MITRE ENGENUITY | 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

+

MITRE

SOLVING PROBLEMS FOR A SAFER WORLD™

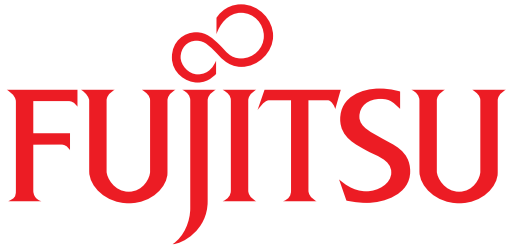
Membership is:

- ❑ 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
Proiects Underway	4
Published Projects	17

Attack Flow Participants



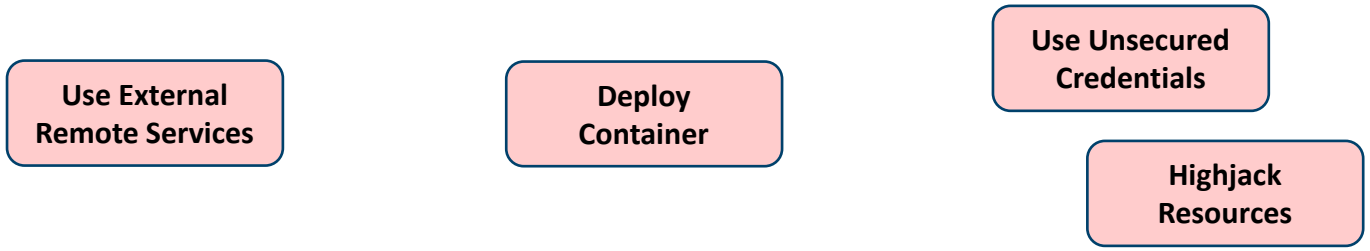
Outline

- 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?

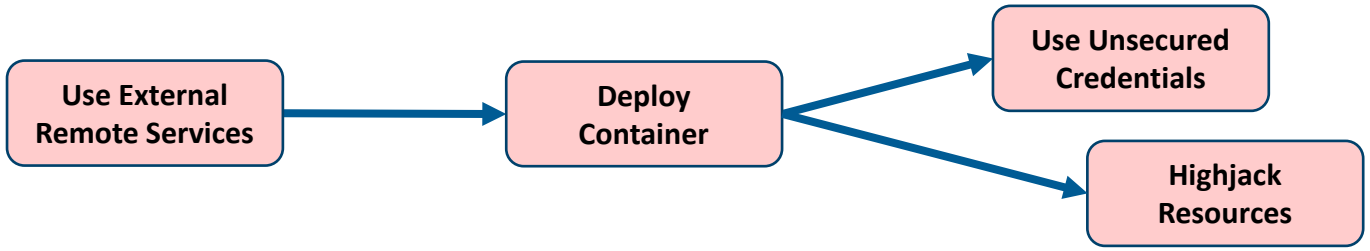
- Defenders track adversary behaviors individually, but adversaries use *sequences* of techniques



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

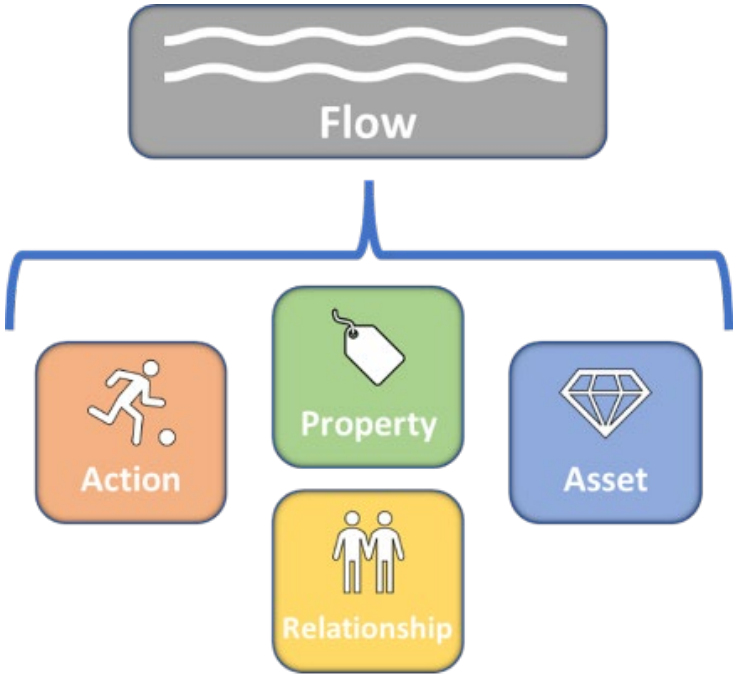
What's the Problem?

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



Sequences of techniques create *relationships*

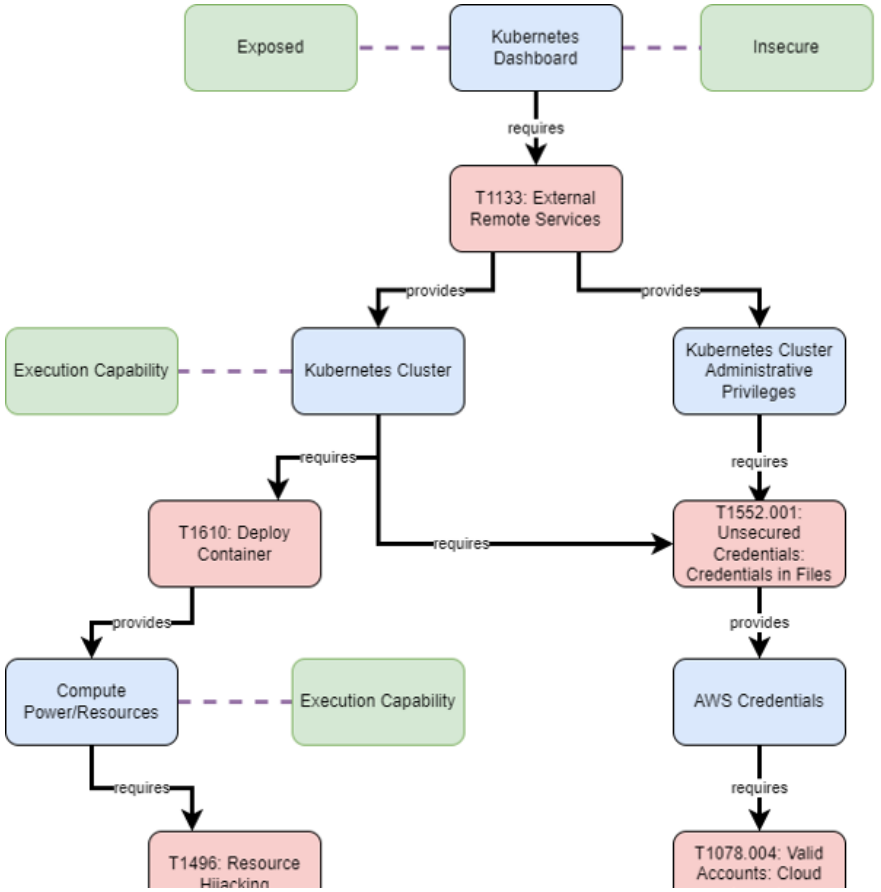
What's an Attack Flow?



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

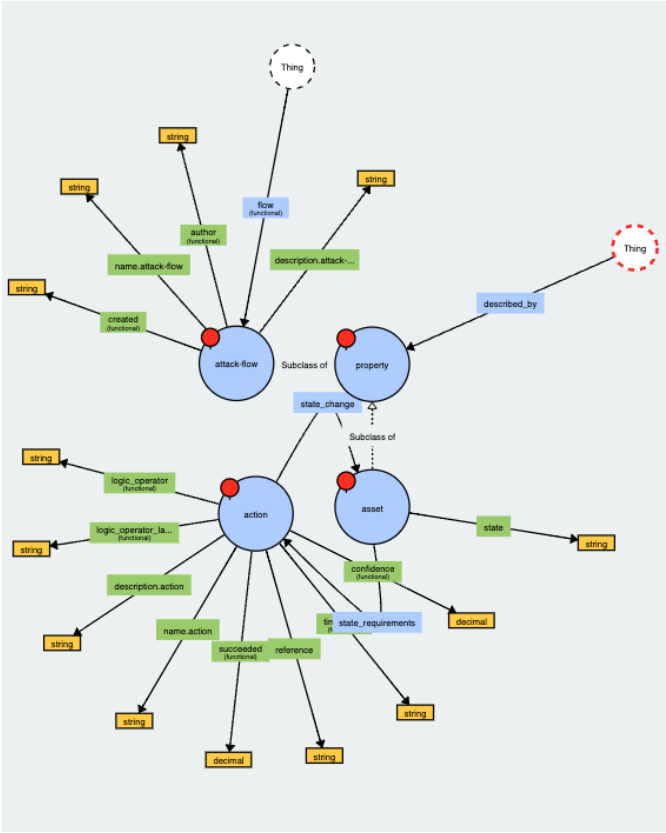
Learn by example

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

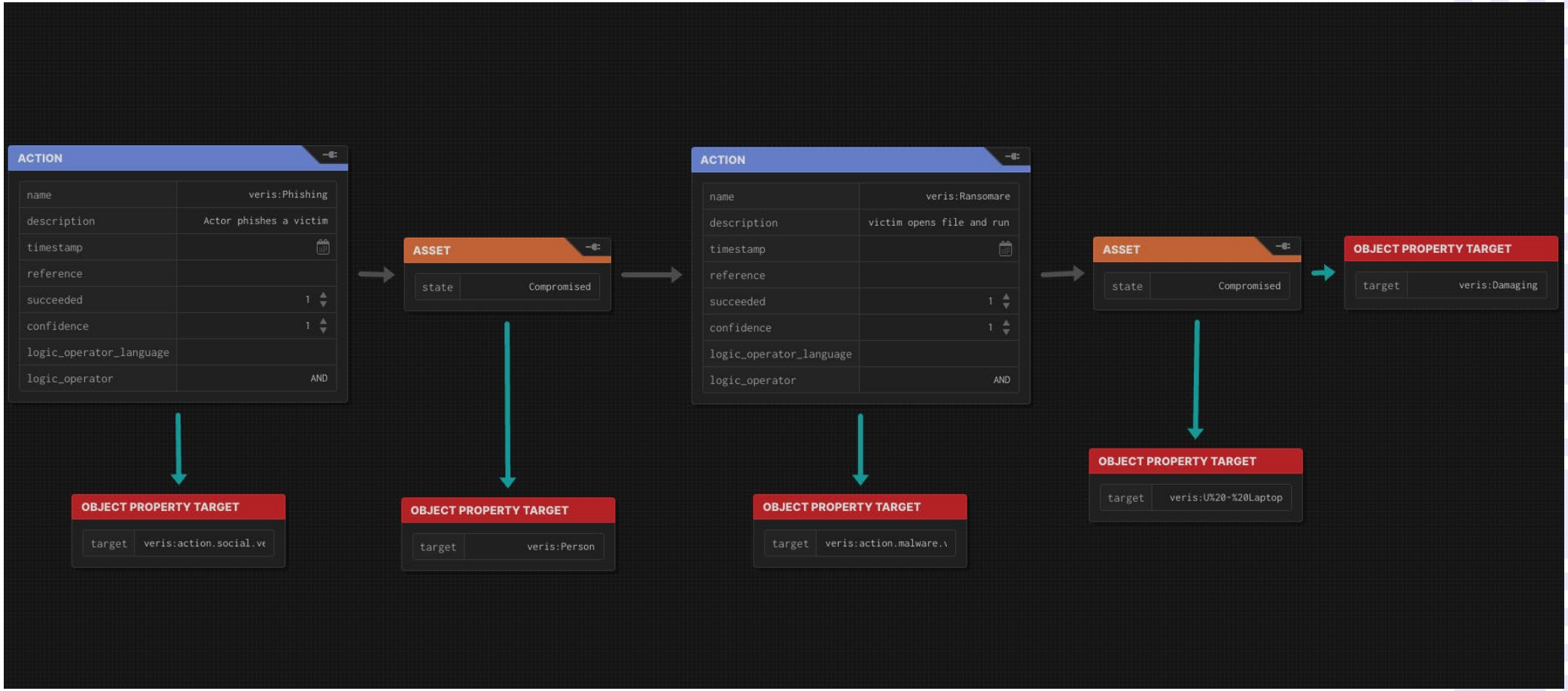
* Mail logs show User A receives phishing email and opens attached macro-enabled word document on Host B
* Proxy and host logs detect Host B beaconing to known C2, downloading the ransomware, and running it

- 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

```
{
  "$schema": "../schema/attack-flow-2021-11-03-draft.json",
  "actions": [
    {
      "description": "actor phishes a victim",
      "id": "urn:absolute:example_3#action1",
      "logic_operator": "AND",
      "name": "action1"
    },
    {
      "description": "victim opens file and runs macro that installs ransomware",
      "id": "urn:absolute:example_3#action2",
      "logic_operator": "AND",
      "name": "action2"
    }
  ],
  "assets": [
    {
      "id": "urn:absolute:example_3#asset1"
    },
    {
      "id": "urn:absolute:example_3#asset2"
    }
  ],
  "data_properties": [],
  "flow": {
    "created": "2022-04-11T16:39:00",
    "id": "urn:absolute:example_3#example_flow3",
    "name": "example_flow3",
    "type": "attack-flow"
  },
  "object_properties": [],
  "relationships": [
    {
      "source": "urn:absolute:example_3#asset1",
      "target": "urn:absolute:example_3#action2",
      "type": "https://vz-risk.github.io/flow/attack-flow/state_requirement"
    },
    {
      "source": "urn:absolute:example_3#action1",
      "target": "urn:absolute:example_3#asset1",
```

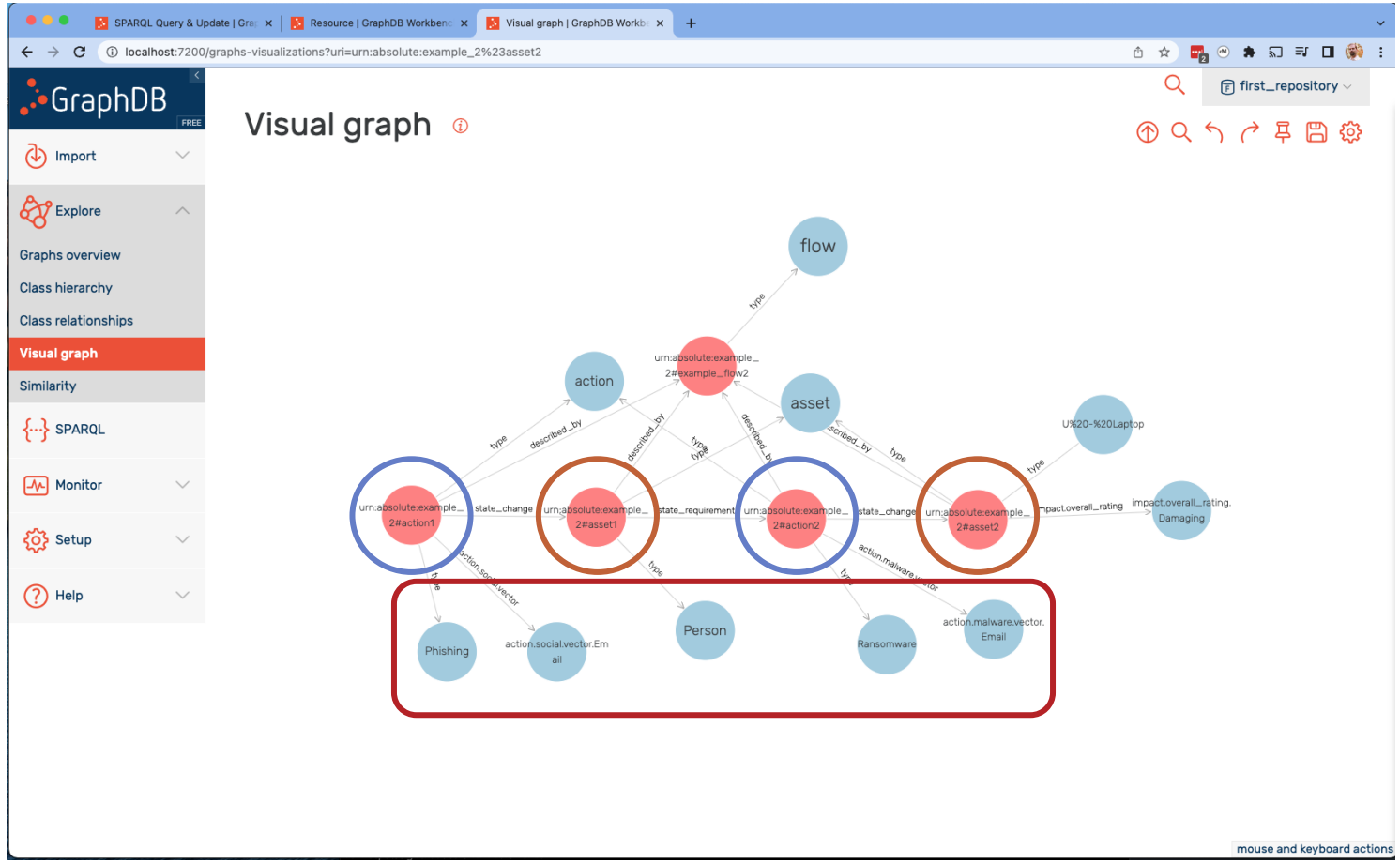
Storage – JSON-LD (Linked Data)

PREFIX owl: <http://www.w3.org/2002/07/owl#>

```
[
{
    "@id": " https://example.com/example_2#action1",
    "@type": ["http://www.w3.org/2002/07/owl#NamedIndividual", "https://veriscommunity.net/attack-flow/Phishing", "https://vz-risk.github.io/flow/attack_flow/action"],
    "https://veriscommunity.net/attack-flow/action.social.vector": [
    {
        "@id": "https://veriscommunity.net/attack-flow/action.social.vector.Email"
    }],
    "https://vz-risk.github.io/flow/attack_flow/description": [
    {
        "@value": "actor phishes a victim"
    }],
    "https://vz-risk.github.io/flow/attack_flow/logic_operator": [
    {
        "@value": "AND"
    }],
    "https://vz-risk.github.io/flow/attack_flow/state_change": [
    {
        "@id": " https://example.com/example_2#asset1"
    }],
    "https://vz-risk.github.io/flow/attack_flow/described_by": [
    {
        "@id": " https://example.com/example_2#example_flow2"
    }]
},
{
    "@id": " https://example.com/example_2#action2",
    "@type": ["http://www.w3.org/2002/07/owl#NamedIndividual", "https://vz-risk.github.io/flow/attack_flow/action", "https://veriscommunity.net/attack-flow/Ransomware"],
    "https://vz-risk.github.io/flow/attack_flow/state_change": [
    {
        "@id": " https://example.com/example_2#asset2"
    }],
    "https://veriscommunity.net/attack-flow/action.malware.vector": [
    {
        "@id": "https://veriscommunity.net/attack-flow/action.malware.vector.Email"
    }],
    "https://vz-risk.github.io/flow/attack_flow/described_by": [
    {
        "@id": " https://example.com/example_2#example_flow2"
    }]
},
```

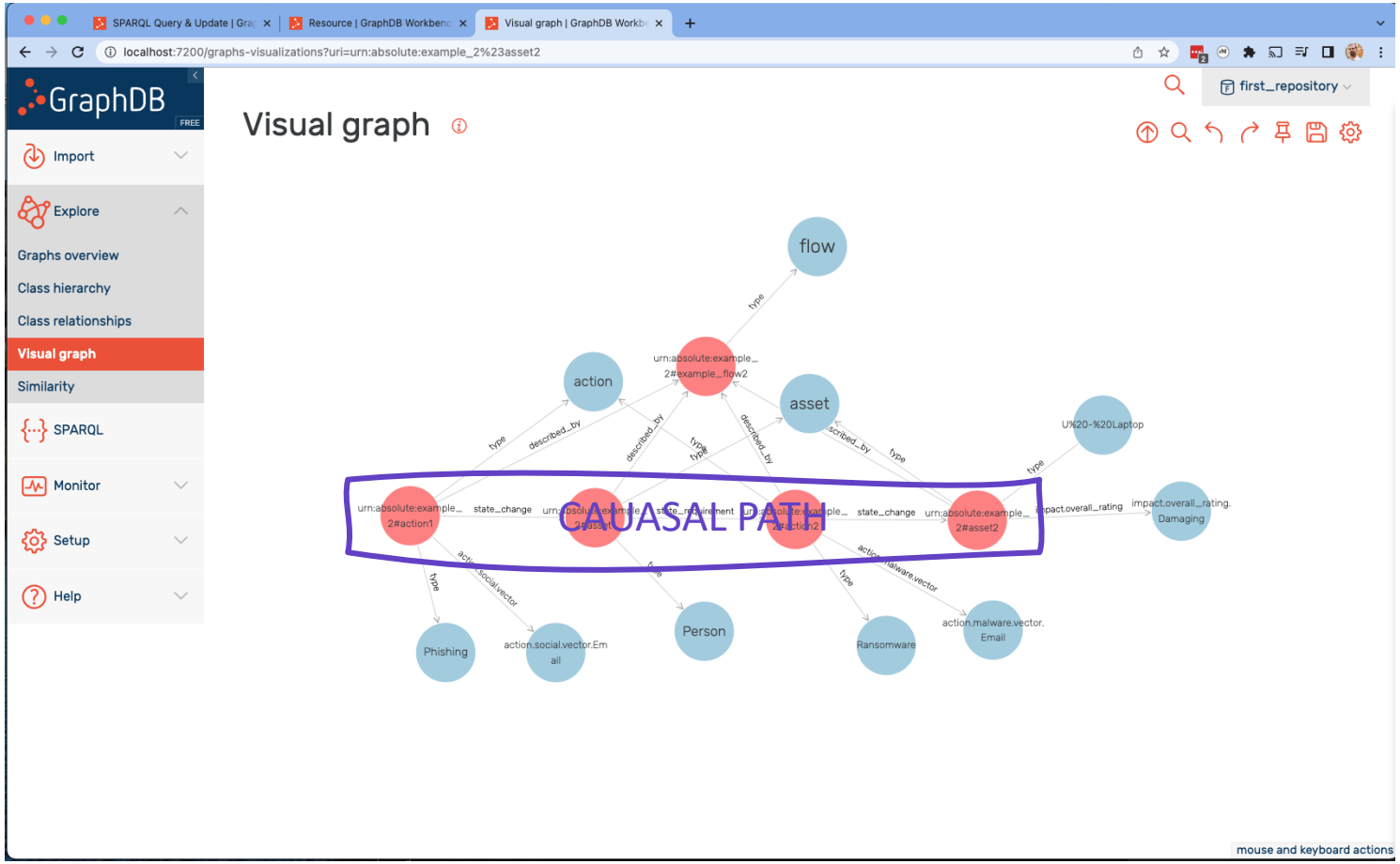
So what's it look like?

Attack Flow Data Format

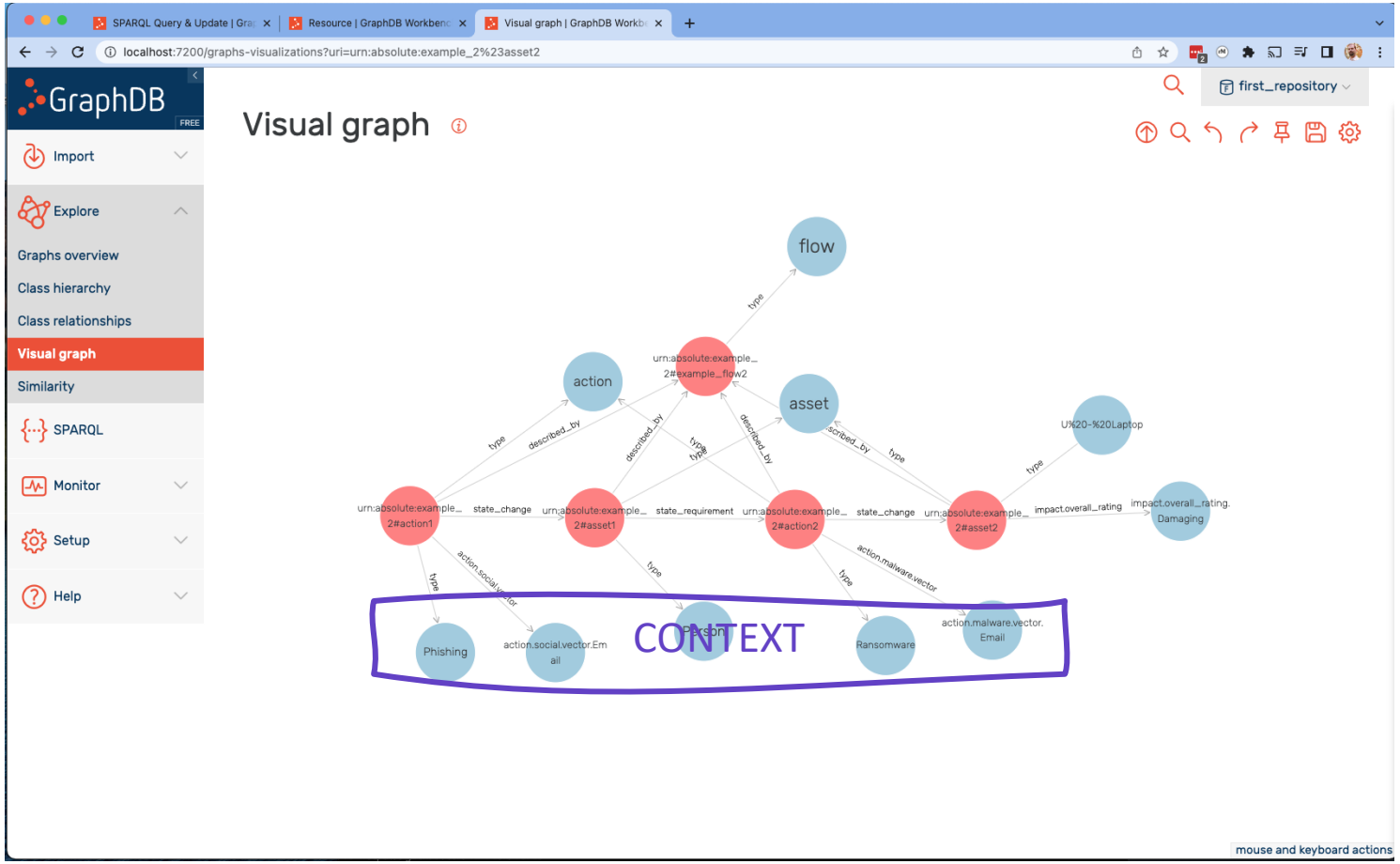


Three C's:
Causality, Context, Complexity

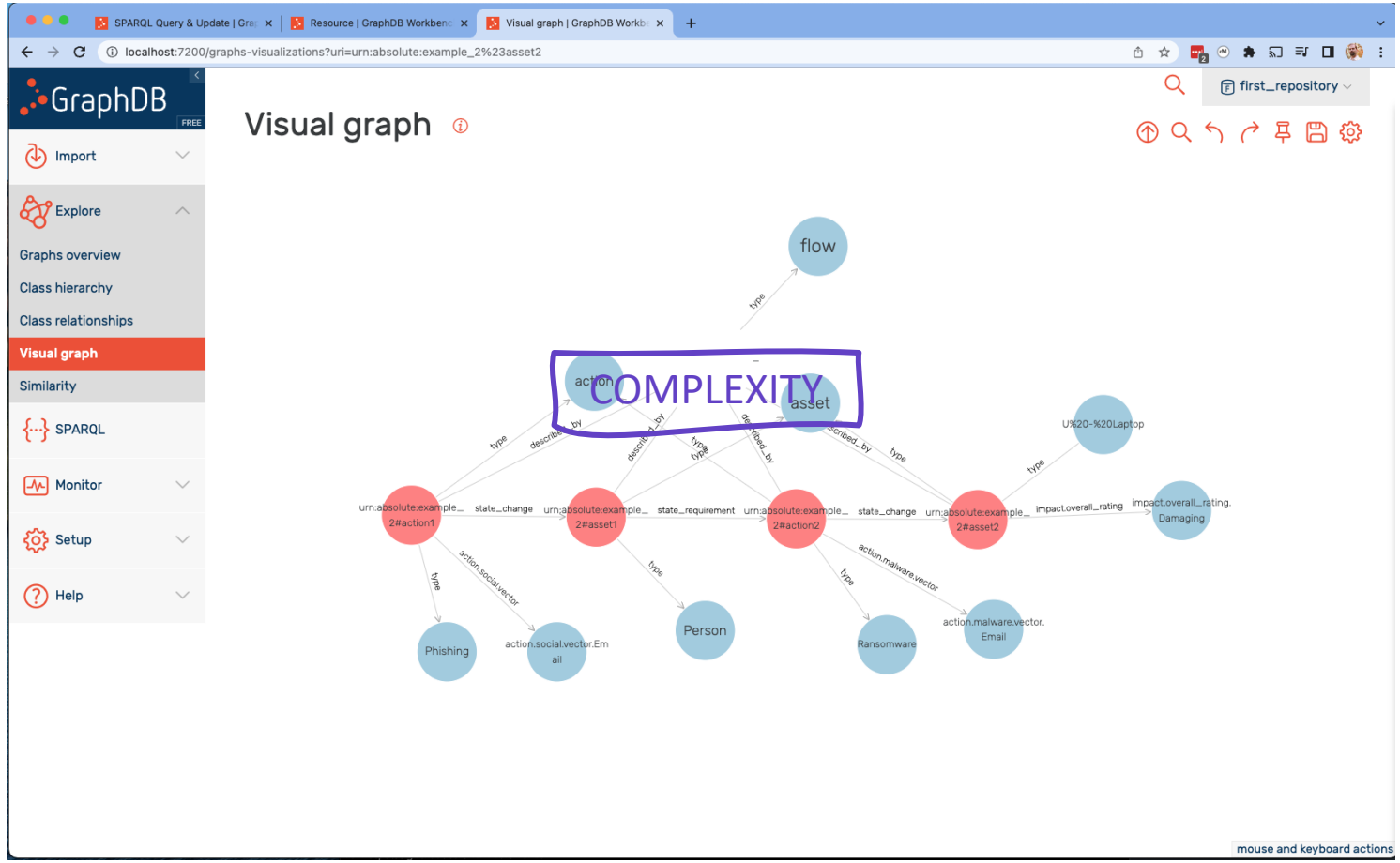
Attack Flow Data Format - Causality



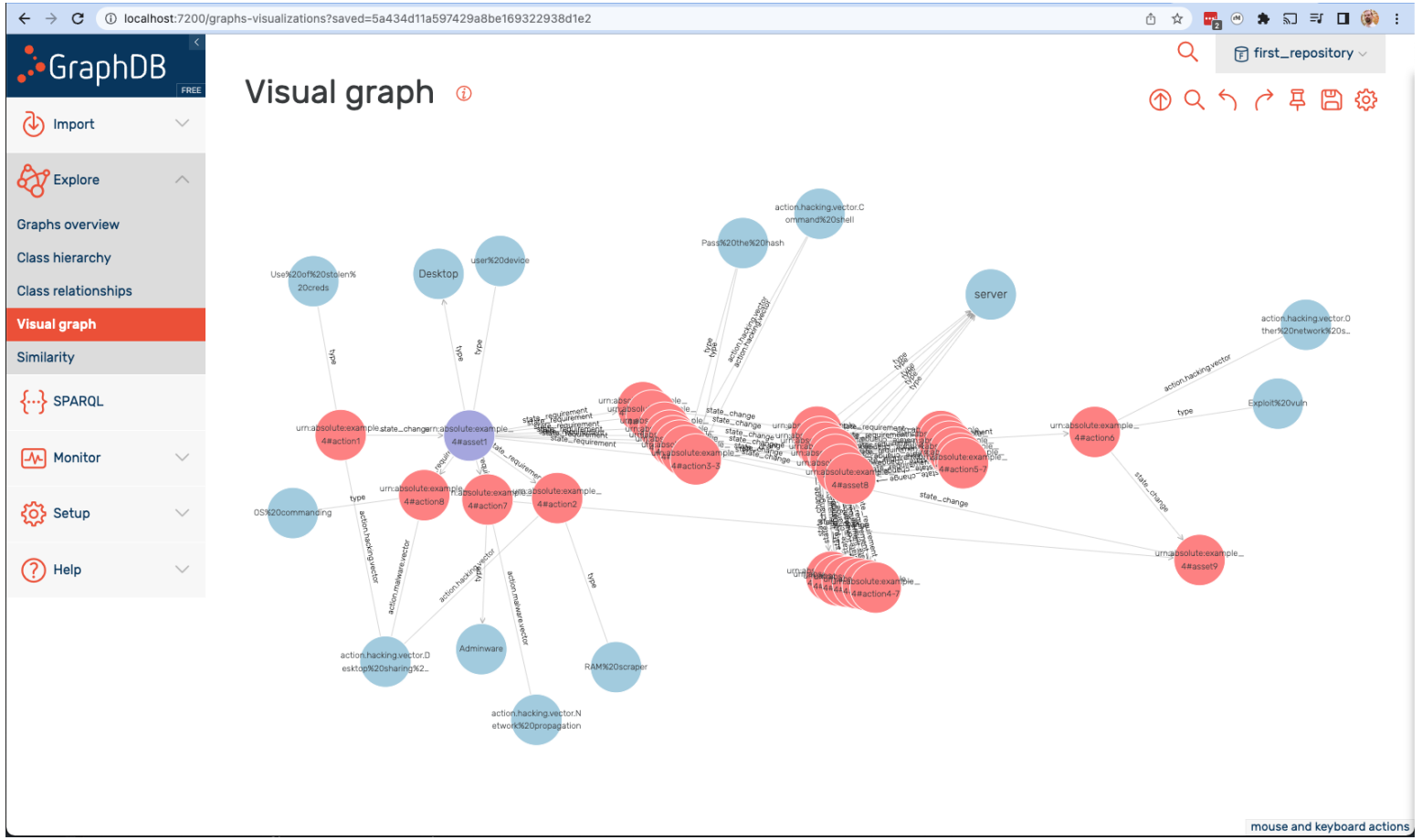
Attack Flow Data Format - Context



Attack Flow Data Format – Complexity



Attack Flow Data Format – Complexity



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

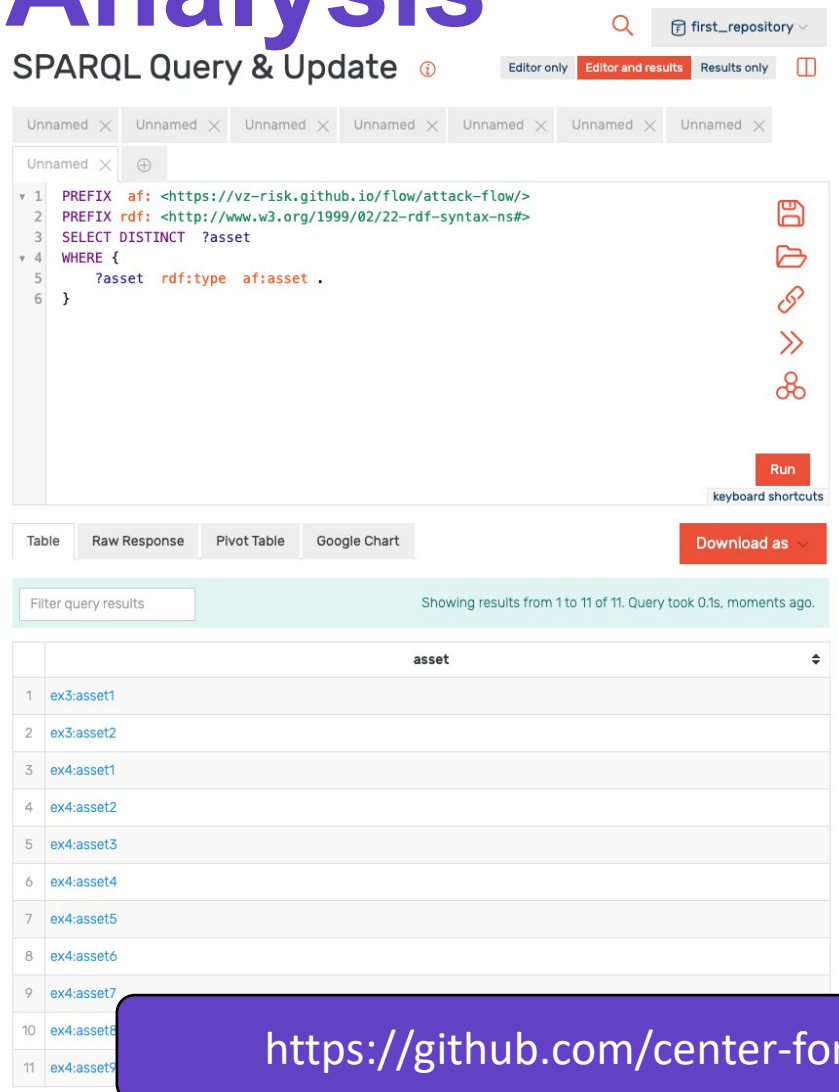
Download as

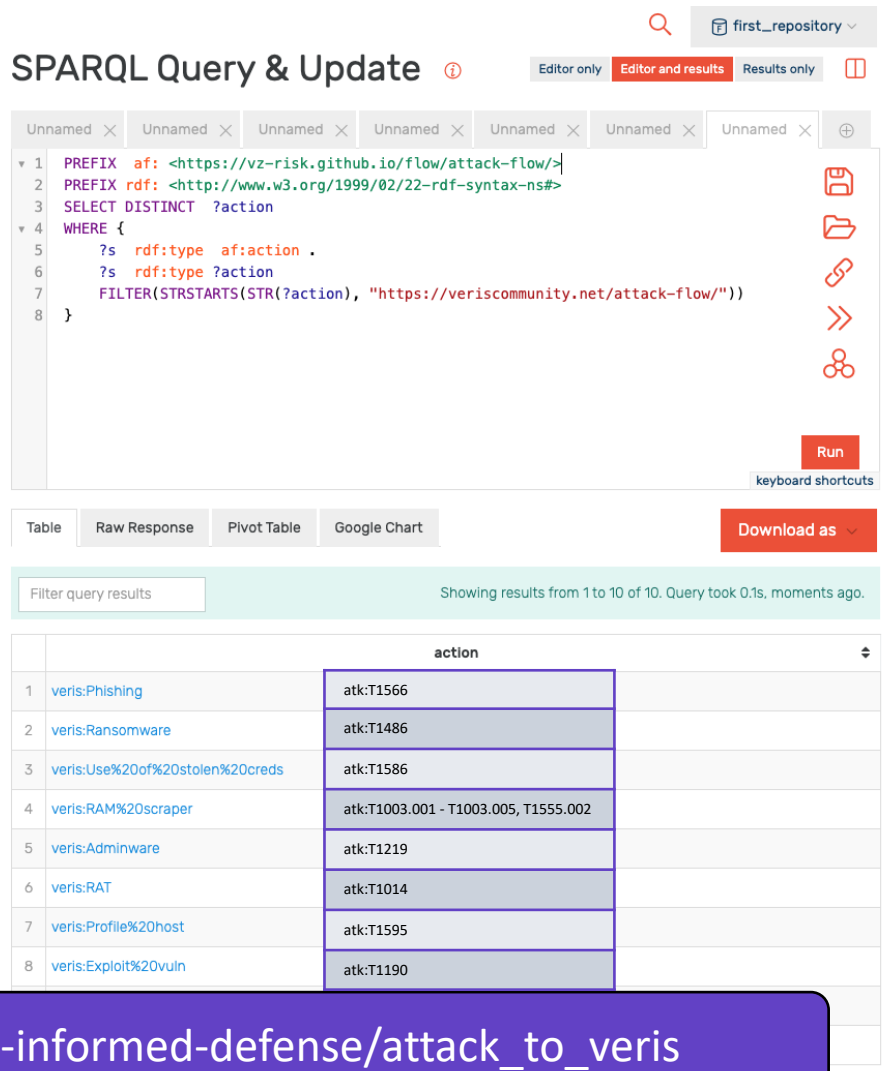
Filter query results

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%20scraper
5	veris:Adminware
6	veris:RAT
7	veris:Profile%20host
8	veris:Exploit%20vuln
9	veris:Pass%20the%20hash
10	veris:OS%20commanding

Analysis





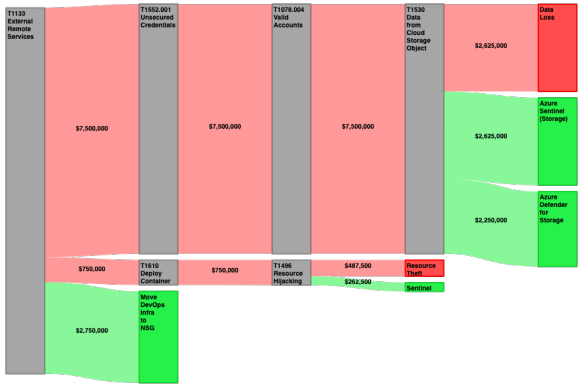
https://github.com/center-for-threat-informed-defense/attack_to_veris

MITRE ENGENUITY | Center for Threat Informed Defense

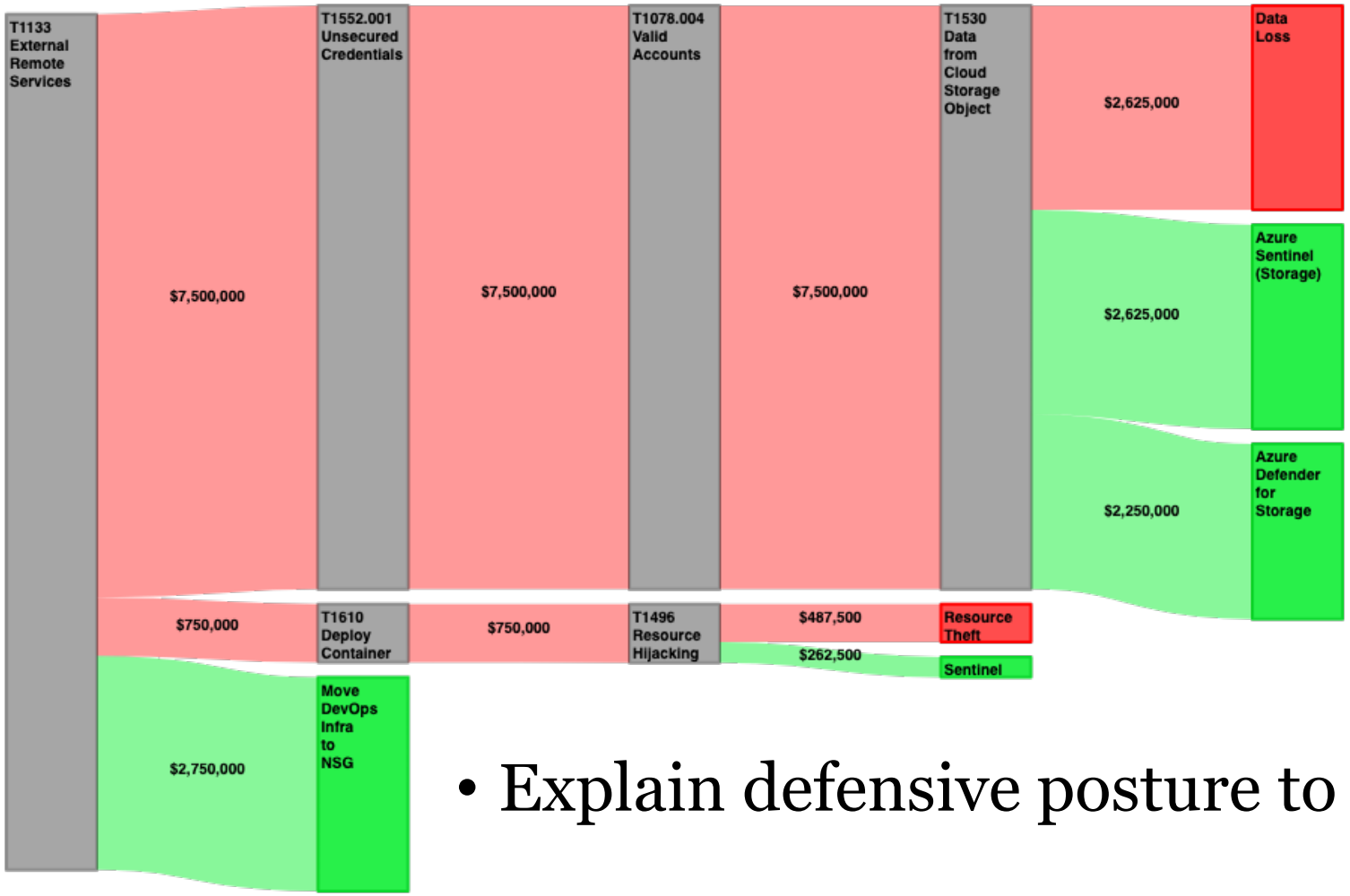
Impact

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



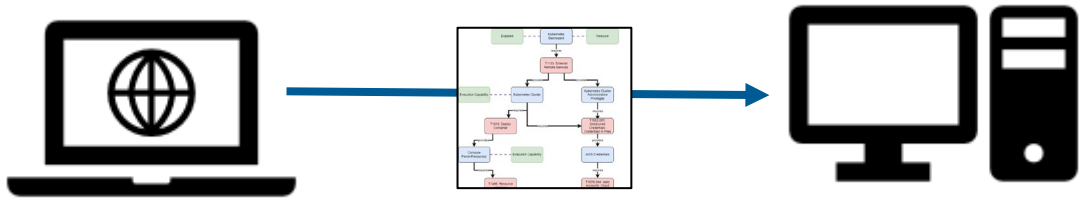
Better Communication



- Explain defensive posture to executives

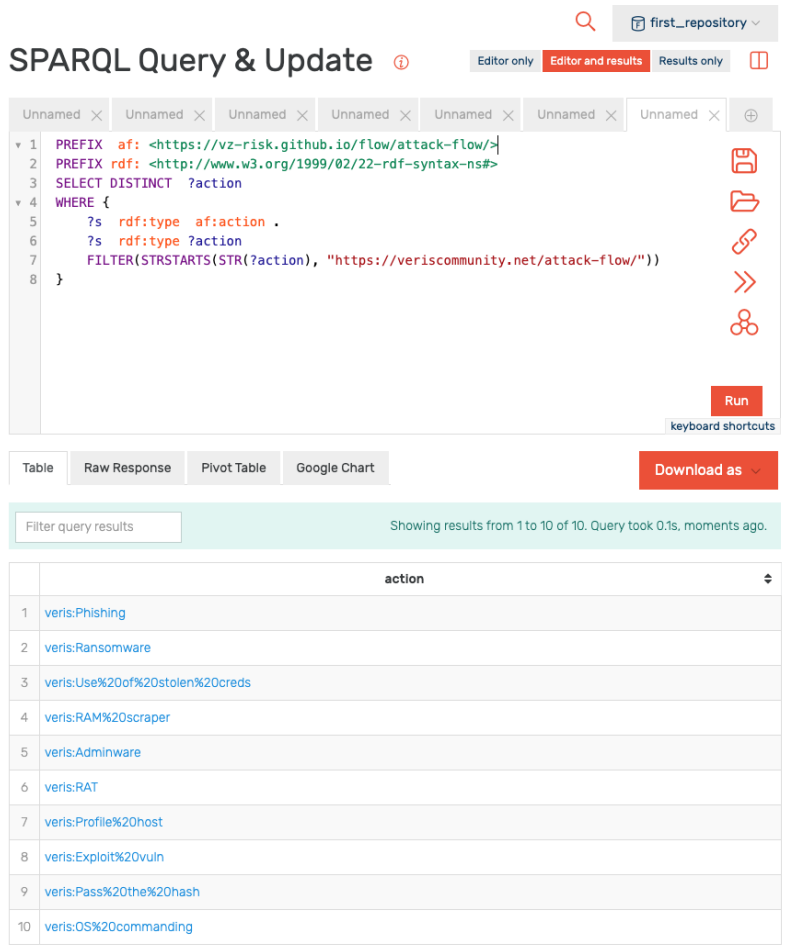
Better Intelligence Exchange

- 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)



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

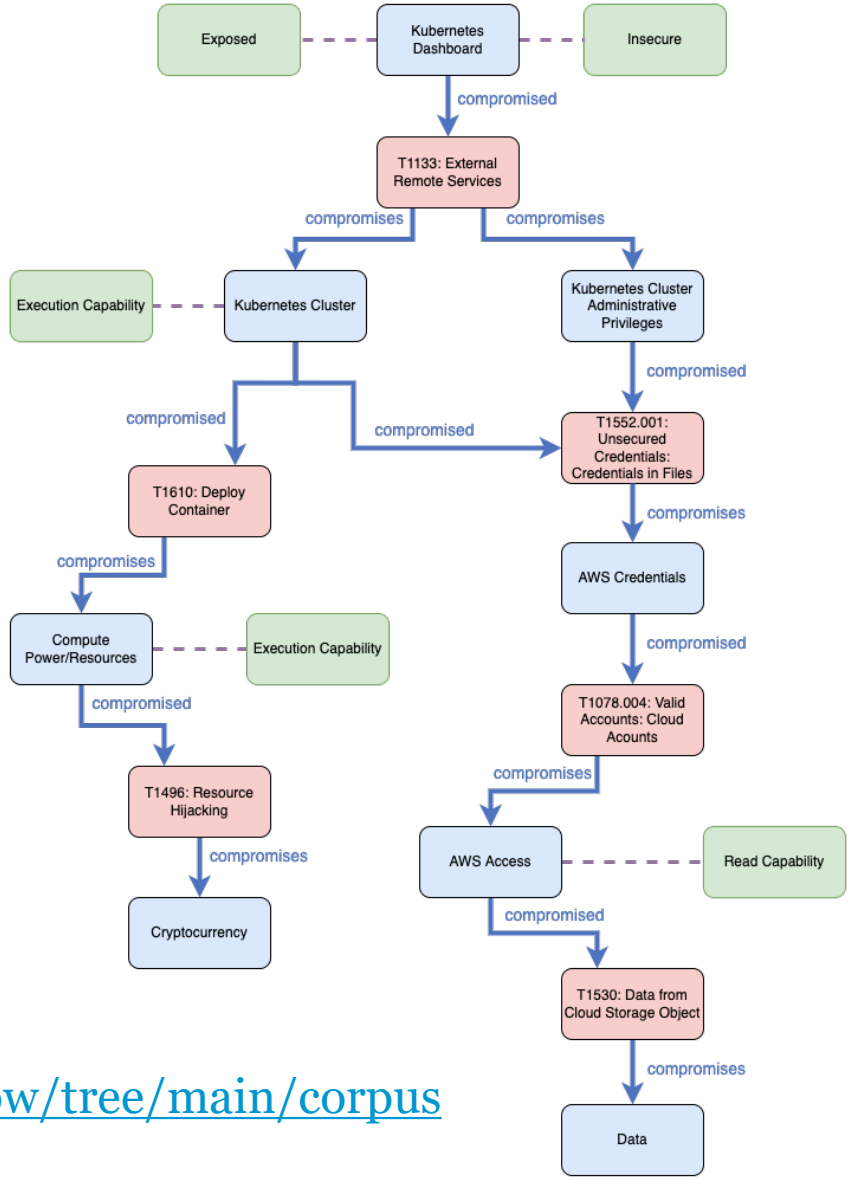
Better Assessments

- 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?