STIX Working Call

2019-07-02

Agenda

- Review Project Plan (1 minutes)
  - Next 2 weeks finish up remaining loose ends
    - Release WD05 + CSD Ballot + 1st Public Review ~July 12th
- Editorial Status Report (3 minutes)
- Items to Discuss (50* minutes)
- Action Items (2 minutes)

Versioning SCOs - Collisions

- The following SCOs have properties that are called “created” and or “modified”. Do we want to fix this?
  - Directory Object
  - File Object
  - Process Object
  - Windows™ Registry Key Object

Language Content

- Language Content pinning to specific version
- Right now this is required
- The request is to make this optional

Relationship: Indicator->OD

- Indicator to Observed Data relationship type
  - “result-of” or “based-upon”

Object Inconsistencies

- Malware Object - boolean is called is_family versus just "family"
- Grouping Object - Name is optional
- Sighting Object - Does not have a description like the Relationship object
- Marking Definition - Name is optional, there is no description defined
- Location Object - Does not have a name
- SCOs - spec_version is optional

SCO Relationships

- SCO Embedded relationships
  - Domain Name, IPv4 Address, IPv6 Address
  - Make “resolves-to-refs” and “belongs-to-refs” external

Hashes Text

- In Section 2.7 we say the entries MUST come from the vocabulary, however, it is still an open-vocabulary.
- I think the problem came from trying to fix external references use of hashes. But changing this back to a SHOULD MAY have cascading changes in several places.
- It would also mean we would need to add the MUST in the external references 2.5 section.

Deterministic ID Examples

- In Section 3.4 the following additional text is proposed:
- Deterministic IDs (UUIDv5) in the example SCOs contained in this specification were computed using the algorithm defined in section 2.x. Every attempt was made for these IDs to be accurate. Certain IDs which were used in reference properties of the examples did not include the actual object, and therefore it was impossible to accurately compute the appropriate UUIDv5. In these cases, a UUIDv4 was generated and the "version" character of the UUID was changed from a 4 to a 5

Versioning

- Allan pointed out that the text in versioning did not work with the changes for SCOs. The following additional text is proposed:

- In STIX 2.1, SCO do not explicitly have those three versioning properties. Therefore, a SCO cannot be versioned unless custom properties (discussed in section 11.1) are used. Producers who plan on doing this SHOULD use the property names created_by_ref, revoked, created, and modified. In the rest of this section "STIX objects" should be read to include SCOs customized in this way.

Malware Analysis Properties

- There are two properties we need clarity on
- Configuration_version
- Module

Observed Data

- Review Introduction Text
- John-Mark's pseudo code

Opinion Object

- Restrictions on relationships to language content and marking definitions
- I think we need to relax that requirement so you can issue an opinion on something.

Additional STIX ID Changes

- Are there any additional STIX ID changes that we need to address?
- Do we need / want to require organizations not using the default deterministic ID generation method to declare how they generated their object IDs?
  - This would be needed for not just SCOs but for all objects based on current definitions
  - Would it be best to do this via the Grouping / Bundle instead of the individual objects?
- Issues Rich P has brought up on the list

COA

- COA vocabulary
  - Maybe add a few well known options like Microsoft Powershell,Cisco IOS, OpenC2

Other Remaining Things

- Github Issue #70
- Remaining Github Issues (reject, move to 2.2, resolve)
  - 34, 47, 49, 123, 155, 157
- Sarah / Jeff to talk about problems with Motivation and how we should look to fix it.

Patterning

- Comments and Suggestions in Patterning Document
- Outstanding GitHub Issues
  - 51, 58, 59, 60, 61, 62, 66, 85, 146