

STIX Working Call

2019-07-09

Agenda

- Review Project Plan (1 minutes)
 - Release WD05 + CSD Ballot + 1st Public Review ~July 12th
- Editorial Status Report (3 minutes)
 - Documents will be locked down after the call
- Items to Discuss (50* minutes)
- Action Items (2 minutes)

Hashes Text

- In Section 2.7 we say the entries MUST come from the vocabulary, however, it is still an open-vocabulary.
- This was a mistake when we were fixing this problem else where. This statement really was supposed to be in 2.5 so that it matches everywhere else it is used in STIX.
- Places it is used like this: 6.7.3.2.1, 6.7.6.1, 6.7.6.2.1, 6.7.6.3.1, 6.18.1

Versioning Text

- ✦ Review the following text addition for 3.6:
- ✦ It should be noted that if a producer versions a SCO (assigns value to these four properties) that no other producer would be allowed to create or modify the same SCO with an equivalent deterministic id, as that would conflict with the strict versioning rules defined in STIX2. Therefore, for interoperability and sharing, producers versioning SCOs **MUST NOT** use the default namespace for deterministic ID creation. Otherwise multiple different producers will conflict with each other if producing the same SCO intelligence.

Observed Data

- ✦ Review Introduction Text
- ✦ Allan's comment that saying the data must be related is un-testable and we should remove it.

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

- Issues Rich P has brought up on the list
- 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?

Other SCO Issues

- ✦ 6.6.1 - Include body_multipart in ID Contributing Properties?
- ✦ 6.18.2 Example is wrong

Other Remaining Things

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

Object Inconsistencies

- ✦ Marking Definition - there is no description defined
- ✦ SCOs - spec_version is optional

COA

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

Patterning

- Two remaining suggestions in Patterning Document