STIX Working Call

2019-04-23

Agenda

- Review Project Plan (2 minutes)
- Editorial Status Report (3 minutes)
- Items to Discuss (50* minutes)
- Action Items (2 minutes)

Editorial Status Review

- Significant editorial work on the following sections: 1.6.11, 1.6.12, 2.13, 3.0, 3.1, 3.5, 3.5
- Conformance language has been merged from old parts 2-4
- Document clean up
  - Trying to fix the Common Properties confusion (the same properties are defined in 4 different places)

Items to Discuss

- Switch from JSON to I-JSON
- Relationships on Cyber Observables
- Versioning a Cyber Observable

I-JSON

- Switch from JSON RFC8259 to I-JSON RFC7493
  - Change our definition of integer to comply with RFC7493
- This was already done in TAXII
- ECMA Script needs I-JSON
- ECMA Script and browsers do not support 64 bit JSON numbers, they only support IEEE 754 double precision number ([-(2**53)+1, (2**53)-1])
- We will need this for JCS and Digital Signatures

Versioning a SCO

- There seems to be two classifications of SCOs
- 1) Simple facts like an IP Address or Domain Name. These need a Relationship to something to be of any use and changing them over time does not really make sense.
- 2) More detailed facts like Email Message Object or File Object. These could contain valuable or sensitive information by themselves, without any relationship. These _may_ actually change over time.

Versioning a SCO

- Use cases in the affirmative that I have heard
  - Data Markings
  - What you know about a file or email message could evolve over time
    - Need ability to revoke a fact so it can be reissued
- Statements in the negative that I have heard
  - A lot of extra bloat on the wire
  - STIX is meant to be a transfer syntax, not a database or internal tool syntax.

Versioning a SCO

- Open Questions
  - What if initial version did not have created/modified?
  - Can you version something with no created_by_ref?
  - There is currently no revoked property on SCOs
  - Do things like Email Message Object need the ability to be translated ?
  - If the Email Message data is in German do we need to support a “lang” property to say the email is “DE”

Versioning a SCO

	STIX Core Objects			STIX Helper Objects		
Property Name	**SDOs**	**SROs**	**SCOs**	**Language**	**Markings**	**Bundle**
`type`	Required	Required	Required	Required	Required	Required
`spec_version`	Required	Required	Optional	Required	Required	N/A
`id`	Required	Required	Required	Required	Required	Required
`created_by_ref`	Optional	Optional	N/A	Optional	Optional	N/A
`created`	Required	Required	Optional	Required	Required	N/A
`modified`	Required	Required	Optional	Required	N/A	N/A
`revoked`	Optional	Optional	N/A	Optional	N/A	N/A
`labels`	Optional	Optional	N/A	Optional	N/A	N/A
`confidence`	Optional	Optional	N/A	Optional	N/A	N/A
`lang`	Optional	Optional	N/A	N/A	N/A	N/A
`external_references`	Optional	Optional	N/A	Optional	Optional	N/A
`object_marking_refs`	Optional	Optional	Optional	Optional	Optional	N/A
`granular_markings`	Optional	Optional	Optional	Optional	Optional	N/A

Action Items

- Mini-Group Report on Infrastructure
- Review COA
- Document top-down review
- Changes to Language Content based on Sponsors