Cyber Threat Intelligence (CTI) Technical Committee (TC) STIX Subcommittee (SC)

Meeting Minutes
October 21, 2015
4:00-5:00PM EDT

Agenda

Agenda:

- STIX 1.2.1 specs
  - Status and Next Steps
- STIX 2.0 kickoff
  - Initial administrative steps
  - Begin deliberative process (get stuff done)
    - Setting the stage and navigating the road
      - Use cases
      - Issues
    - Some decisions to make
      - "voting" approach for issues
      - how to start "getting stuff done" as soon as possible
- Example of Opinion Contribution for an Issue (Aharon Chernin: Sightings)

Notes

- On the "nominating editors" slide, Pat wanted to nominate Sean as the "modeling" perspective
  - Sean said we should send those suggestions to the list
- On the same slide, John Anderson (Soltra) wondered what Sean meant by something representing an "implementation" perspective…a particular focus (Java, etc) in mind?
  - Sean explained that it just meant somebody building the tools (vendors, etc)
  - John A. then suggested bringing up a user perspective, separate from modeler or implementor
- On the use cases slide, someone (unsure who) noted that the link on the Github page was wrong. I didn't follow which page exactly.
- Discussion on how to support "voting" to decide what to talk about

    - Aharon suggested that it might be a TC issue
        - Sean said they were approaching it first so should find something that works, then maybe bring it broader
    - John Wunder suggested that the co-chairs could propose some topics and see if anybody objects
    - Pat wanted to make sure we maintained some kind of issue tracker
    - Bret suggested Stack Exchange
    - Sean suggested moving the discussion to the list
- Trey developed a tool to survey usage of STIX/CybOX (works against a TAXII server)
    - Pat had some raw STIX files that he couldn't get a TAXII server to accept, asked if Trey could get it to work against that
    - He could, asked Pat to send e-mail / file an issue
- Aharon went through his opinion discussion of the sightings use case
    - John commented that it would be good to show how it would be used
    - Aharon said that might be in the use case
- Question about using references/TAXII for sightings, I didn't really follow.
    - Mark answered that TAXII SC was looking into it

Calls to Action

- Members: nominate editors on the list for STIX v2.0 work product
- Members: Review use cases on STIXProject/use-cases github wiki (add missing use cases and flesh out existing ones)
- Members: Review issue trackers (identify new issues, comment on existing issues, consider prioritization)
- Members: Offer thoughts on the list for technology approach for issue "voting"
- Members: Offer thoughts on the list for initial issues to tackle
    - Candidates
        - Sightings
        - Relationships
        - ID format
        - Abstracting constructs (identity, victim, source and asset)
        - In-line vs referencing of content
        - Data Markings
        - Other suggestions?