



Center for Threat  
Informed Defense

# Attack Flow – Beyond Atomic Behaviors

**Desiree Beck, Gabriel Bassett, Ryusuke Masuoka**

**30 June 2022**

# Who Are We?



**Desiree Beck**

Principal Cybersecurity Engineer  
MITRE  
dbeck@mitre.org



**Gabriel Bassett**

Lead Data Scientist and Co-author  
Verizon DBIR  
gabriel.bassett@verizon.com



**Ryusuke Masuoka**

Research Principal  
Fujitsu System Integration Labs  
masuoka.ryusuke@fujitsu.com

# The Center for Threat-Informed Defense conducts collaborative R&D projects that **improve cyber defense at scale**



## Membership is:

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

## The center by the numbers

Mission  
1

Members  
29

Affiliates  
7

Ideas in Pipeline  
24

Projects Underway  
4

Published Projects  
17

# Attack Flow Participants



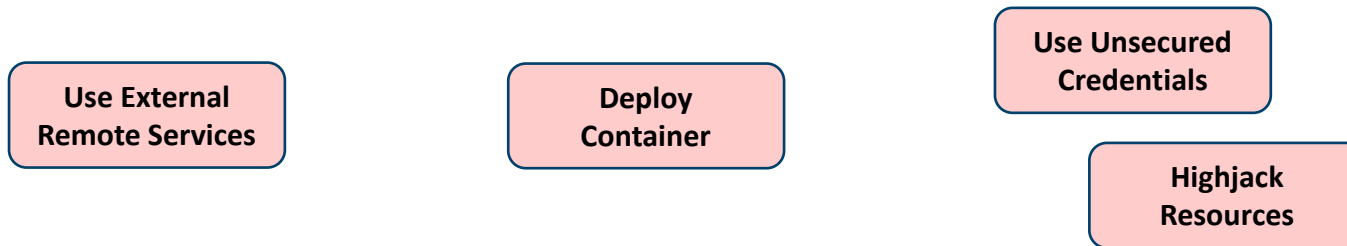
# Outline

- Problem
  - What's the problem?
  - What's an attack flow?
- Solution
  - Attack flow data format
- Impact
  - How do attack flows help?
  - Attack flow corpus

# Problem

# What's the Problem?

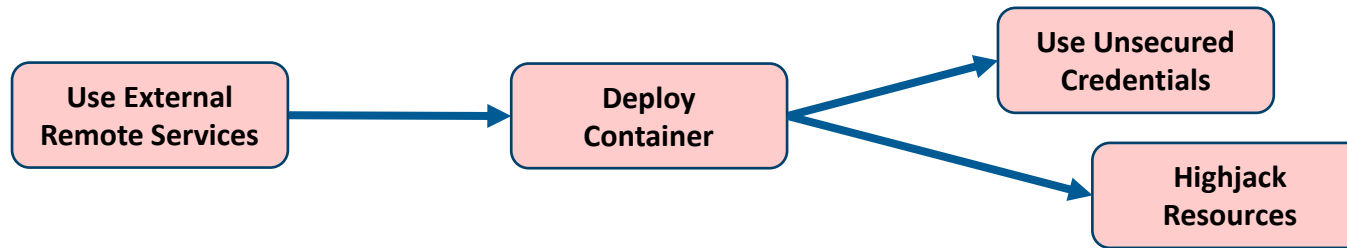
- Defenders track adversary behaviors individually, but adversaries use *sequences* of techniques



- False positives harder to identify
- Incidents harder to understand
- Defensive planning is less effective
- Cyber assessments are less useful

# What's the Problem?

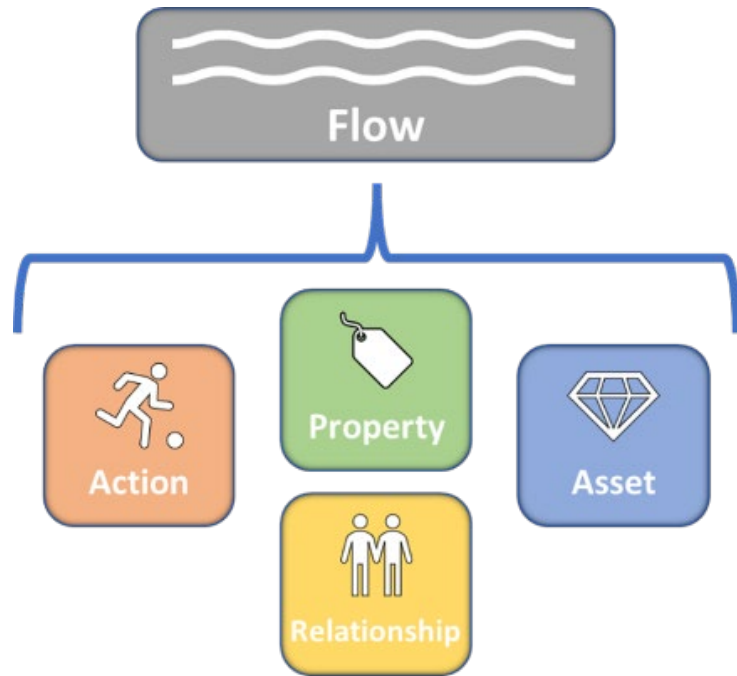
- Defenders track adversary behaviors individually, but adversaries use *sequences* of techniques



Sequences of techniques create *relationships*



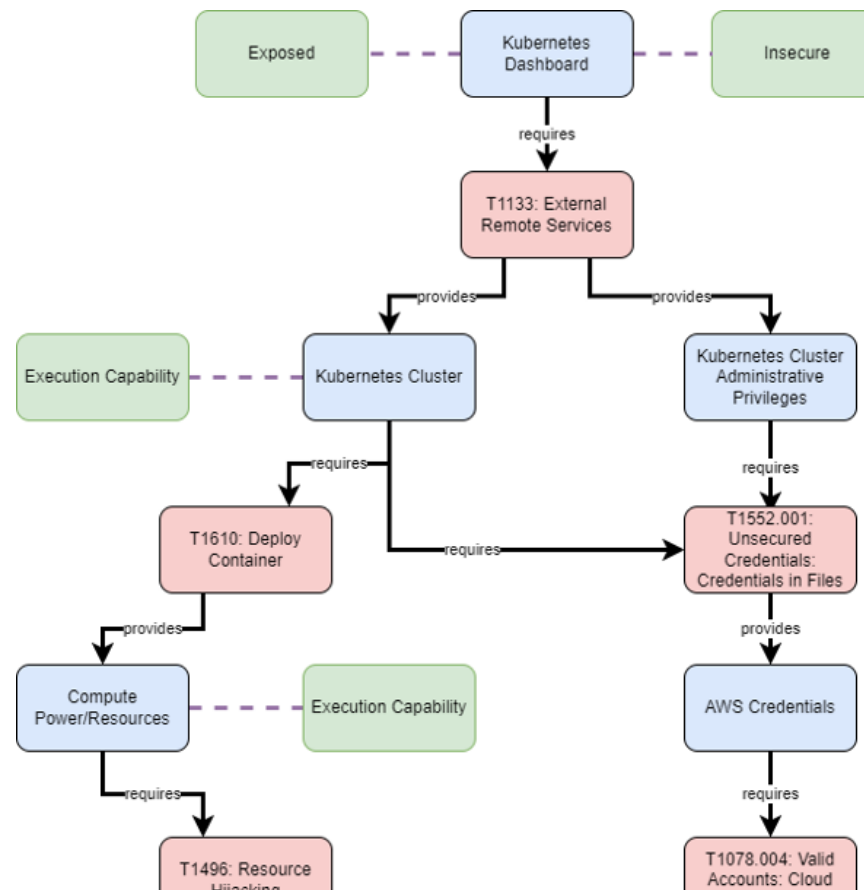
# What's an Attack Flow?



An attack flow is a machine-readable representation of a sequence of actions and assets, plus knowledge properties.

# How Do Attack Flows Help?

- Communication
- Intelligence exchange
- Operations
- Defensive planning
- Assessments



# Solution

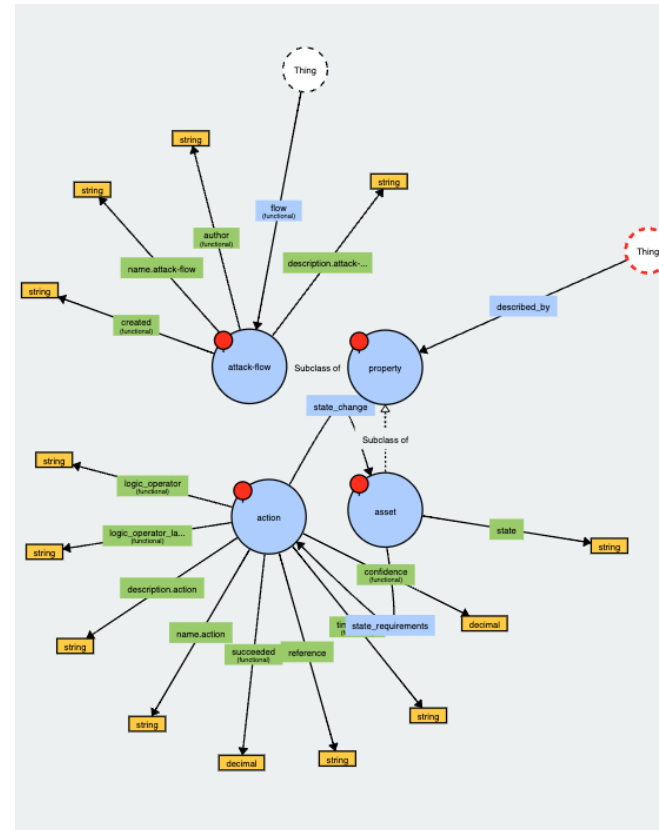
# Learn by example

# Schemas

## • JSON Schema

```
▼ object {8}
  $schema : https://json-schema.org/draft/2020-12/schema
  $id : https://mitre-engenuity.com/schema/attack-flow/2021-10-13-draft.json
  title : Attack Flow
  description : This schema describes the Attack Flow JSON format.
  type : object
  ▼ properties {6}
    ▼ flow {4}
      description : An Attack Flow Meta object
      type : object
      ▼ properties {6}
        ▼ type {3}
          description : Indicate that this is an Attack Flow.
          type : string
          ▼ enum [1]
            0 : attack-flow
        ▼ id {3}
          description : The identifier for this Attack Flow. MUST be unique within this document. TODO: Ideally is unique among Attack Flows produced by a particular organization.
          type : string
          format : uri
        ▼ name {2}
          description : The name of the Attack Flow.
          type : string
```

## • RDF (Graph) Schema



# Short Interlude: RDF

# What is RDF?

- RDF = Resource Description Framework



- URI = Unique Resource Identifier

RDF takes 3 URIs and turns them into a source node, relationship edge, and target node.

# Ok, back to the example...



# Start with data

## • IR Report

### Incident 12345

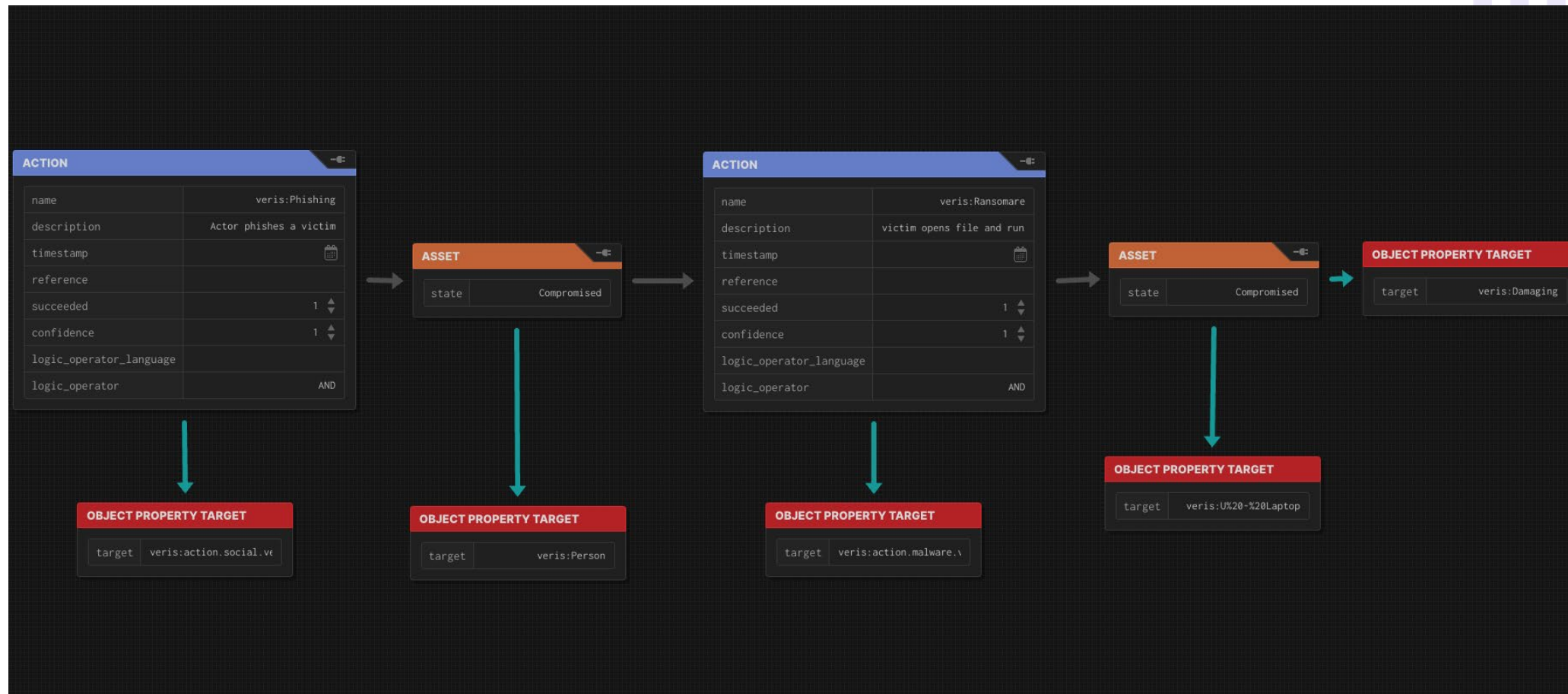
- \* Mail logs show User A receives phishing email and opens attached macro-enabled word document on Host B
- \* Proxy and host logs detect Host B beaconing to known C2, downloading the ransomware, and running it

## • Red Team Report

### Engagement 56789

- \* Phished User A to run macro-enabled office document on Host B
- \* Installed simulated ransomware through shell embedded in document on Host B

# Structuring Data



# Storage – JSON-SCHEMA

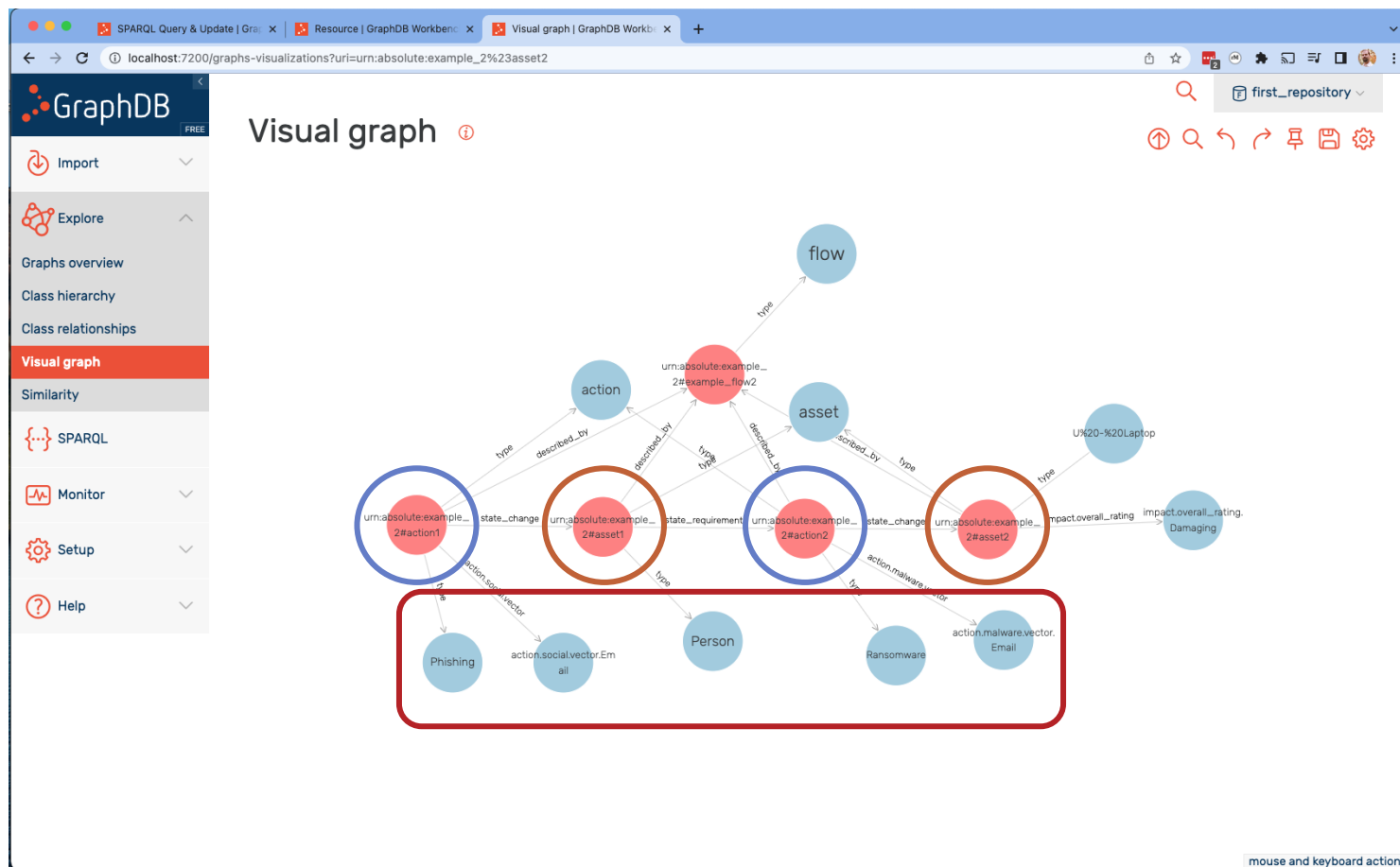
```
example_3.jsonld  example_3.json
1 {
2   "$schema": "../schema/attack-flow-2021-11-03-draft.json",
3   "actions": [
4     {
5       "description": "actor phishes a victim",
6       "id": "urn:absolute:example_3#action1",
7       "logic_operator": "AND",
8       "name": "action1"
9     },
10    {
11      "description": "victim opens file and runs macro that installs ransomware",
12      "id": "urn:absolute:example_3#action2",
13      "logic_operator": "AND",
14      "name": "action2"
15    }
16  ],
17  "assets": [
18    {
19      "id": "urn:absolute:example_3#asset1"
20    },
21    {
22      "id": "urn:absolute:example_3#asset2"
23    }
24  ],
25  "data_properties": [],
26  "flow": {
27    "created": "2022-04-11T16:39:00",
28    "id": "urn:absolute:example_3#example_flow3",
29    "name": "example_flow3",
30    "type": "attack-flow"
31  },
32  "object_properties": [],
33  "relationships": [
34    {
35      "source": "urn:absolute:example_3#asset1",
36      "target": "urn:absolute:example_3#action2",
37      "type": "https://vz-risk.github.io/flow/attack-flow/state_requirement"
38    },
39    {
40      "source": "urn:absolute:example_3#action1",
41      "target": "urn:absolute:example_3#asset1",
```

# Storage – JSON-LD (Linked Data)

```
PREFIX owl: <http://www.w3.org/2002/07/owl#> [
1  {
2  {
3    "@id": " https://example.com/example_2#action1",
4    "@type": ["http://www.w3.org/2002/07/owl#NamedIndividual", "https://veriscommunity.net/attack-flow/Phishing", "https://vz-risk.github.io/flow/attack_flow/action"],
5    "https://veriscommunity.net/attack-flow/action.social.vector": [
6      {
7        "@id": "https://veriscommunity.net/attack-flow/action.social.vector.Email"
8      },
9    ],
10   "https://vz-risk.github.io/flow/attack_flow/description": [
11     {
12       "@value": "actor phishes a victim"
13     },
14   ],
15   "https://vz-risk.github.io/flow/attack_flow/logic_operator": [
16     {
17       "@value": "AND"
18     },
19   ],
20   "https://vz-risk.github.io/flow/attack_flow/state_change": [
21     {
22       "@id": " https://example.com/example_2#asset1"
23     },
24   ],
25   "https://vz-risk.github.io/flow/attack_flow/described_by": [
26     {
27       "@id": " https://example.com/example_2#example_flow2"
28     }
29   ]
30 },
31 {
32   "@id": " https://example.com/example_2#action2",
33   "@type": ["http://www.w3.org/2002/07/owl#NamedIndividual", "https://vz-risk.github.io/flow/attack_flow/action", "https://veriscommunity.net/attack-flow/Ransomware"],
34   "https://vz-risk.github.io/flow/attack_flow/state_change": [
35     {
36       "@id": " https://example.com/example_2#asset2"
37     },
38   ],
39   "https://veriscommunity.net/attack-flow/action.malware.vector": [
40     {
41       "@id": "https://veriscommunity.net/attack-flow/action.malware.vector.Email"
42     },
43   ],
44   "https://vz-risk.github.io/flow/attack_flow/described_by": [
45     {
46       "@id": " https://example.com/example_2#example_flow2"
47     }
48   ]
49 }
50 ],
51 }
```

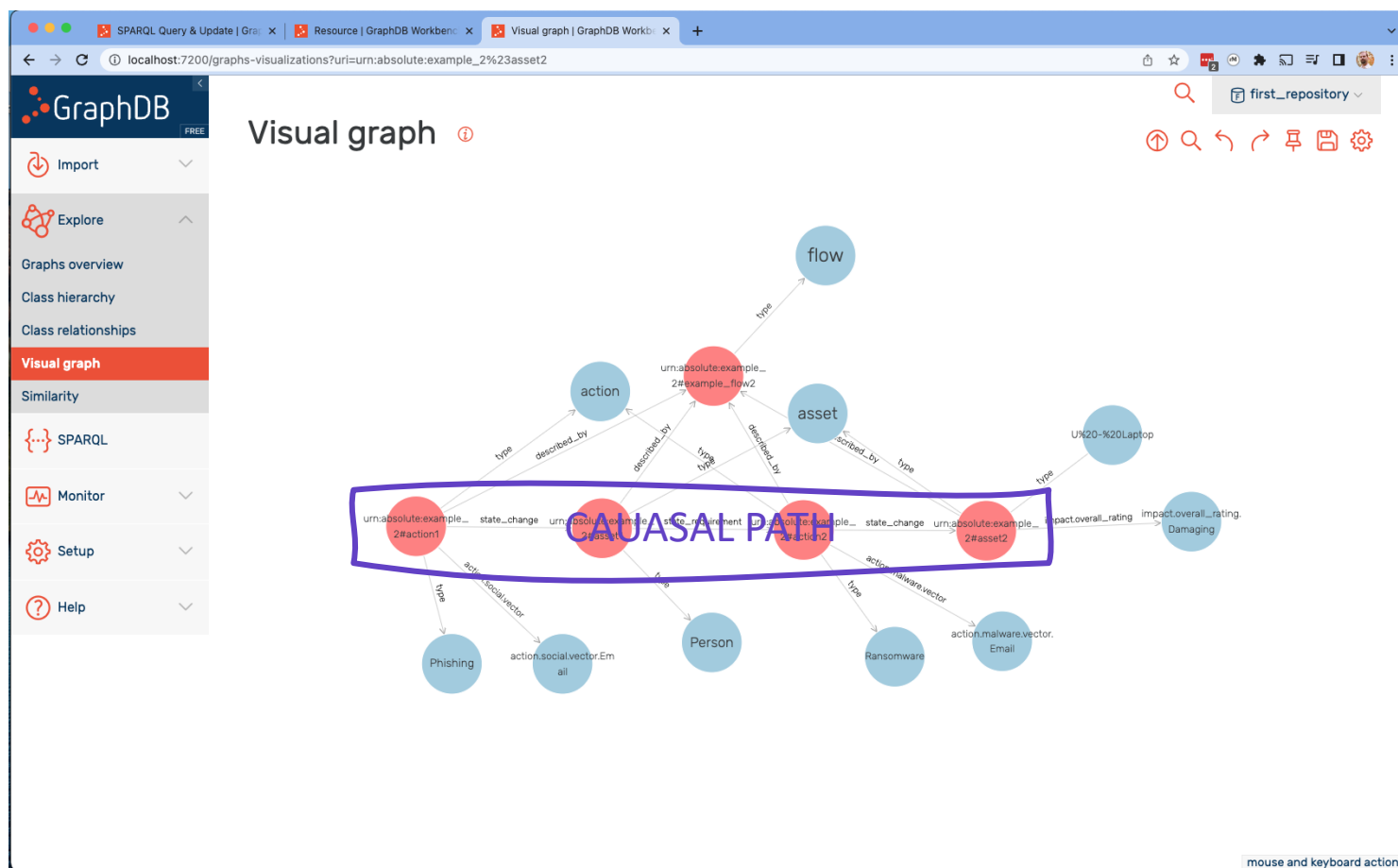
# So what's it look like?

# Attack Flow Data Format



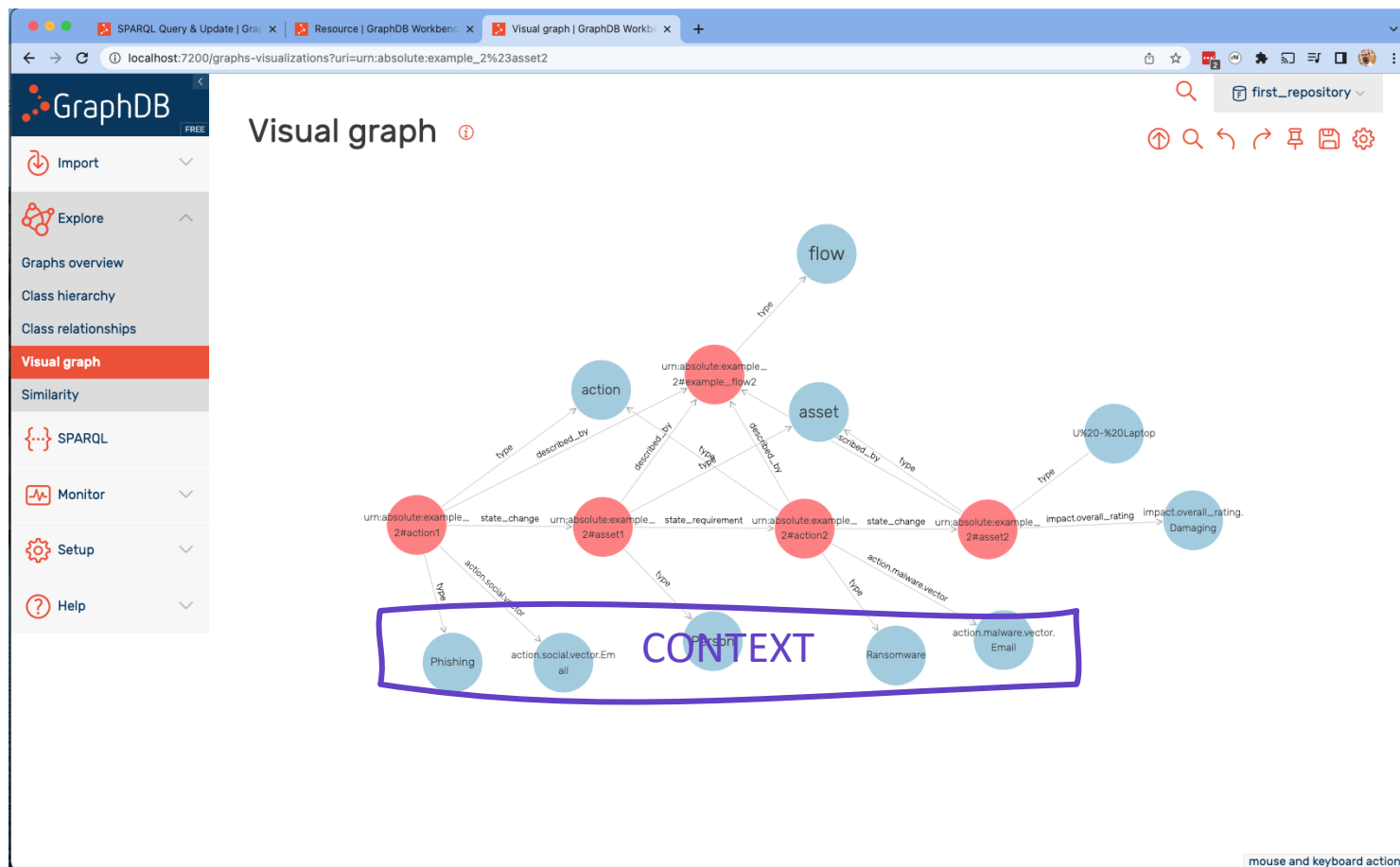
# Three C's: Causality, Context, Complexity

# Attack Flow Data Format - Causality

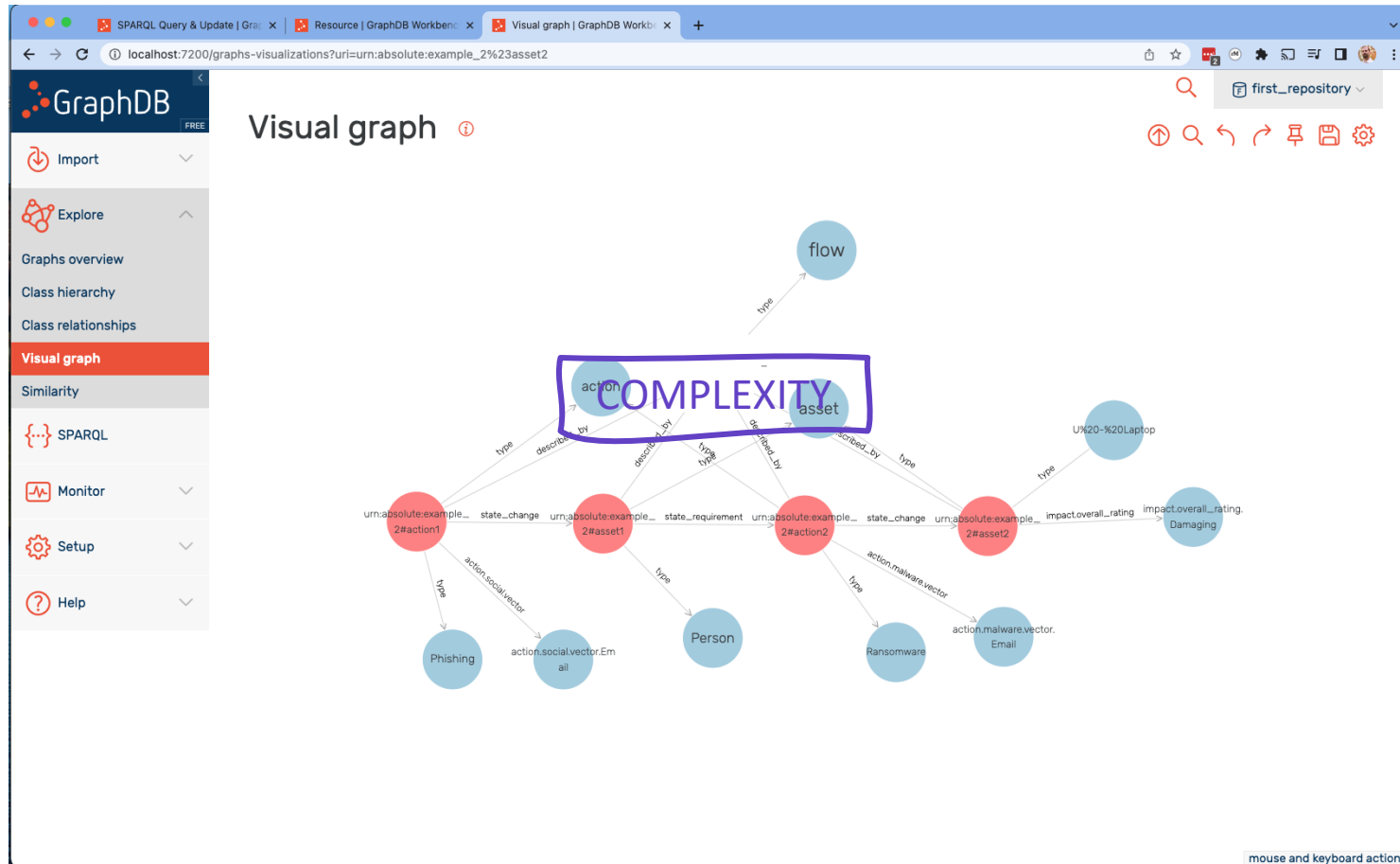




# Attack Flow Data Format - Context



# Attack Flow Data Format – Complexity





y

ITY. | Center for Threat  
Informed Defense



# Analysis

# Analysis

## SPARQL Query & Update

first\_repository

Editor only Editor and results Results only

Unnamed × Unnamed × Unnamed × Unnamed × Unnamed × Unnamed × Unnamed ×

Unnamed ×

```
1 PREFIX af: <https://vz-risk.github.io/flow/attack-flow/>
2 PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
3 SELECT DISTINCT ?asset
4 WHERE {
5   ?asset rdf:type af:asset .
6 }
```

Run

keyboard shortcuts

Table Raw Response Pivot Table Google Chart Download as

Filter query results Showing results from 1 to 11 of 11. Query took 0.1s, moments ago.

|    | asset      |
|----|------------|
| 1  | ex3:asset1 |
| 2  | ex3:asset2 |
| 3  | ex4:asset1 |
| 4  | ex4:asset2 |
| 5  | ex4:asset3 |
| 6  | ex4:asset4 |
| 7  | ex4:asset5 |
| 8  | ex4:asset6 |
| 9  | ex4:asset7 |
| 10 | ex4:asset8 |
| 11 | ex4:asset9 |

## SPARQL Query & Update

first\_repository

Editor only Editor and results Results only

Unnamed × Unnamed × Unnamed × Unnamed × Unnamed × Unnamed × Unnamed ×

```
1 PREFIX af: <https://vz-risk.github.io/flow/attack-flow/>
2 PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
3 SELECT DISTINCT ?action
4 WHERE {
5   ?s rdf:type af:action .
6   ?s rdf:type ?action
7   FILTER(STRSTARTS(STR(?action), "https://veriscommunity.net/attack-flow/"))
8 }
```

Run

keyboard shortcuts

Table Raw Response Pivot Table Google Chart Download as

Filter query results Showing results from 1 to 10 of 10. Query took 0.1s, moments ago.

|    | action                          |
|----|---------------------------------|
| 1  | veris:Phishing                  |
| 2  | veris:Ransomware                |
| 3  | veris:Use%20of%20stolen%20creds |
| 4  | veris:RAM%20scrapers            |
| 5  | veris:Adminware                 |
| 6  | veris:RAT                       |
| 7  | veris:Profile%20host            |
| 8  | veris:Exploit%20vuln            |
| 9  | veris:Pass%20the%20hash         |
| 10 | veris:OS%20commanding           |

# Analysis

## SPARQL Query & Update

first\_repository

Editor only Editor and results Results only

Unnamed × Unnamed × Unnamed × Unnamed × Unnamed × Unnamed × Unnamed ×

Unnamed ×

```
1 PREFIX af: <https://vz-risk.github.io/flow/attack-flow/>
2 PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
3 SELECT DISTINCT ?asset
4 WHERE {
5   ?asset rdf:type af:asset .
6 }
```

Run

keyboard shortcuts

Table Raw Response Pivot Table Google Chart Download as

Filter query results Showing results from 1 to 11 of 11. Query took 0.1s, moments ago.

|    | asset      |
|----|------------|
| 1  | ex3:asset1 |
| 2  | ex3:asset2 |
| 3  | ex4:asset1 |
| 4  | ex4:asset2 |
| 5  | ex4:asset3 |
| 6  | ex4:asset4 |
| 7  | ex4:asset5 |
| 8  | ex4:asset6 |
| 9  | ex4:asset7 |
| 10 | ex4:asset8 |
| 11 | ex4:asset9 |

## SPARQL Query & Update

first\_repository

Editor only Editor and results Results only

Unnamed × Unnamed × Unnamed × Unnamed × Unnamed × Unnamed × Unnamed ×

```
1 PREFIX af: <https://vz-risk.github.io/flow/attack-flow/>
2 PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
3 SELECT DISTINCT ?action
4 WHERE {
5   ?s rdf:type af:action .
6   ?s rdf:type ?action
7   FILTER(STRSTARTS(STR(?action), "https://veriscommunity.net/attack-flow/"))
8 }
```

Run

keyboard shortcuts

Table Raw Response Pivot Table Google Chart Download as

Filter query results Showing results from 1 to 10 of 10. Query took 0.1s, moments ago.

|   | action                          |
|---|---------------------------------|
| 1 | veris:Phishing                  |
| 2 | veris:Ransomware                |
| 3 | veris:Use%20of%20stolen%20creds |
| 4 | veris:RAM%20scraper             |
| 5 | veris:Adminware                 |
| 6 | veris:RAT                       |
| 7 | veris:Profile%20host            |
| 8 | veris:Exploit%20vuln            |

[https://github.com/center-for-threat-informed-defense/attack\\_to\\_veris](https://github.com/center-for-threat-informed-defense/attack_to_veris)

# Impact

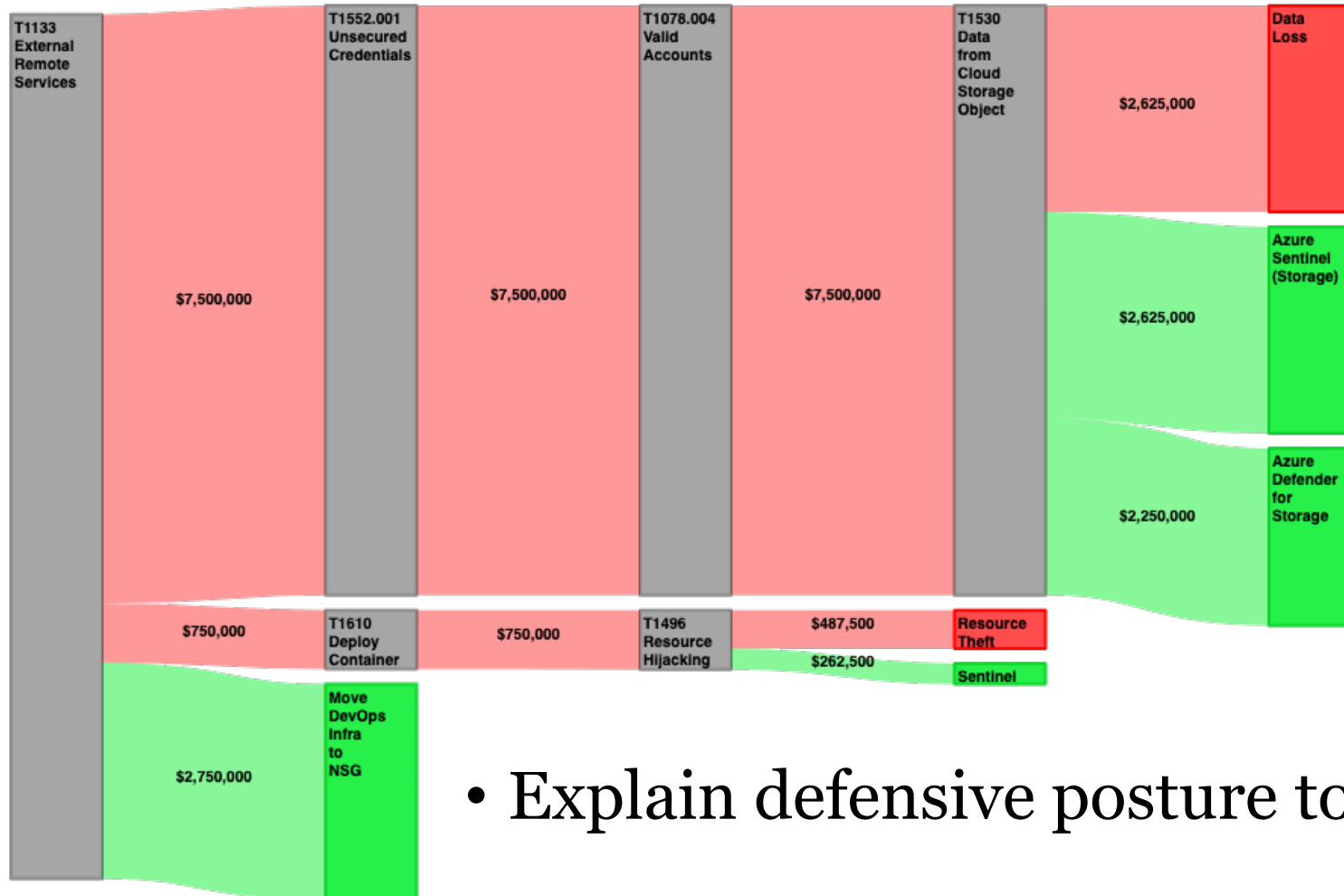
# Better Communication

- Document incident lessons learned
- Visualize IR/Threat Intel/Red Team data
  - Aggregate like nodes & actions
  - Filter tangential properties to simplify
- Explain defensive posture to executives





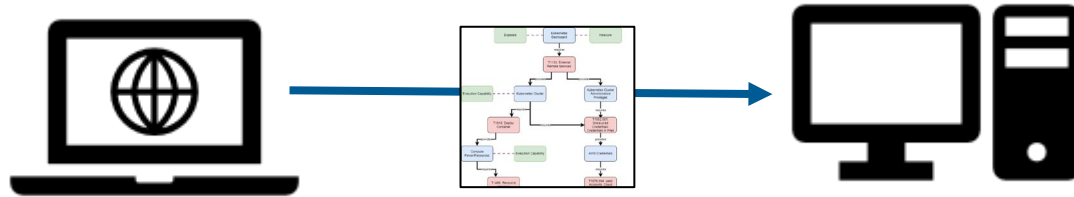
# Better Communication



- Explain defensive posture to executives

# Better Intelligence Exchange

- Attack flow sightings can be shared machine-to-machine
- Graph pattern communication



# Better Operations

- Attack flow queries
- Determining paths to/from an adversary technique difficult to mitigate
- Query datasets for strategic insights (what happens the most → most important for me to mitigate)



SPARQL Query & Update ⓘ Editor only Editor and results Results only ⏏

first\_repository ▾

```
1 PREFIX af: <https://vz-risk.github.io/flow/attack-flow/>
2 PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
3 SELECT DISTINCT ?action
4 WHERE {
5   ?s rdf:type af:action .
6   ?s rdf:type ?action
7   FILTER(STRSTARTS(STR(?action), "https://veriscommunity.net/attack-flow/"))
8 }
```

Run keyboard shortcuts

Table Raw Response Pivot Table Google Chart Download as ▾

Filter query results Showing results from 1 to 10 of 10. Query took 0.1s, moments ago.

|    | action                                          |
|----|-------------------------------------------------|
| 1  | <a href="#">veris:Phishing</a>                  |
| 2  | <a href="#">veris:Ransomware</a>                |
| 3  | <a href="#">veris:Use%20of%20stolen%20creds</a> |
| 4  | <a href="#">veris:RAM%20scraper</a>             |
| 5  | <a href="#">veris:Adminware</a>                 |
| 6  | <a href="#">veris:RAT</a>                       |
| 7  | <a href="#">veris:Profile%20host</a>            |
| 8  | <a href="#">veris:Exploit%20vuln</a>            |
| 9  | <a href="#">veris:Pass%20the%20hash</a>         |
| 10 | <a href="#">veris:OS%20commanding</a>           |

# Better Defensive Planning

- Understand attack surfaces (attack graph generation)
- Analyze risk
- Aggregate attack flows
- Build and communicate non-atomic detections
  - Hinges on data in records being properties that are connected to ground-truth actions and assets
- Identify cyberthreat choke points
  - Enables disruption of the adversary's attack model

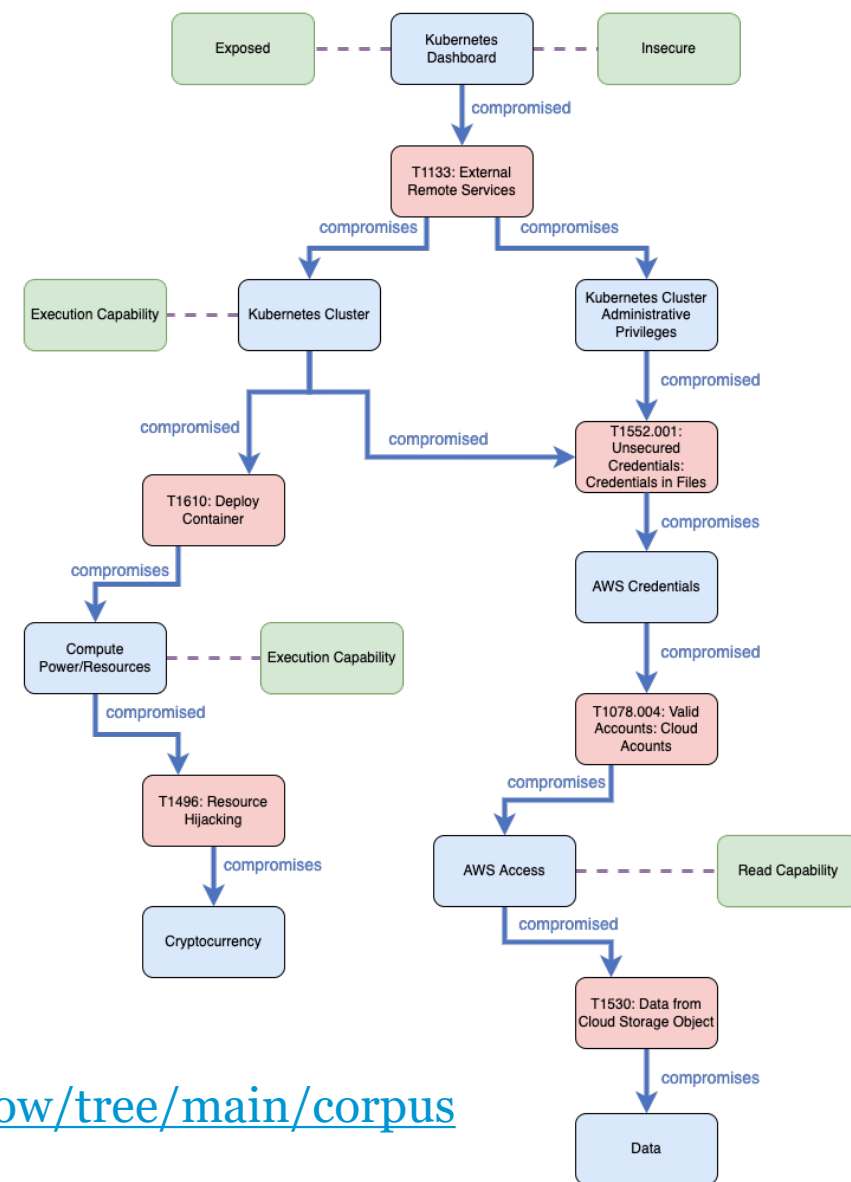
# Better Assessments

- Build Realistic Adversary Emulation Scenarios
  - Data driven red teaming
  - Subgraphs are key and are strung together:  
*If we succeed in action X on an asset, then we will attempt action Y from that asset*
- Pen Testing
- Breach and Attack Simulation
  - Logic operator is key
  - Pair attack flow with planner & choose from available options

# Attack Flow Corpus\*

- Operation Cobalt Kitty
- Conti Ransomware Incident
- “From Zero to Domain Admin”
- “Mac Malware Steals Cryptocurrency”
- “Right to Left Override”
- Tesla’s Kubernetes Breach

\* <https://github.com/center-for-threat-informed-defense/attack-flow/tree/main/corpus>



# Please Contribute

Become an early adopter!

- Prototype capabilities
- Create structured reports – submit attack flows to corpus
- Provide feedback as GitHub issues
- Project Summary
  - <https://ctid.mitre-engenuity.org/our-work/attack-flow>
- “Attack Flow – Beyond Atomic Indicators”
  - <https://medium.com/mitre-engenuity/attack-flow-beyond-atomic-behaviors-c646675cc793>
- GitHub
  - <https://github.com/center-for-threat-informed-defense/attack-flow>
  - <https://github.com/vz-risk/flow>

# Questions?



Center  
for Threat  
Informed  
Defense