Cyber Threat Intelligence: Technical Committee (CTI TC)

Monthly Meetings – 20 September 2018
Session #1 & Session #2

OASIS STIX™ & TAXII™

Agenda

Richard Struse – Chair, CTI TC

- Ballots
- Proposed TC structural changes
- Upcoming F2F Meetings
- Community Development Corner
- Subcommittee updates
- STIX Sightings & Semantic Equivalence Documents
- Q&A

Open Ballots

Richard Struse – Chairman, CTI TC

- STIX 2.1 CSD01
  - http://bit.ly/2phfjY8
- TAXII 2.1 CSD01
  - http://bit.ly/2PNRdQe
- STIX Preferred Terms of Use
  - http://bit.ly/2OzkvBJ

GO VOTE!!!

OASIS

Proposed TC changes

Richard Struse – Chair, CTI TC

- Two proposed structural changes for the TC to consider:

- **Proposal One:** that we fold responsibility for Cyber Observables into the STIX subcommittee, eliminating Cyber Observables as a subcommittee.
    - **Rationale:** Since the decision was taken two years ago to fold CybOX into STIX as a single, coherent standard, the STIX and CybOX SC co-chairs have been effectively working as a single team. It's only logical after two years of these two SCs being defacto a single SC that we formalize that.

- **Proposal Two:** that we add a co-chair to the TC chair resulting in having two TC co-chairs.
    - **Rationale:** TC chair responsibilities are a lot of work for just one person.
    - **Rationale:** Eliminates a single point-of-failure and helps ease succession planning.

Proposed TC changes (cont)

Richard Struse – Chair, CTI TC

- **Motion One:** Motion to combine the Cyber Observables subcommittee into the STIX subcommittee and eliminate Cyber Observables.
    - Assuming there are no objections to Motion One during the TC calls, we will proceed accordingly.

- **Motion Two:** Motion to expand from one TC chair to two TC co-chairs.

- Assuming there are no objections to Motion Two during the TC calls, we will open a call for nominations for the open TC co-chair position Friday morning EDT. The nominations will be open for three business days.

    - Upon the close of nominations, an electronic ballot will be open for one week to select the TC co-chair from the list of nominees.

    - OASIS rules require a full majority vote (to be considered the winner, a nominee must receive more than 50% of all votes eligible to be cast). If no nominee receives >50% of eligible votes, another ballot would need to be opened.

NYC F2F Event

Richard Struse – Chairman, CTI TC

On-Site Participants

- Hitachi - 101 Park Avenue, 10F

  Large training Room, 1035A
- Wednesday, 26th September
  - 8:30 am - 5:00pm EDT
- Thursday, 27th September
  - 8:30 am - 5:00pm EDT

Remote Participants

- The bridge will be up by 8:15 US EST. There is an app for iOS and Android.
- When not speaking, mute your microphone.
- Use the WebEx "raise hand" feature to raise your hand when you wish to comment.

REGISTER HERE: https://bit.ly/2QLUxML

OASIS

Upcoming F2F Events

Richard Struse – Chairman, CTI TC

Save the Date!

January 29-31 2019 at Fujitsu in Sunnyvale, CA USA

Community Dev. Corner

Jason Keirstead, Bret Jordan

STIX Shifter

https://github.com/ibm/stix-shifter

Goal: Make STIX patterns and Observables usable in common security repositories incl. SIEM,Endpoint,data lakes, etc.

- Converts STIX Patterning => Queries (merged from stix2patterns_translator)
- Convert Results => Observed Data
- 5 adapters already in progress
- Maintained by IBM, contributors from MITRE

Community Dev. Corner

Jason Keirstead, Bret Jordan

- Test Suites - https://github.com/freetaxii/testlab

- Basic Tests
  - No Authentication Parameter
  - Incorrect Authentication Parameter
  - Correct Authentication Parameter
  - Missing Trailing Slash
  - Invalid Media Types for Accept
  - Valid Media Types for Accept
  - Valid Media Type for Content-type

Community Dev. Corner

Jason Keirstead, Bret Jordan

- Filtering Tests
  - No filtering Sort Order
  - Version filtering using ALL
  - Version filtering using FIRST
  - Version filtering using LAST
  - Version filtering using FIRST,LAST
  - Version filtering using VERSION
  - Version filtering using LAST,FIRST,VERSION
  - ID filtering using single ID
  - ID filtering using two IDs
  - Type filtering using single Type

Community Dev. Corner

Jason Keirstead, Bret Jordan

- Current Endpoints Tested (read-only)
  - Discovery
  - API Root
  - <api>/collections/
  - <api>/collections/<id>/
  - <api>/collections/<id>/objects/
  - <api>/collections/<id>/objects/<id>/

- Roadmap
  - Manifests
  - Write-only and read-write collections

Interop Update

Allan Thomson and Jason Keirstead - Co-Chairs

- **Self-Certification Portal (STIX Preferred) Project - ballot is open, Please VOTE**
  - https://www.oasis-open.org/apps/org/workgroup/cti/ballot.php?id=3253
- **Part 2** Edits are still in progress - **Please** review!
  - https://docs.google.com/document/d/1VY-uz3qnWpF8LMCWLgB_tY3uVLmw_IVcuXSwgdGEFHc/edit#heading=h.gjdgxs
- **Target** for Part 2 to move to a ballot is in the next few weeks (pending feedback)
- **Ongoing: test contributions to help prepare for STIX Preferred & future Plugfests - please help!**
  - **https://github.com/freetaxii/testlab**

STIX Specification Update

Trey Darley, Ivan Kirillov, Sarah Kelley, John Wunder – Co-Chairs

- **STIX 2.1 CSD01**
  - It's out!
  - Once the ballot passes the 185 day clock will start counting down...

- **Continuing work on:**
  - Observables
  - Infrastructure (and how it uses observables)
  - Malware (and how it uses observables)
  - STIX Enhancements Proposals (SEPs) and supporting TC processes

STIX 2.1 Sponsor Status

John Wunder and Sarah Kelley – Co-Chairs

Name	Sponsors (2 needed)
Confidence	IBM (Tentative), DHS
i18n	Fujitsu, New Context
Location	DHS
Note	DHS, JP Morgan, CTIN
Opinion	DHS, JP Morgan, CTIN, Perch

Need additional sponsors!

TAXII Specification Update

Bret Jordan and Mark Davidson – Co-Chairs

- **TAXII 2.1 CSD01**
  - Ballot is open
- **Issues to Address Post CSD01**
  - Bundle and Content Types
  - Error code to be returned under certain conditions
- **New Work**
  - Pagination
  - Query

Newly released docs

Ivan Kirillov

- STIX Sightings Document
- Semantic Equivalence Document

Q&A

Richard Struse – Chair, CTI TC

Cyber Threat Intelligence: Technical Committee (CTI TC)

OASIS