Cyber Threat Intelligence (CTI) Technical Committee (TC) Co-Chairs Face-to-Face
Meeting Minutes
January 12-13, 2015

In Attendance:

1. Aharon Chernin
2. Alex Foley
3. Bret Jordan
4. Dave Eilken
5. Ivan Kirillov
6. Mark Davidson
7. Rich Struse
8. Sean Barnum
9. Trey Darley

Not In Attendance:

1. Pat Maroney
   Pat was remote for a portion of January 13

January 12th

Timing of MVP

- There was also a discussion regarding the timeline for STIX 2.0 / TAXII 2.0 / CybOX 3.0 working drafts.
- The co-chairs suggested aiming for June or July to be pragmatic… although the end of May is possible, it may not work given the number of issues to resolve
- To meet aggressive timelines, we will work to schedule recurring discussion calls for complex issues to make aggressive progress.

STIX Issue Prioritization

- The co-chairs went through the STIX Github to decide Yes, No or Maybe for each issue to decide if they should be included in a minimally viable product (MVP) for STIX 2.0
- There are currently 167 open issues in the STIX schemas repository
  - 81 of these were labeled 2.0-Yes
  - 27 were labeled 2.0-Maybe
  - 28 were labeled 2.0-No
  - The rest were unrelated to STIX 2.0 specifically
- These decisions will be presented to the larger CTI committee on Thursday, January 14th

January 13th

STIX Issue Time Estimates

- The co-chairs went through the STIX Github to estimate the amount of effort required for each of the issues labeled 2.0-Yes for inclusion in STIX 2.0 (hours, days or weeks) to try to identify issues that may require complex solutions and as such may not need to be included in the MVP.
  - 8 issues were labeled Effort-weeks
  - 24 were labeled Effort-days
  - 49 were labeled Effort-hours
- There was a vigorous discussion of how to categorize / group issues together so they can be decided at one time; the discussion focused around the implementation of custom vocabularies as a matter of course.

STIX Discussion Topics for Greater F2F

- One of the focuses of this discussion was working through how controlled / custom vocabularies would be handled using JSON.
- There was lengthy discussion of how to balance the need for expansion with the need for standardization.
- We covered the basic way custom vocabularies might be included in raw JSON code, which will be presented to the larger CTI committee on Thursday or Friday.

TAXII Preview

- The TAXII co-chairs went over their presentation, covering a discussion of how TAXII works today and what the vision is for TAXII 2.0
- The subcommittee is working towards a model where we have not only collections of threat intelligence to download / revision against, but also a pub / sub model to power streams that don't persist on disk
- TAXII seems to have made the most progress towards a draft specification

CybOX Preview

- The CybOX co-chair presented the most recent numbers from CTI-Stats
- There was also a presentation of a new visualization to cover CybOX 3.0 and what's in and out
- Rich continued to emphasize that our goal is a minimally viable product – we will likely not be able to include every single object from CybOX 2 in CybOX 3.0
- General discussion of the problems caused by object hierarchy causes and a potential solution with different names – "property sets" / "extensions" / "property groups"

Strawmen Previews

- John Wunder and John Baker joined us for this portion of the discussion to cover the strawmen discussions
- Aharon, John and Sean gave high level overviews of their presentations

Meeting Times and Voting

- The co-chairs discussed the logistics of switching to an integrated meeting calendar
- We will stop having monthly subcommittee status update meetings until the MVPs for each of the next versions of the standards are decided.
- The co-chairs discussed the issues surrounding voting rights and developed potential solutions for OASIS to help us consider to enable remote participation and grease the skids on obtaining voting rights so that new members don't have to wait two months.