DoD Cyber Crime Center

A Federal Cyber Center

Empowering Cyber Operators with Enhanced CTI Pipelines

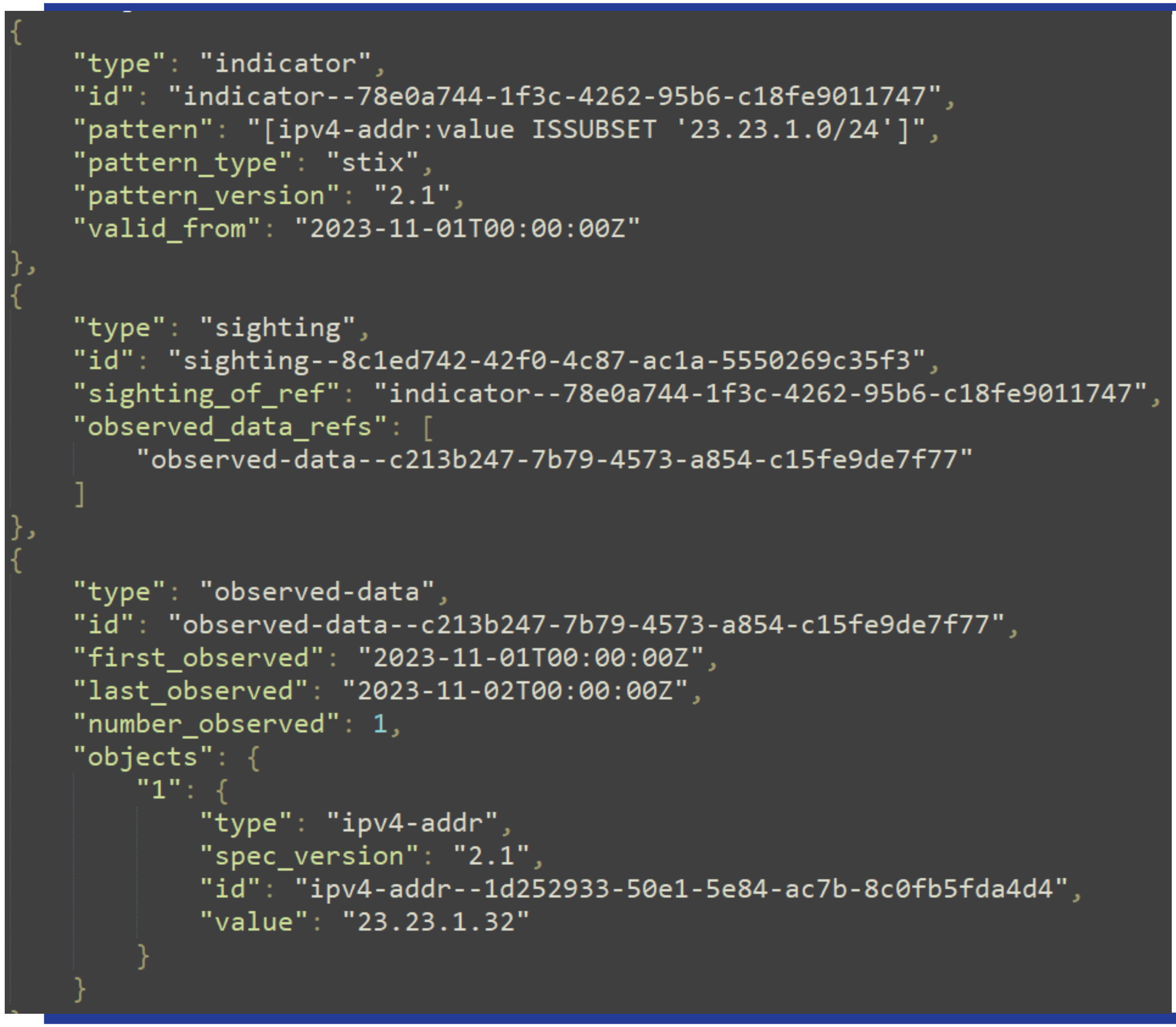
Jeff Mates
Computer Scientist

January 9, 2024

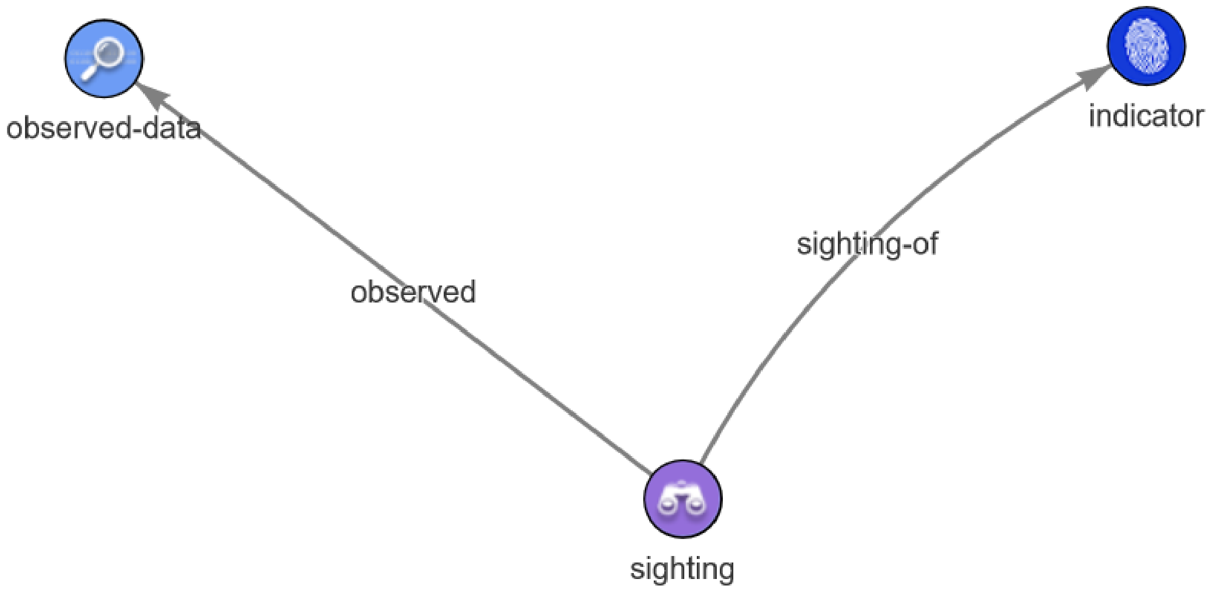
What STIX Is

- A cyber threat information exchange format so that tools can play nicer with each other
- A better way to get tools to talk to each other than CSVs
- A guide on how to structure various forms of CTI data for product backends
- It is an international standard produced by the OASIS Cyber Threat Intelligence Technical Committee (CTI-TC)
- A graph-based model
- JSON or XML depending on the version

STIX JSON / Graph



```
{
    "type": "indicator",
    "id": "indicator--78e0a744-1f3c-4262-95b6-c18fe9011747",
    "pattern": "[ipv4-addr:value ISSUBSET '23.23.1.0/24']",
    "pattern_type": "stix",
    "pattern_version": "2.1",
    "valid_from": "2023-11-01T00:00:00Z"
},
{
    "type": "sighting",
    "id": "sighting--8c1ed742-42f0-4c87-ac1a-5550269c35f3",
    "sighting_of_ref": "indicator--78e0a744-1f3c-4262-95b6-c18fe9011747",
    "observed_data_refs": [
        "observed-data--c213b247-7b79-4573-a854-c15fe9de7f77"
    ]
},
{
    "type": "observed-data",
    "id": "observed-data--c213b247-7b79-4573-a854-c15fe9de7f77",
    "first_observed": "2023-11-01T00:00:00Z",
    "last_observed": "2023-11-02T00:00:00Z",
    "number_observed": 1,
    "objects": {
        "1": {
            "type": "ipv4-addr",
            "spec_version": "2.1",
            "id": "ipv4-addr--1d252933-50e1-5e84-ac7b-8c0fb5fda4d4",
            "value": "23.23.1.32"
        }
    }
```



Note: STIX JSON excludes the following properties:

1. created
2. modified
3. spec_version

Types of Data STIX Models

- **Indicator Sharing**
- **CTI Feeds – Consuming and Producing**
- **Malware Analysis**
- **Sensors**
  - Network Traffic
  - Host Based
- **Vulnerability Reporting**
- **Incident Reporting**
- **Data Fusion**

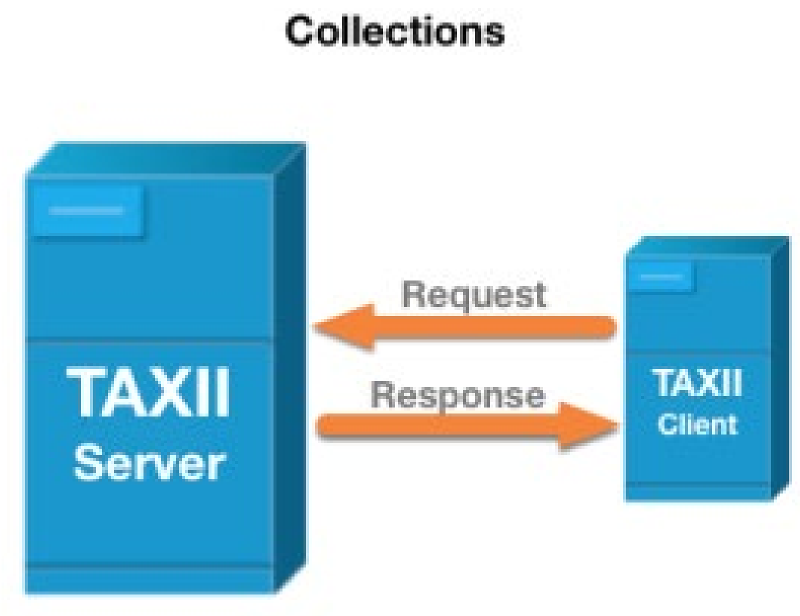
Indicator Sharing

- **Indicators** are patterns
  - valid_from / valid_until
  - confidence
  - pattern
    - STIX Patterning
    - Yara
    - Snort
- **Indicator** indicates...
  - Attack Pattern
  - Campaign
  - Infrastructure
  - Malware / Tool
  - Threat Actor

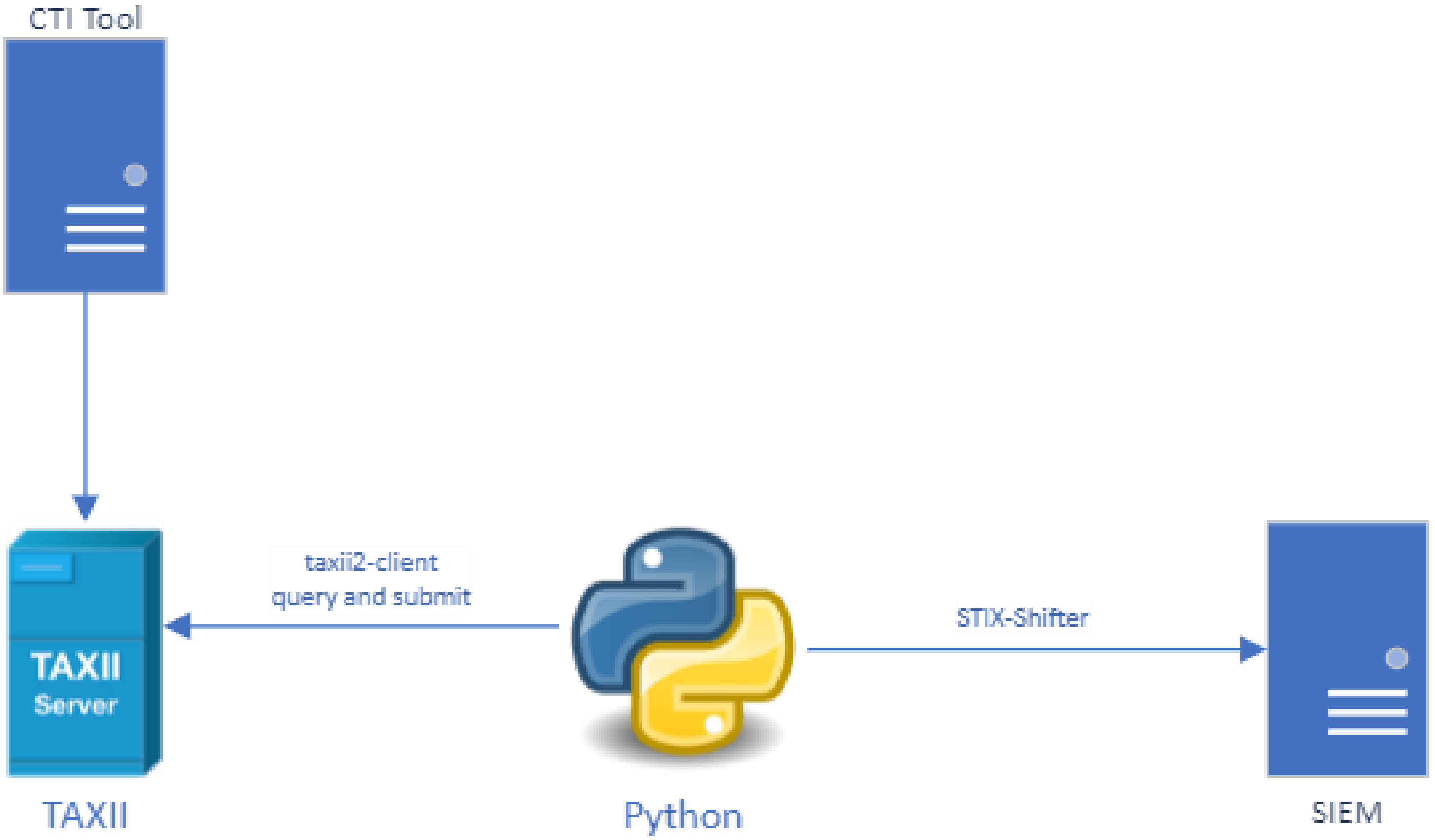
- **Sighting** of **Indicator**
  - start / end
  - confidence
  - References Observed Data
    - Domains
    - Files
    - IPs
    - and more
- **Report**

What about TAXII?

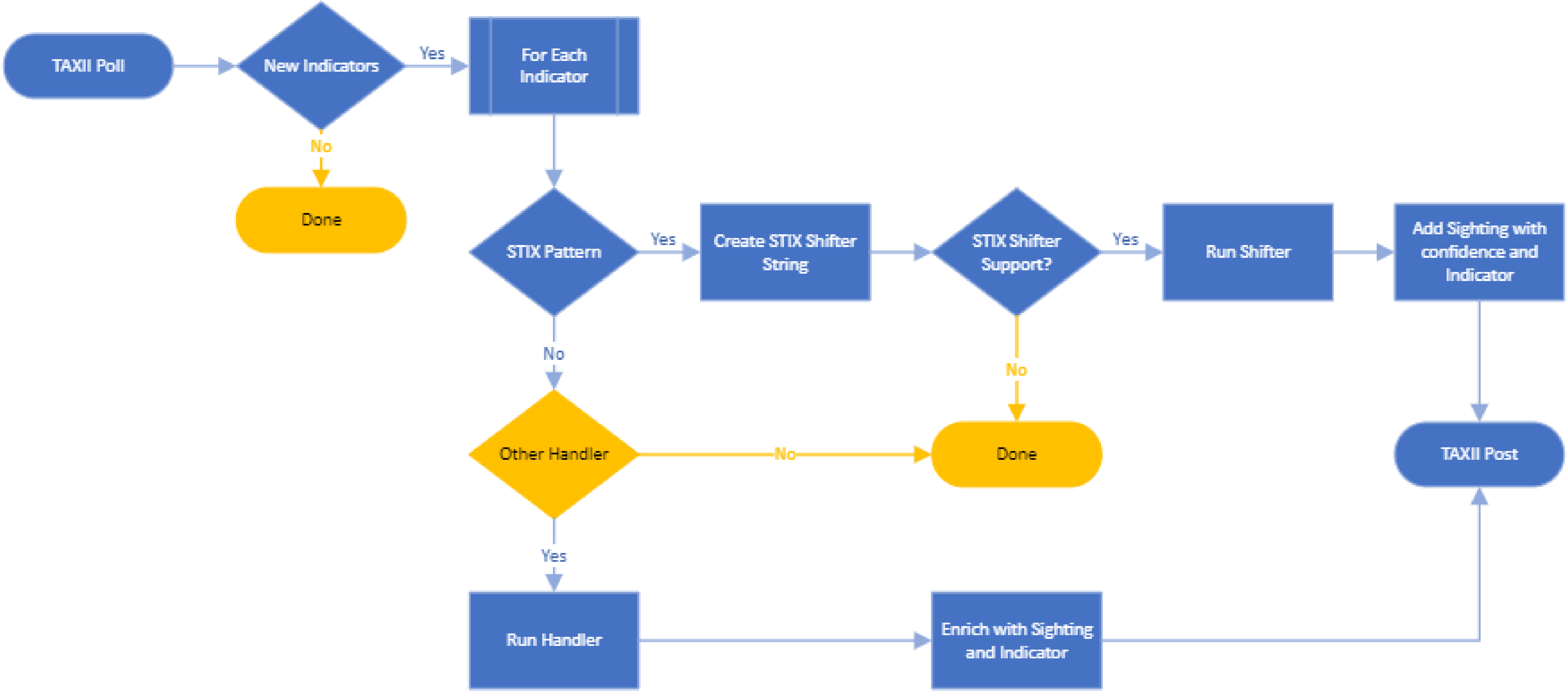
- **A client / server protocol for exchanging STIX content**
  - Clients push data to server
  - Clients poll data from the server
- **Three main types**
  - STIX Storage
  - STIX Ingest
  - STIX Output
- **Multiple Levels of Interoperability**
  - Higher levels support more query options



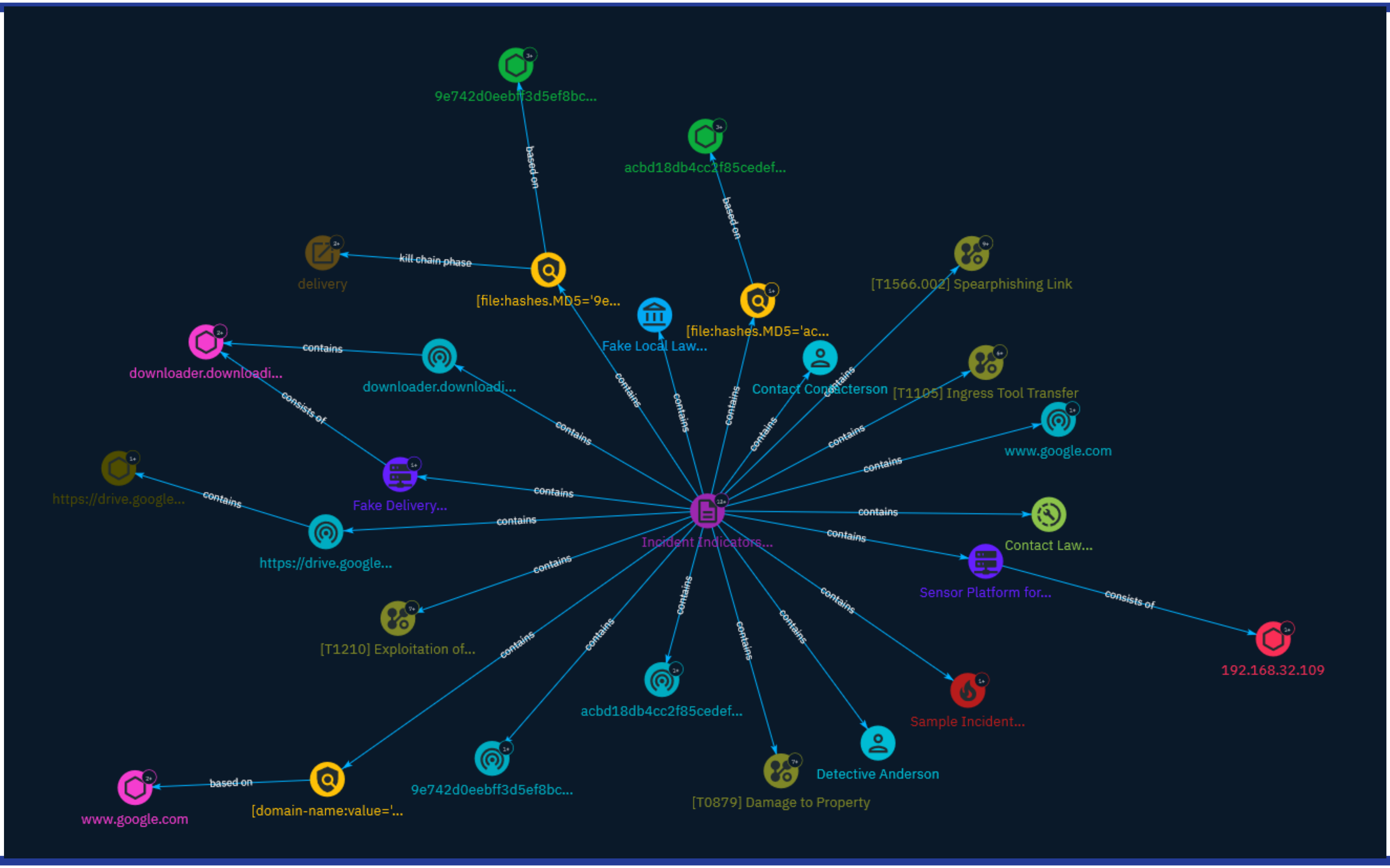
Python TAXII Network



Python TAXII Indicator Flow



OpenCTI


9e742d0eebff3d5ef8bc...
based on
acbd18db4cc2f85cedef...
based on
delivery
kill chain phase
[file:hashes.MD5='9e...
[file:hashes.MD5='ac...
Fake Local Law...
[T1566.002] Spearphishing Link
downloader.downloadi...
contains
downloader.downloadi...
Contact Conactperson
[T1105] Ingress Tool Transfer
consists of
www.google.com
https://drive.google...
Fake Delivery...
contains
https://drive.google...
Incident Indicators...
Contact Law...
Sensor Platform for...
consists of
192.168.32.109
[T1210] Exploitation of...
acbd18db4cc2f85cedef...
Sample Incident...
Detective Anderson
9e742d0eebff3d5ef8bc...
[T0879] Damage to Property
www.google.com
based on
[domain-name:value='...

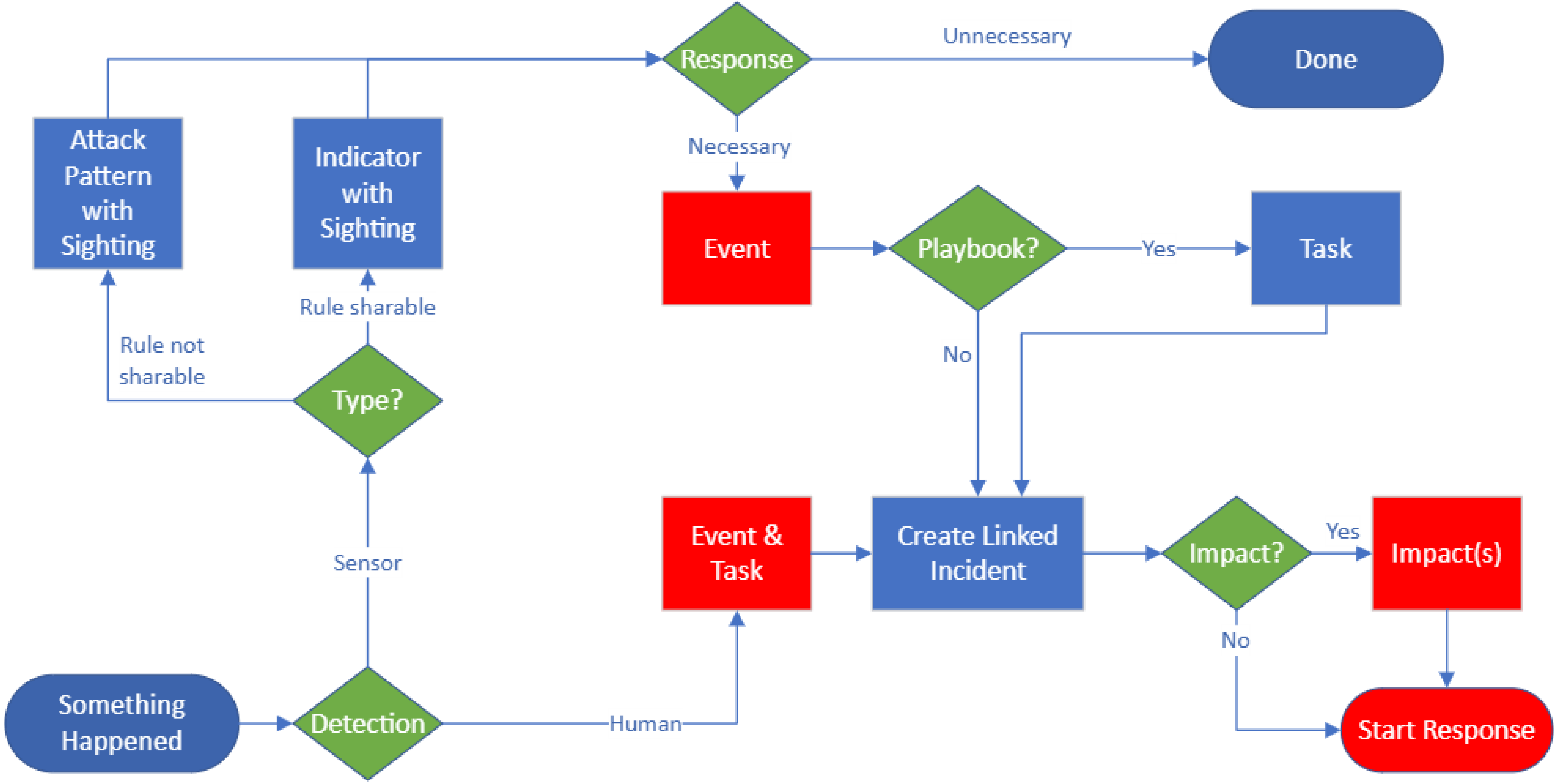
TAXII Poll

- **Filter for Indicators -** ?match[type]=indicator
  - Pros:
    - Easy
  - Cons:
    - No native context
- **Filter to Reports -** ?match[type]=report
  - Query all indicators and identities in each report separately
    - ?match[id]=indicator--3600ad1b-fff1-4c98-bcc9-4de3bc2e2ffb,identity--f1e3042d-5397-47e7-890c-c2040812314c
  - Pros:
    - Allows for more enrichment
  - Cons:
    - Not all indicators are in Reports
    - Slower with more code

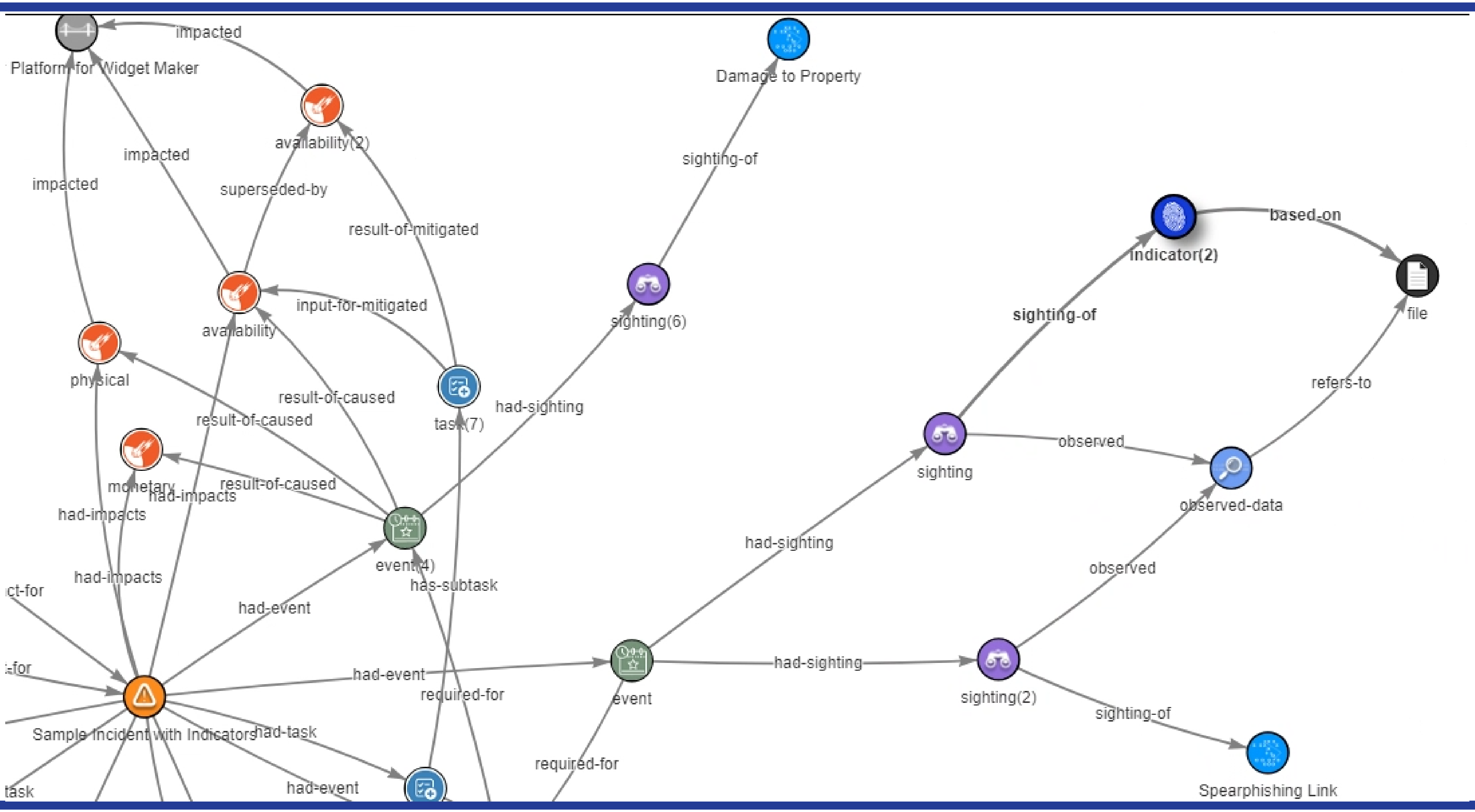
Incident Reporting

- **Next major item for STIX**
  - Incident Rollup Data / Cases
  - Events – Bad activities
  - Impacts – The boom
  - Tasks – Defender activities
- **Direct SIEM submissions**
  - Share actual observables no more regex for IoCs
- **Uses well known objects for easier adoption**

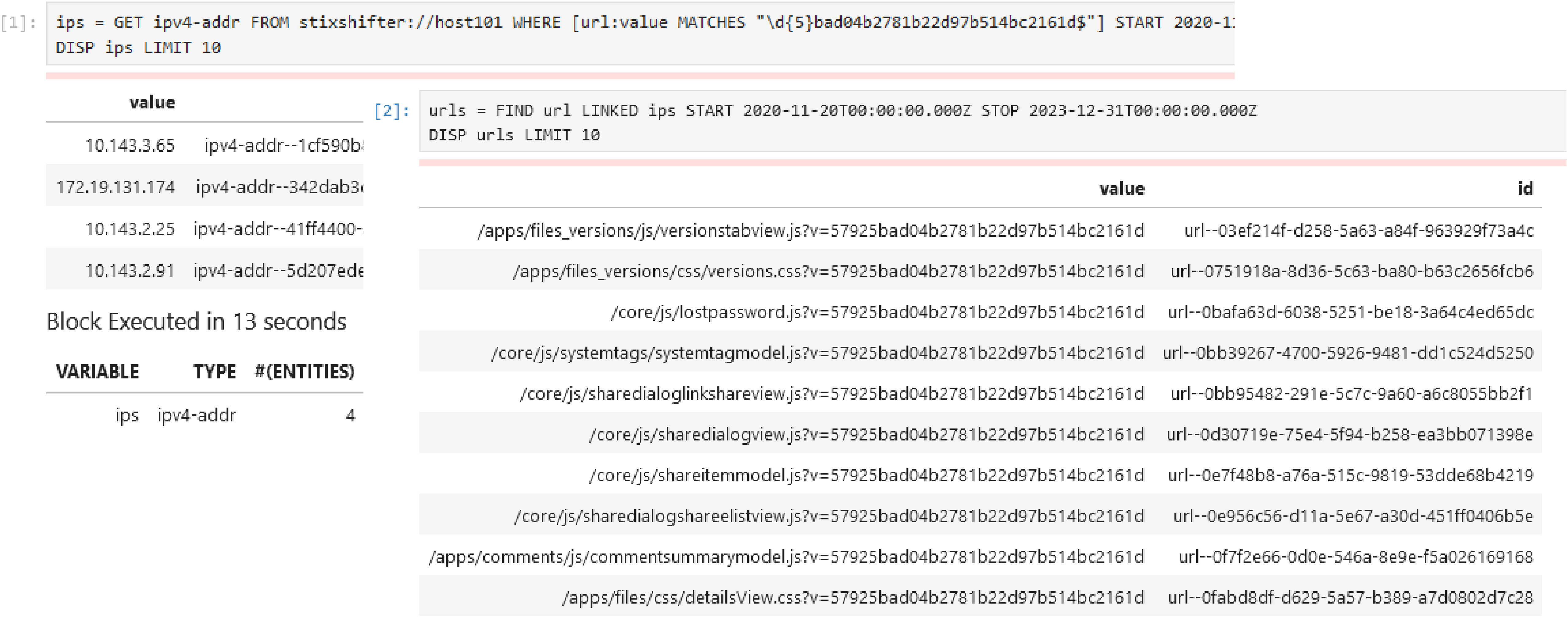
STIX Incident Flow



Incident Report Graph



Kestrel - Human Enabled Flows



[1]:

```
ips = GET ipv4-addr FROM stixshifter://host101 WHERE [url:value MATCHES "\d{5}bad04b2781b22d97b514bc2161d$"] START 2020-1
DISP ips LIMIT 10
```

value	
10.143.3.65	ipv4-addr--1cf590b
172.19.131.174	ipv4-addr--342dab3
10.143.2.25	ipv4-addr--41ff4400-
10.143.2.91	ipv4-addr--5d207ede

Block Executed in 13 seconds

VARIABLE	TYPE	#(ENTITIES)
ips	ipv4-addr	4

[2]:

```
urls = FIND url LINKED ips START 2020-11-20T00:00:00.000Z STOP 2023-12-31T00:00:00.000Z
DISP urls LIMIT 10
```

value	id
/apps/files_versions/js/versionstabview.js?v=57925bad04b2781b22d97b514bc2161d	url--03ef214f-d258-5a63-a84f-963929f73a4c
/apps/files_versions/css/versions.css?v=57925bad04b2781b22d97b514bc2161d	url--0751918a-8d36-5c63-ba80-b63c2656fcb6
/core/js/lostpassword.js?v=57925bad04b2781b22d97b514bc2161d	url--0bafa63d-6038-5251-be18-3a64c4ed65dc
/core/js/systemtags/systemtagmodel.js?v=57925bad04b2781b22d97b514bc2161d	url--0bb39267-4700-5926-9481-dd1c524d5250
/core/js/sharedialoglinkshareview.js?v=57925bad04b2781b22d97b514bc2161d	url--0bb95482-291e-5c7c-9a60-a6c8055bb2f1
/core/js/sharedialogview.js?v=57925bad04b2781b22d97b514bc2161d	url--0d30719e-75e4-5f94-b258-ea3bb071398e
/core/js/shareitemmodel.js?v=57925bad04b2781b22d97b514bc2161d	url--0e7f48b8-a76a-515c-9819-53dde68b4219
/core/js/sharedialogshareelistview.js?v=57925bad04b2781b22d97b514bc2161d	url--0e956c56-d11a-5e67-a30d-451ff0406b5e
/apps/comments/js/commentsummarymodel.js?v=57925bad04b2781b22d97b514bc2161d	url--0f7f2e66-0d0e-546a-8e9e-f5a026169168
/apps/files/css/detailsView.css?v=57925bad04b2781b22d97b514bc2161d	url--0fabd8df-d629-5a57-b389-a7d0802d7c28

Future Work Areas

- **STIX Shifter / Kestrel Enhancements and Fixes**
- **STIX Incident Extension Support in OpenCTI and MISP**
- **Dedicated STIX Incident Viewing Tools**
- **Commercial Tools Removing Glue Code Requirements**
  - Open Source Options: OpenCTI / MISP / TheHive suite
- **More Public TAXII 2.1 Servers**

Interesting Free Tools

- **Open Cyber Security Alliance - https://opencybersecurityalliance.org/**
  - Indicators of Behavior - https://github.com/opencybersecurityalliance/oca-iob
  - Kestrel - https://github.com/opencybersecurityalliance/kestrel-lang
  - STIX Shifter (45+ data providers) - https://github.com/opencybersecurityalliance/stix-shifter
- **Platforms**
  - MISP - https://www.misp-project.org/
  - OpenCTI - https://github.com/OpenCTI-Platform/opencti
  - TheHive - https://thehive-project.org/
- **Libraries**
  - STIX Validator - https://pypi.org/project/stix2-validator/
  - STIX View - https://www.npmjs.com/package/stixview
  - STIX Visualizer - https://github.com/oasis-open/cti-stix-visualization
  - TAXII Client - https://github.com/oasis-open/cti-taxii-client
- **Related OASIS Efforts**
  - CACAO - https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cacao
  - TAC Ontology - https://github.com/oasis-tcs/tac-ontology

Additional References

- **ATT&CK Data:** https://github.com/mitre-attack/attack-stix-data
- **STIX 2.1 Incidents:** https://github.com/oasis-open/cti-stix-common-objects/blob/main/extension-definition-specifications/incident-core/Incident%20Extension%20Suite.adoc
- **STIX 2.1 Interoperability:** https://docs.oasis-open.org/cti/stix-2.1-interop/v1.0/stix-2.1-interop-v1.0.pdf
- **STIX 2.1 Spec:** https://www.oasis-open.org/standard/stix-version-2-1/
- **TAXII 2.1 Spec:** https://docs.oasis-open.org/cti/taxii/v2.1/os/taxii-v2.1-os.html
- **TypeDB Mapping:** https://github.com/os-threat/Stix-ORM/tree/driver_trial

DoD Cyber Crime Center

A Federal Cyber Center

Questions?