Cyber Threat Intelligence: Technical Committee (CTI TC)

Monthly Meetings – 13 December 2018
Session #1 & Session #2

&

Agenda

Richard Struse & Trey Darley – CTI TC Co-chairs

1. Introduction & Welcome (Trey & Rich)
2. TAXII Ballot (Bret)
3. STIXPreferred Update (Allan)
4. Update on Cyber Observables Mini-Group (Allan)
   a. Background & Motivation
   b. Use Cases for 95% & Current Proposals
   c. Update on Status
5. Sub-Committee Updates
   a. STIX (Sarah & Ivan)
   b. TAXII (Bret) + CDC Demo
6. F2F Update - Sunnyvale (Rich, Trey & Ryu)

TAXII 2.1 Ballot Update

Bret Jordan – TAXII SC Chair

- Committee Specification Draft 02 (Working Draft 05)
  - Editorial changes and User-Agent description
  - Please vote

- Proposed Schedule Post CSD 02 (if it passes)
  - 30 day Public Review Period
  - CSD 03 based on Working Draft 06 (changes from PRP)
  - 15 day Public Review Period
  - Ballot to make TAXII 2.1 a Committee Specification

STIXPreferred Update

Allan Thomson & Jason Keirstead - Interoperability SC Co-Chairs

- **STIXPreferred Launch Planning**
  - **Mini-group formed on STIXPreferred launch tasks**
    - **Chet, Carol and Dee (OASIS)**
    - **Allan, Jason, Rich, Trey, (CTI TC)**

- **Pre-Launch Activities (now to Feb 15th)**
  - **Committee review team alias updates/operational checks**
  - **Define & Review rules of review committee operation**
  - **Test examples posted for use by vendors**

- **Phase 1 Launch Targeting Vendors (now to Mar 31st)**
  - **Outreach to orgs that wish to be included in the initial launch activity announcements including press release, social presence...etc.**
  - **Must have at least 1 approved STIXPreferred certified product**

- **Phase 2 Launch Market/Vendors (April 2019)**
  - **Press release; Social media; Web-site updates**
  - **Webinar**

STIXPreferred - Plugfest Planning

Allan Thomson & Jason Keirstead - Interoperability SC Co-Chairs

- **Future plugfests sign-up sheet**

https://docs.google.com/document/d/1V7zAg2rI-QOkIFbZjv4mgDZ-Z2_GRTjGsoI2ZUi99bk/edit?ts=5bec471c#heading=h.r4ruh38j0l6

- **SIGN UP!!!!!**

- **We will hold plugfests based on interest, need and use cases requiring validation**

Observed Data/Object Update

Observed data slide deck

STIX Specification Update

Ivan Kirillov & Sarah Kelley – STIX SC Co-Chairs

- Sponsor updates - Confidence/Note/Opinion
- Documents:
  - Confidence: https://docs.google.com/document/d/1-Bl7dEYIbepKHunc6Narcpa79laRlePb28wv8lbHJtY/edit#heading=h.gjdgxs
  - Opinion: https://docs.google.com/document/d/17hEBdomv6zqUCQTXnmXRzhX5mLqrSgsX3Vc5ZqNoJu4/edit#heading=h.gjdgxs
  - Note: https://docs.google.com/document/d/11piq3g99fTDbiKpXrO1V3WV0581VjKlxJejm908cJd4/edit#heading=h.gjdgxs
- Documents will include
  - Specific use cases that were tested
  - If use case POC code demonstrates Producer or Respondent
  - Interop tests

STIX 2.1 Sponsor Status

Ivan Kirillov & Sarah Kelley – STIX SC Co-Chairs

Name	Sponsors (2 needed)	Due Date
Confidence	IBM (tentative), DHS, New Context (tentative)	April 2, 2019
i18n	Fujitsu, New Context	April 2, 2019
Location	DHS	April 2, 2019
Note	DHS, JP Morgan, CTIN	April 2, 2019
Opinion	DHS, JP Morgan, CTIN, Perch, New Context (tentative)	April 2, 2019

Need additional sponsors!
Four months left and counting...

TAXII Specification Update

Bret Jordan – TAXII SC Chair

- Open TAXII 2.1 Ballot - Please vote
- Additional Features / Enhancements
  - For TAXII 2.1
  - Post TAXII 2.1
  - Please submit to the email list your feature / change requests
- Long Term Goals for TAXII
  - Please submit your ideas

TAXII - Verification Process

Bret Jordan – TAXII SC Chair

- Should TAXII have similar requirements to STIX for measuring its DONE-ness?

- What should those be?
  - Specification Text (obviously)
  - Interoperability Tests
  - Working Proof of Concept Code

- What constitutes a features that needs to be assessed?
  - In STIX this generally means new objects but not really changes or additions to objects.

TAXII - Process Questions

Bret Jordan – TAXII SC Chair

- How should we determine in TAXII:
  - If a feature or enhancement should be worked on / added to the specification?
  - Which proposal we should adopt if there is more than one?
  - When a feature or enhancement is deemed complete or shippable by the TC?

- How should we handle requests when the TC is either
  - contentious about a feature or
  - apathetic about a feature

Community Development Corner (CDC)

- Demo of TAXII 2.1 compliant features
  - New envelope and Pagination
  - Media Type Changes
  - New Versions Endpoint

https://test.freetaxii.com:8000/taxii2/

Upcoming F2F Event

Richard Struse & Trey Darley – CTI TC Co-chairs

January 29-30 2019 at Fujitsu in Sunnyvale, CA USA

GCDP North Café
H Building - Fujitsu
Sunnyvale Campus
1250 E. Arques Avenue
Sunnyvale, CA 94085-5401
Go to Front Desk of H Building to be escorted to the Meeting Room

Fujitsu Sunnyvale Campus Map

https://www.eventbrite.com/e/oasis-cyber-threat-intelligence-f2f-tc-meeting-january-2019-registration-53540053742

OASIS

Q&A

Richard Struse & Trey Darley – CTI TC Co-chairs

Cyber Threat Intelligence: Technical Committee (CTI TC)

OASIS