STIX Working Call

2019-07-30

Agenda

- Current Status (5 minutes)
- Sponsorships (3 minutes)
- Comments (40* minutes)
- Future Items (10 minutes)

Current Status

- Update on ballots
- Update on public review
- What happens after public review

Long-term Schedule

- Friday July 26th - Ballot Closes
- Monday July 29th - Timer starts for sponsors to implementation new concepts
- Monday July 29th - Ask Chet from OASIS to start 1st public review (30-days). It will probably take him a week to get this done.
- August - Public Review

Long-term Schedule

- Early/Mid September - Address any comments / suggestions / feedback that comes from the CSD02 ballot and 1st public review
  - If non-substantive changes, issue Working Draft 06 and do motion for CSD03 (2 week ballot)
  - If substantive changes, issue Working Draft 06 and do motion for CSD03 and 2nd public review (15-day) total time about 4-5 weeks (2 week ballot + 2 weeks for public review)
- Rinse and repeat until all changes are done

Long-term Schedule

- End of January is the deadline for sponsors to implement POC.
  - Hopefully sponsors will finish this work much earlier!
- Address any changes that come from the sponsors work
  - If non-substantive changes issue Working Draft 07 and do motion for CSD04 (2 week ballot)
  - If substantive changes issue Working Draft 07 and do motion for CSD04 and 3rd 15-day public review (4-5 weeks)
- Motion and ballot for latest CSD to be made a Committee Specification (CS01), 2 week ballot

Sponsorship

- Course of Action
- Grouping
- Infrastructure
- Malware
- Malware Analysis
- SCOs as top-level objects
- SCO relationships
- Deterministic IDs

Comments

- John-Mark
- Jason Keirstead
- Chris Lenk
- Github Issues (70, 164) - Drew
- Kill Chain Concerns

Chris Lenk - 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

Chris Lenk - Editorial

- In section 9.1 the patterning definition of Observation is still defined as represented by Observed Data SDOs, but those are now deprecated.
- 4.6.1 indicator:valid_until description first paragraph typo: 'should no longer considered'
- 4.11.2 malware-analysis relationships table, typo in description for 'malware-analysis characterizes malware': 'is describes'

Chris Lenk - Editorial

- 4.16.2 threat-actor relationships table, typo in description for 'threat-actor impersonates identity': two spaces between 'an' and 'impersonates'
- 4.18 vulnerability description first sentence has a space before the period, and maybe the period should go inside the quotes
- 7.1 language-content description first paragraph, last sentence starts with 'Instead...' which doesn't make sense after previous sentence was removed

Future

- ????