TWIGS

BTW – the name is just temporary…

These People Worked Together

SOLTRA
A DTCC and FS-ISAC Company

eclectic iq

MITRE

threatloop.com

Why?

Kick Start STIX 2.0 Discussions

- Two distinct viewpoints emerged
  - Model All the Things
  - Focus on Serialization

Conversations Focused on Minutiae

- Big picture often seemingly overlooked
  - Too easy to focus on the unimportant things
  - Easy to get distracted

Why?

Why Not?

- JSON isn’t XML
- STIX v2.0 is potentially very different
  - Not obvious what STIX v2.0 would look like
  - Would be easier of we had some examples

WE NEEDED A STRAWMAN

Why make a strawman?

Saves Time

- No need to get consensus on everything
- Consensus occurs at the end

What Will Work?

- Test the ideas the community suggested.
- Which ones would work best together?

Focus
ON
WHAT
matters

WHAT MATTERS?

Community Had Already Spoken

We already had an idea of what was important…

- The STIX v2.0 Roadmap listed the top 10
- STIX Difficulties document
- STIX Issues list (and CybOX and TAXII)
- **Many** different discussions on mailing list

WHAT MATTERS?

And of course
we had some **ideas** of our own…

We COULD ADD...

- The ability to ask a threat sharing group questions and get a response
- The ability to link together other people’s threat intel
- The ability for others to agree or disagree with a producers assertions and leave commentary

We could enhance...

- Allow more descriptiveness
- Support Observations earlier in the kill-chain
  - E.g. “Bigpanda posted login details for Bigbanks customer portal on the Evilshare web forum”
- Allow consumers to ask for more detail

OASIS

THOUGHT

“Hmm, what we need is a strawman of a strawman”

OASIS

JOHN WUNDER

TO THE RESCUE!

John had ALREADY invented

TWIGS

So we used it as a starting point

TWIGS IS different from STIX v1.2

-But in a good way-

GOALS

Simplicity

- Target the 80%
- Easy to implement
- Easy to understand
- One way of doing things

Reduce Optionality

- Support customization in a standardized way
- Don’t allow customization everywhere

GOALS -2-

Standardization

- Do things the same way across STIX and CybOX
- Reuse similar structures in similar places

Modularity

- Provide building blocks that can be reused
- Ensuring tight cohesion and low coupling

GOALS -3-

Flexibility

- Use modularity to provide flexibility
- Flexibility is less important than simplicity

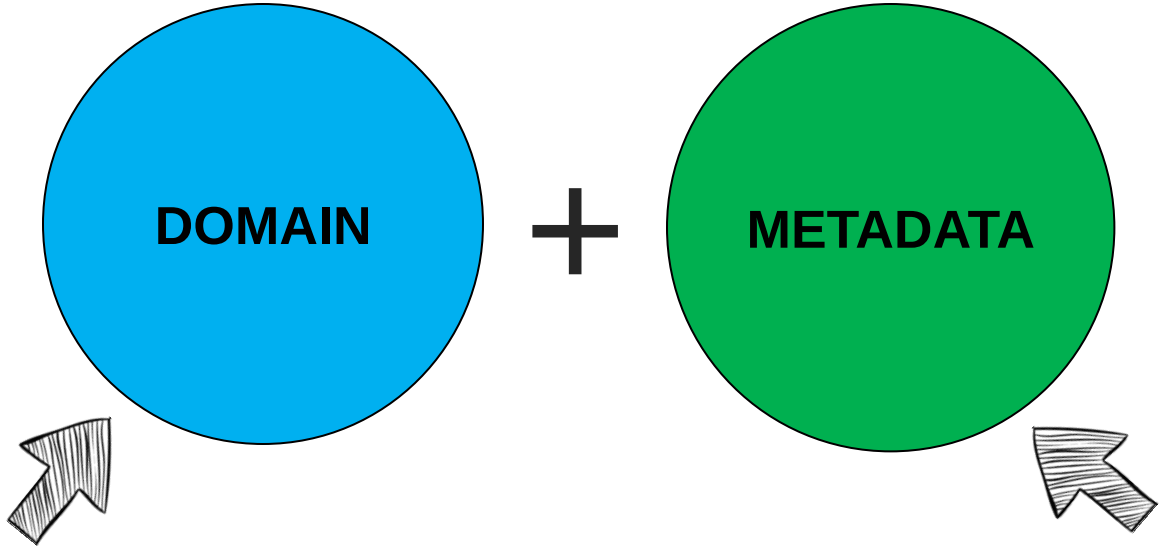
Improve Analysis

- Explicitly modeled as a graph
- Ensure data structures are separate from metadata

OVERVIEW

The basics

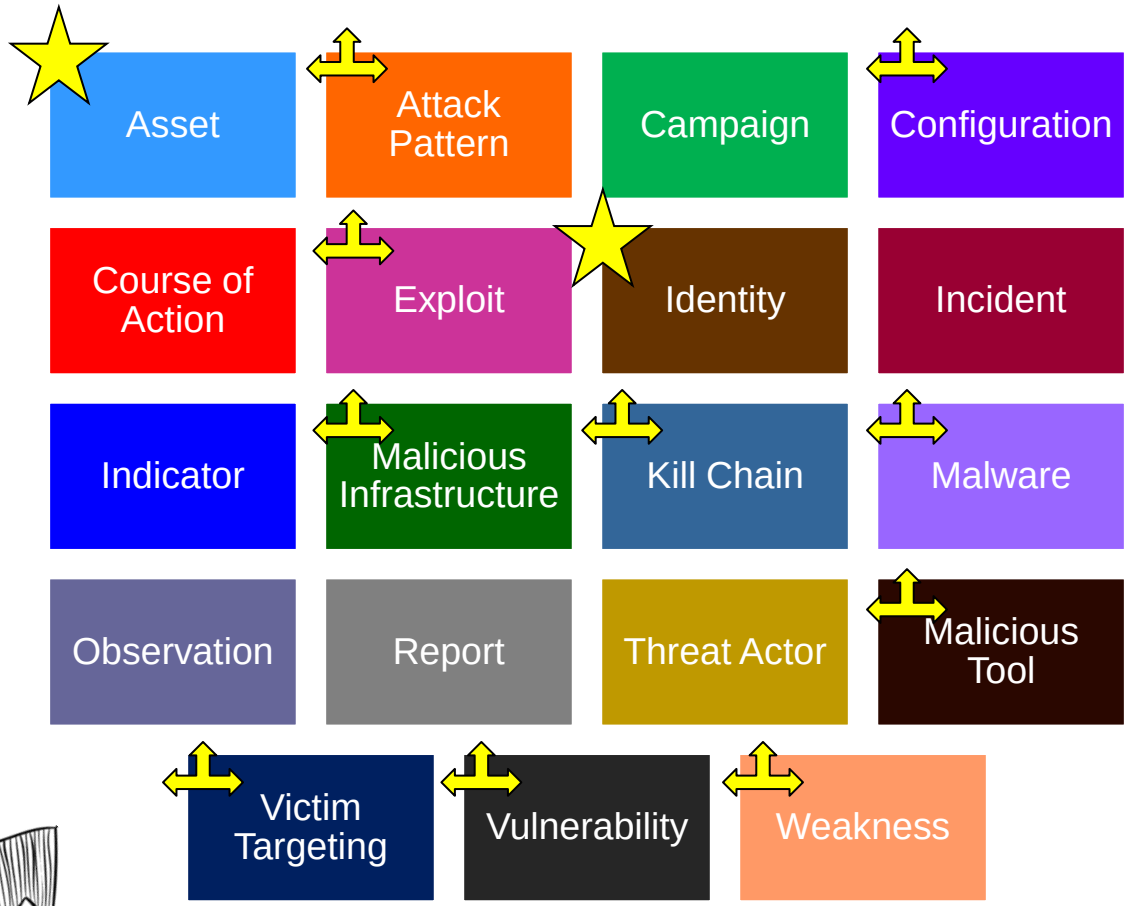
TWO Types of Objects



Building blocks

Relationships and everything else

DOMAIN Objects = Building Blocks

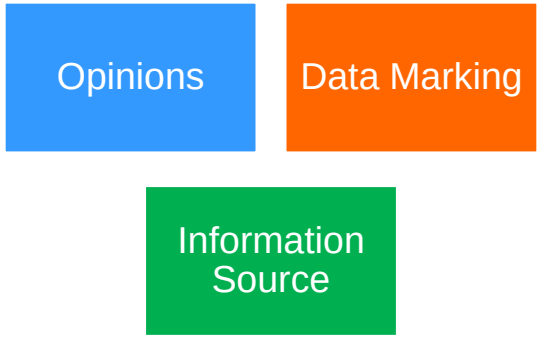


Extend from common base

METADATA Objects = Data About Data

RELATIONSHIPS Join BUILDING BLOCKS Together

Other Metadata Objects



Twigs in practice: basics

Twigs in practice: basics

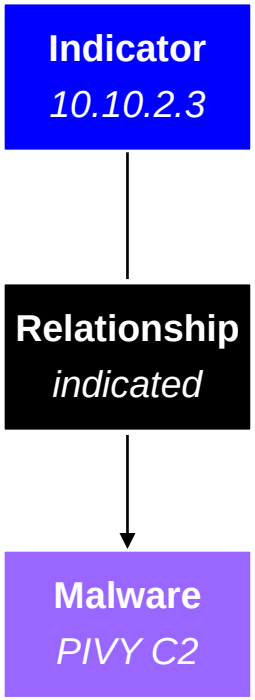
Indicator
10.10.2.3

Relationship
indicated

Malware
PIVY C2

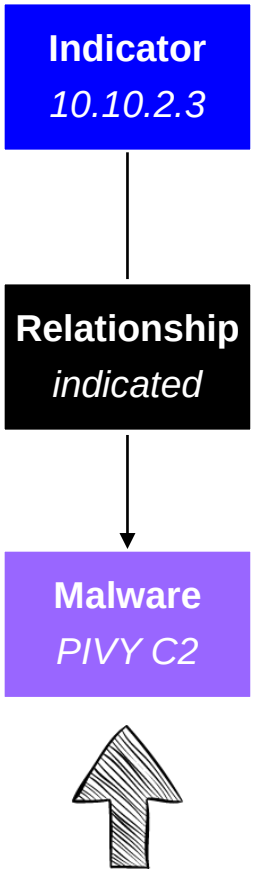
```
{
  "type": "indicator",
  "id": "example.com:indicator:628a75ab-7b63-4e88-9175-2c190e38233c",
  "created_at": "2016-01-06T19:13:17.778545-05:00",
  "producer_ref": "example.com:information-source:example",
  "pattern": {
    "type": "twigs",
    "properties": {
      "$prop1": {
        "key": "IPv4Obj:ipv4addr",
        "condition": "equals",
        "value": "10.0.0.0"
      }
    }
  },
  "condition": "$prop1"
},
```

Twigs in practice: basics




```
{
  "type": "malware",
  "id": "example.com:malware:52c6211a-ab03-4fab-b613-f78ffbf8059f",
  "created_at": "2016-01-06T19:15:32.963619-05:00",
  "producer_ref": "example.com:information-source:example",
  "title": "Poison Ivy C2"
}
```

Twigs in practice: basics

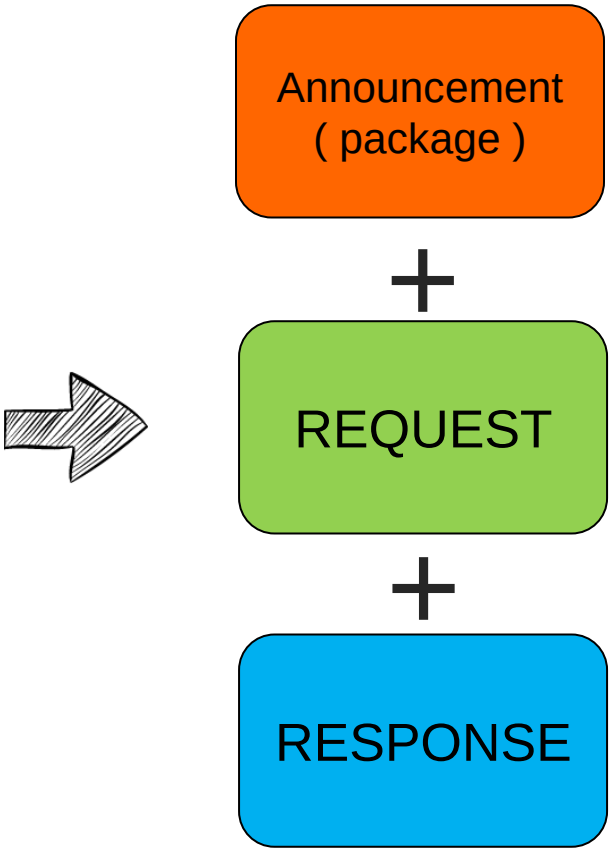



```
{
  "type": "relationship",
  "id":
    "example.com:relationship:6d8a1ef3-3b9b-4241-8f57-0f25b5db52d5",
  "created_at": "2016-01-06T19:16:06.357578-05:00",
  "producer_ref": "example.com:information-source:example",
  "source_ref":
    "example.com:indicator:628a75ab-7b63-4e88-9175-2c190e38233c",
  "target_ref":
    "example.com:malware:52c6211a-ab03-4fab-b613-f78ffbf8059f",
  "value": "indicated",
  "credibility": 4
}
```

Messages

STIX currently has only one message type

Twigs
HAS Three
Message
Types



Announcement
(package)

Used to TELL PEOPLE STUFF

REQUEST

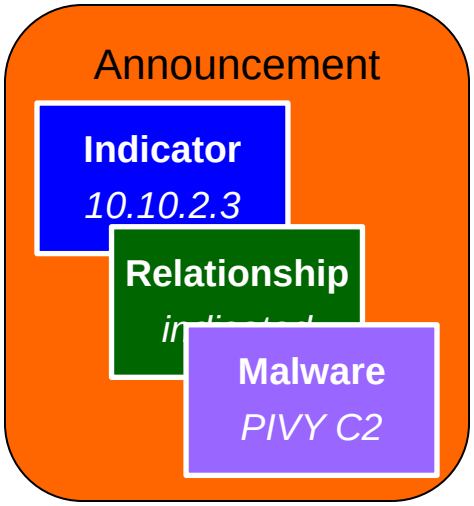
+

RESPONSE

Not yet defined

Used to ASK Questions and get answers FROM COMMUNITY

Twigs in practice: messaging



Twigs in practice: sighting relationships

REQUEST

RESPONSE

announcement

```
"type": "announcement",
"producer_ref": "example.com:information-source:example",
"id": "example.com:announcement:495c4c04-b5d8-11e3-b7bb-000c29789db9",
"created_at": "2014-02-20T09:00:00.000000+00:00",
"contents": [
```

malicious infrastructure

```
{
  "type": "malicious-infrastructure",
  "id": "example.com:malicious-infrastructure:dd955e08-16d0-6f08-5064-50d9e7a3104d",
  "producer_ref": "example.com:information-source:example",
  "created_at": "2014-05-08T09:00:00.000000+00:00",
  "title": "Malware C2 Channel",
  "kind": {
    "value": "Communications",
    "credibility": 4
  }
},
```

asset

```
{
  "type": "asset",
  "id": "example.com:asset:a0777daa-84bf-41e7-89a2-30d7ebb8018d",
  "producer_ref": "example.com:information-source:example",
  "created_at": "2014-05-08T09:00:00.000000+00:00",
  "title": "198.51.100.2",
  "technical_characteristics": {
    "object": {
      "ipv4_address": "198.51.100.2"
    }
  }
},
```

asset as part of infrastructure


```
{
  "type": "relationship",
  "id": "example.com:relationship:7bc8d066-acc2-4bfb-bc08-acbeb0f52c6b",
  "producer_ref": "example.com:information-source:example",
  "created_at": "2014-05-08T09:00:00.000000+00:00",
  "source_ref": "example.com:dd955e08-16d0-6f08-5064-50d9e7a3104d",
  "target_ref": "example.com:a0777daa-84bf-41e7-89a2-30d7ebb8018d",
  "value": "characterized-by",
  "credibility": 5
},
```