# Modeling in STIX

## How to tell what goes where

HS SEDI
Homeland Security Systems Engineering and Development Institute

Homeland Security

# Resources

HS SEDI
Homeland Security Systems Engineering and Development Institute

- The first place to go: http://stixproject.github.io/
  - Documentation on fields and types mean
  - How to use cross-cutting capabilities
  - Examples of how to map common use cases

- The second place to go: cti-users@lists.oasis-open.org

# Disclaimer

HS SEDI
Homeland Security Systems Engineering and Development Institute

- **Intel is an interpretive space, so don't expect 100% "correct answers" all the time**
- **The "answer" *always* depends on context**
- **This will NOT cover all possible things to consider**
  - Just some of the most common ones we run into
- **STIX does NOT currently cover everything you may want to map**
  - It is still evolving to meet the community's needs



Homeland Security


# Incidents vs Indicators




You have some observations of things that are probably malicious.

- Are you providing a **history of malicious behavior**?
  - Map your content into appropriate **Incident** constructs
- Are you wanting to convey **detection guidance** of what to look for?
  - Map your content into appropriate **Indicator** constructs
- The most common answer is **Indicator**


# Threat Actors and Campaigns




You have some names and grouping of adversary activity.

- Look for **identity** info (**names**, **places**, etc.)
  - Means a **Threat Actor**
- Look for coordinated patterns of attacks against **common targets** and/or with a **common purpose**
  - Means a **Campaign**
- Sometimes you can have both
- Other times, reports use them interchangably

# Identity



HS SEDI
Homeland Security Systems Engineering and Development Institute

You have identity information about victim targets or threat actors

- How far down the Identity rabbit hole do you go?
  - Do you have to use the **CIQ extension**?
  - Understand the **use case for the consumer**
- **Granularize** to support better pivoting
  - **Generalize** from **specific targeting** in incidents to **general targeting** in TTP VictimTargeting.
- Dealing with **sensitivities around victim identity information**
  - **Abstractions**
  - **Data Markings**


# TTP Abstraction

HS SEDI
Homeland Security Systems Engineering and Development Institute

You have TTP info as it relates to indicators, incidents, actors, or campaigns.

- Always use **separate** TTPs to represent separate concepts
- Consider using **generalized** TTPs for the pattern itself alongside **more specific** TTPs as used by particular actors
- Abstraction enables potential for **shared community knowledge**



Homeland Security


# Courses of Action

HS SEDI
Homeland Security Systems Engineering and Development Institute

Your content contains some sort of descriptions of actions by victims/defenders

- Distinguish between **Indicators (detection)** and **COAs (prevention/response)**
  - Understand the **use case for the consumer**

- Make sure to recommend COAs at the correct **layer of abstraction**



Homeland Security

# Questions?

**What do you need help modeling?**

**What confuses you about STIX?**

HS SEDI
Homeland Security Systems Engineering and Development Institute

Homeland Security