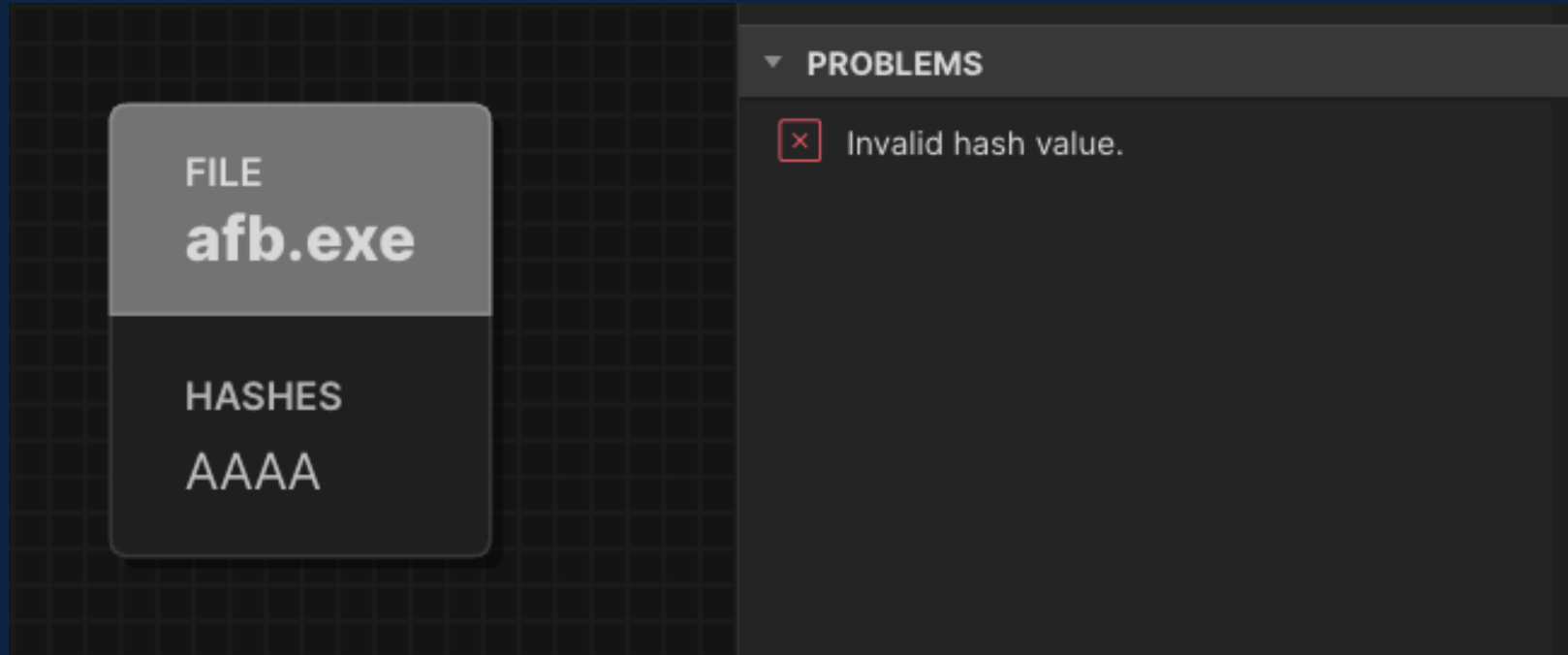
The screenshot displays the Attack Flow Builder interface. On the left, a File object is shown with the following properties:

- FILE**
afb.exe
- SIZE**
2048
- HASHES**
912ec803b2ce49e4a541068d495ab570,
3da541559918a808c2402bba5012f6c60b2766
1c
- CTIME**
Wed Jan 01 2025 07:00:00 GMT-0500 (Eastern
Standard Time)

On the right, the **PROPERTIES** panel is visible, showing the following fields:

- Name**: afb.exe
- Name Enc**: Null
- Size**: 2048
- Hashes**:
 - ▶ 912ec803b2ce49e4a541068d495ab570
 - ▶ 3da541559918a808c2402bba5012f6c60b27661c
 - + Add
- Magic Number Hex**: Null
- Mime Type**: Null
- Ctime**: Jan 1, 2025 - 12:00:00
- Mtime**: Null
- Atime**: Null

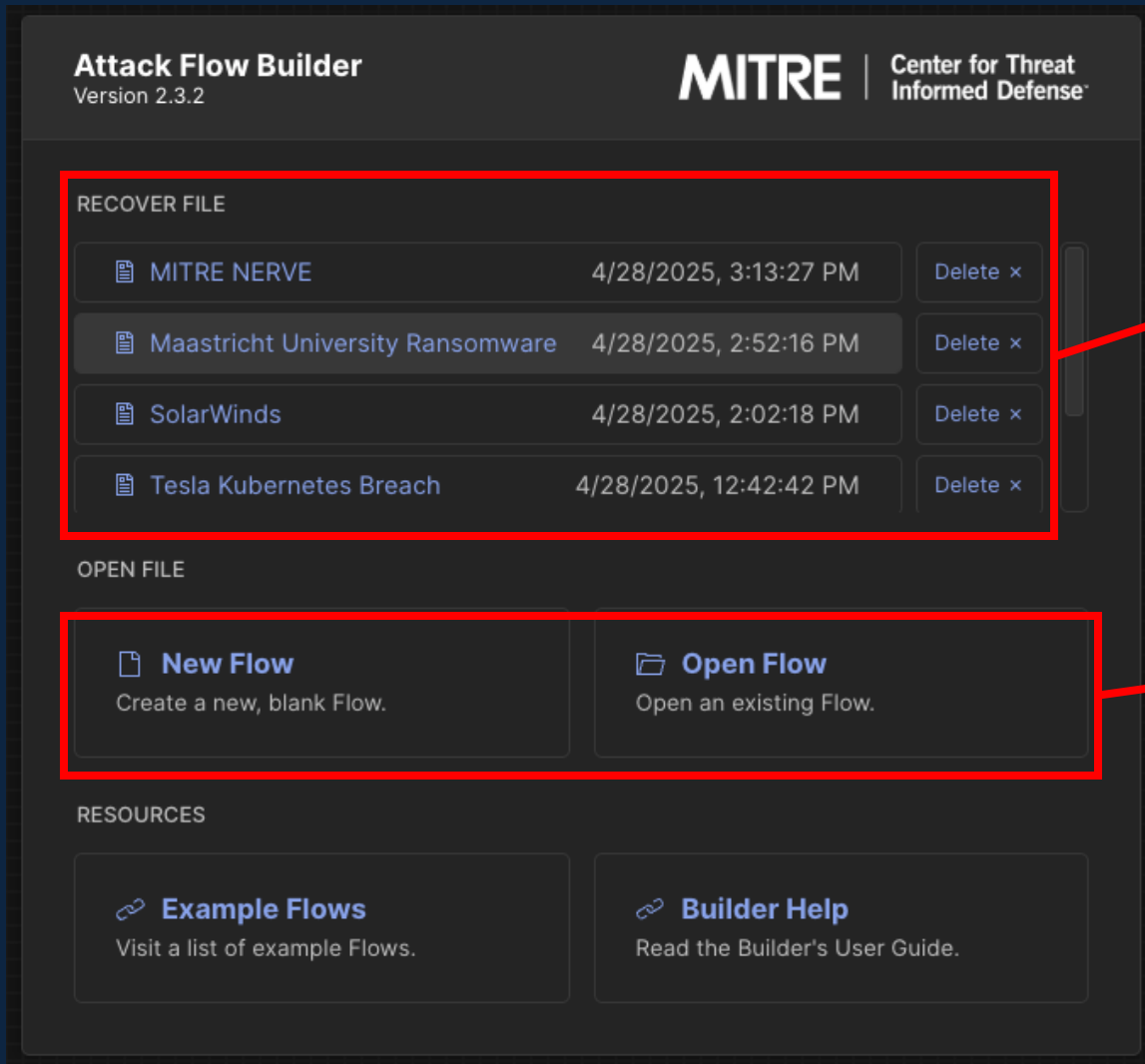
STIX Data Validation



STIX is easy to work with in Attack Flow. The validator helps you enter STIX data correctly.

Attack Flow Features

Splash Screen

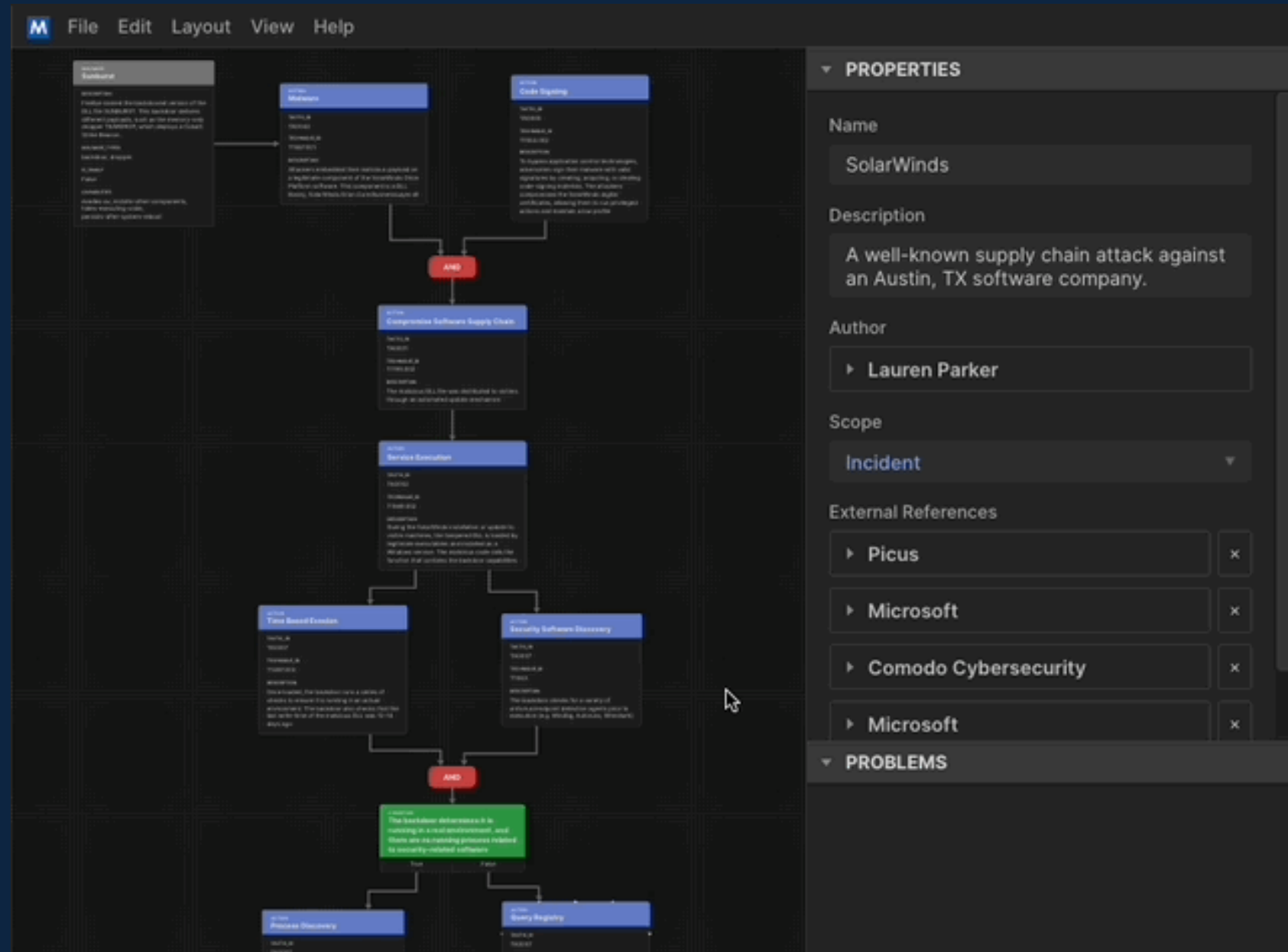


If you accidentally close a flow without saving, you can recover it here.

Create or open a flow

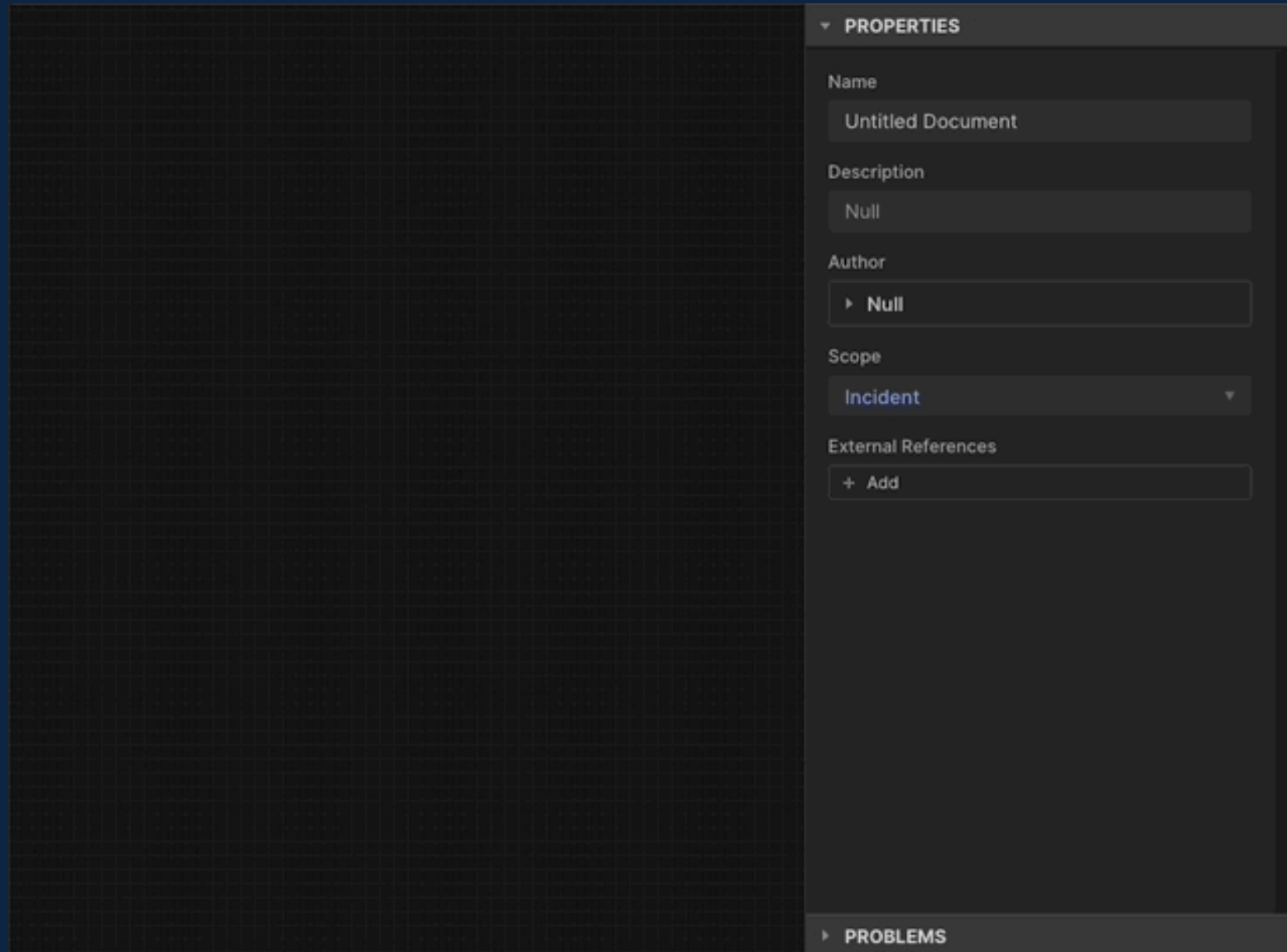
Moving Around

- Click anywhere on the background and drag to pan the diagram.
- Use the scroll wheel to zoom in and out. (Or use the “View” menu.)



Creating a Node

- Right click on the diagram and select Create → Attack Flow → Action.
 - Or go to the menu bar → Edit → Create → ...
- Click the action to display its properties in the side panel.
- Key in the properties.
- Some properties autocomplete, e.g. tactic and technique.



The screenshot displays the MITRE ATT&CK Editor interface. The main workspace is a dark grid. On the right, a 'PROPERTIES' panel is visible with the following fields:

- Name:** Untitled Document
- Description:** Null
- Author:** ▸ Null
- Scope:** Incident (dropdown menu)
- External References:** + Add

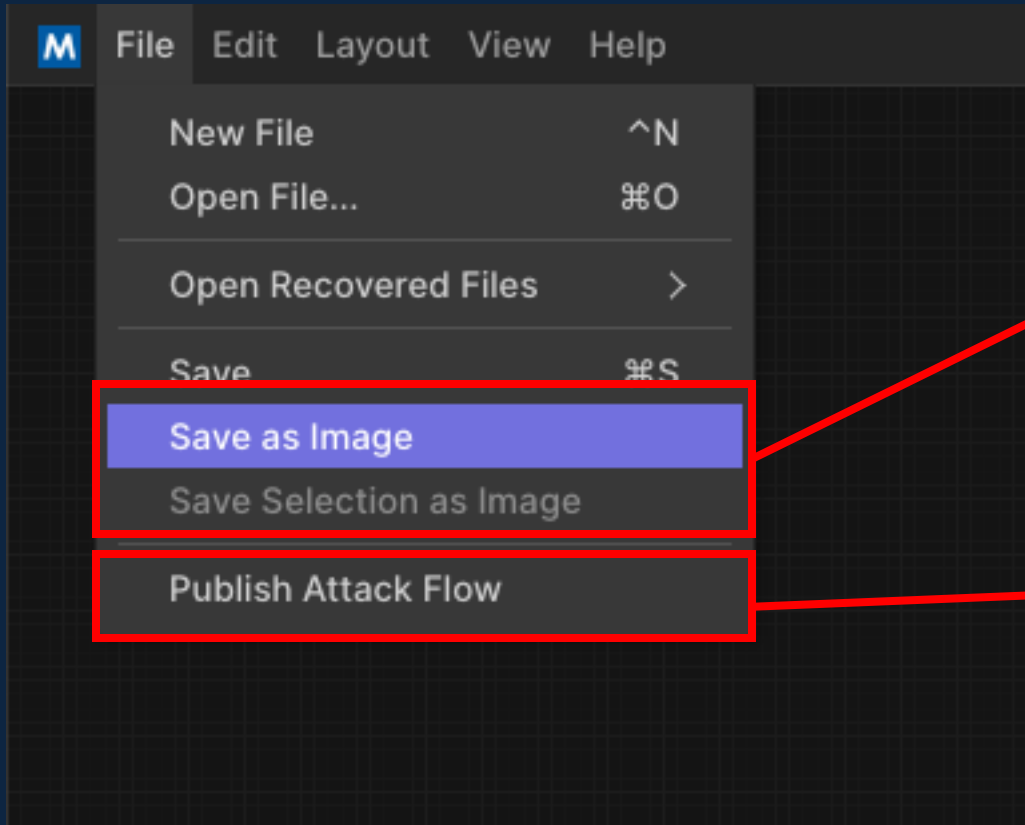
At the bottom of the properties panel, there is a 'PROBLEMS' section with a right-pointing arrow.

Connecting Nodes

- When the mouse hovers over a node, it displays its anchor points.
- Click on an anchor and drag to create a new line.
- Connect the other end of the line to a different anchor.
- Once connected, lines follow the nodes they are attached to if the node is moved.

The screenshot displays the MITRE ATT&CK interface. Two nodes are visible on a grid background. The top node is titled 'ACTION LSASS Memory' and contains the following details: TACTIC_ID: TA0006, TECHNIQUE_ID: T1003.001, and DESCRIPTION: The adversary dumps password hashes from LSASS. The bottom node is titled 'ACTION Password Cracking' and contains: TACTIC_ID: TA0006, TECHNIQUE_ID: T1110.002, and DESCRIPTION: The adversary cracks the password hashes using JohnTheRipper. A line connects the 'Anchor' point of the top node to the 'Anchor' point of the bottom node. On the right, the 'PROPERTIES' panel is open, showing fields for Name (Untitled Document), Description (Null), Author (Null), Scope (Incident), and External References (+ Add). The bottom of the sidebar shows the 'PROBLEMS' panel.

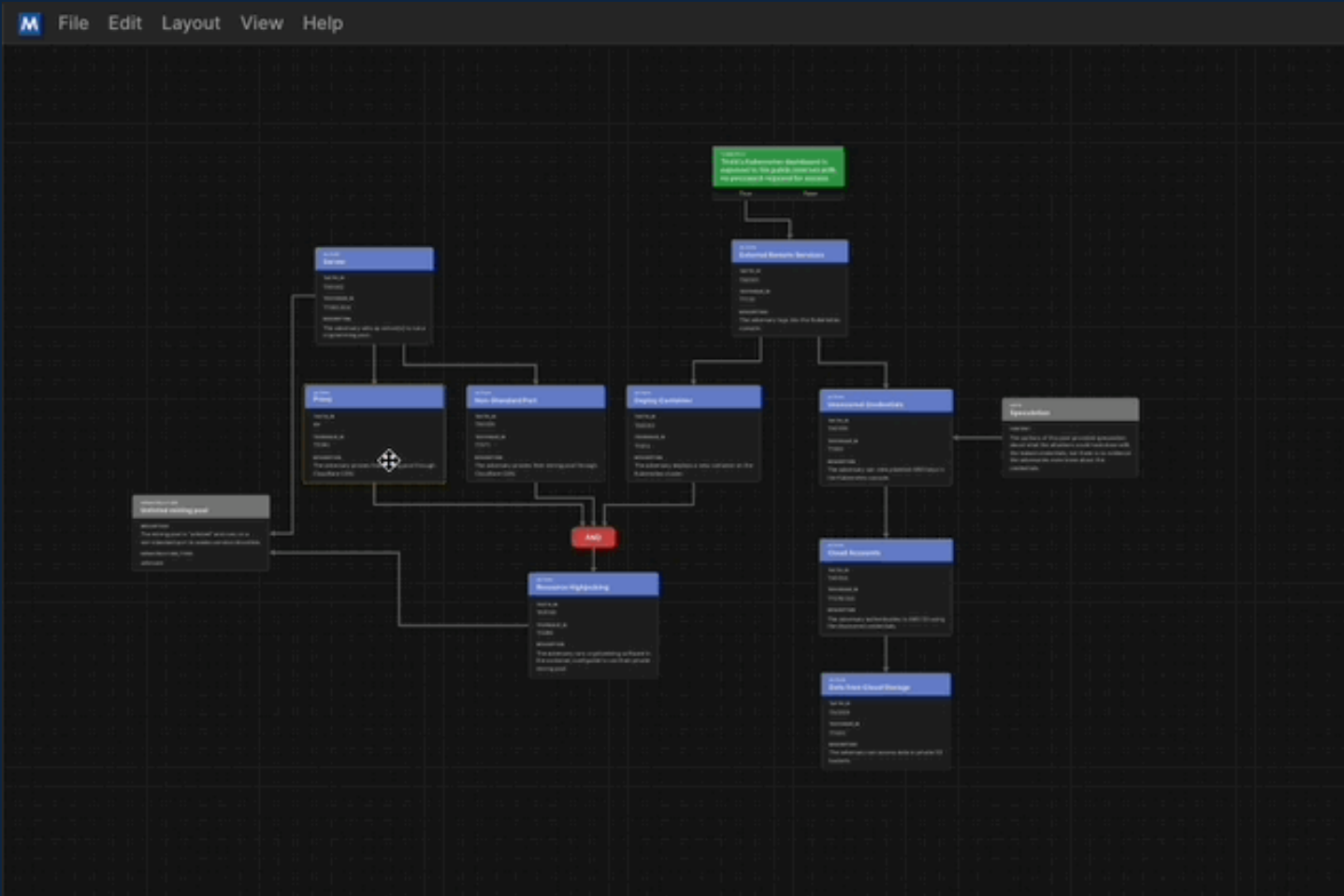
Exporting



Save a flow (or part of a flow) as a PNG image. Huge timesaver for presentations. (Including the one you're viewing right now.)

Export to STIX bundle

Zooming Shortcuts

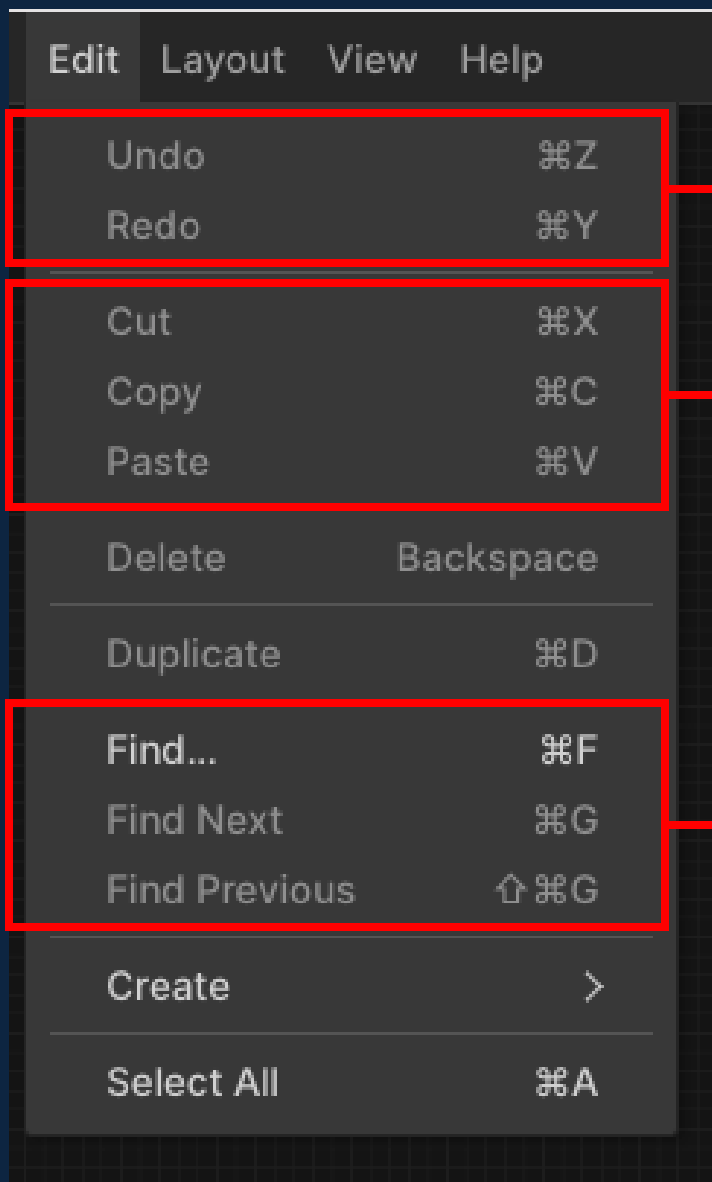


Press *Shift*+Z to zoom into a selected object.

Press *Shift*+C to zoom to the next set of connected nodes.

(Also accessible from the “View” menu)

Edit



Undo or redo the last action.

Cut and paste any nodes or edges'

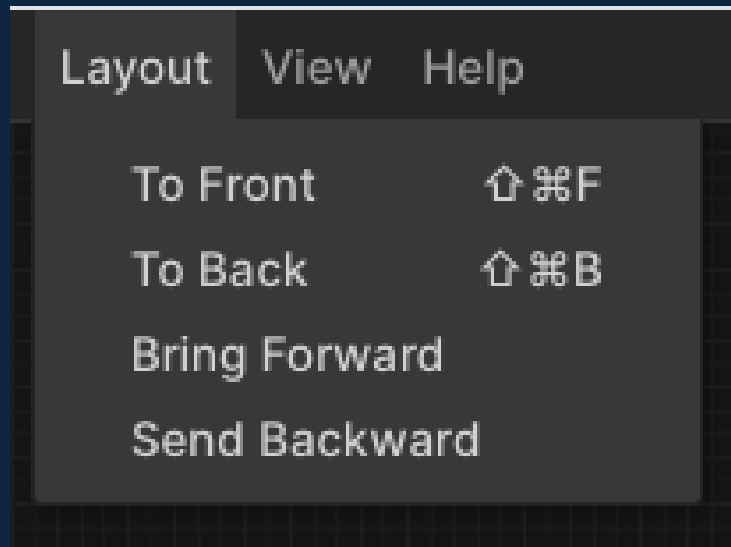
Search the flow

Search a Flow

- Keyword search to quickly find specific items in the flow.
- It zooms into the matching items so that you can see them clearly.



Layout



The layout menu lets you change how items are stacked in the diagram. (In practice, you don't need to do this very often.)

End of Section 3

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