Cyber Threat Intelligence: Technical Committee (CTI TC)

Monthly Meetings – **29 March 2018**

Session #1 & Session #2

Agenda

Moderating: Richard Struse - Chair, CTI TC

- **Plugfest, Training Activities**
- **Working Call Update**
- **Path Forward for 2.1 Release**
- **Other Business**

OASIS

Spring 2018 - DC Area

Allan Thomson

- Agenda and registration
  - https://www.eventbrite.com/e/oasis-cyber-threat-intelligence-plugfest-training-june-2018-registration-44601011827
- Day 1: Plugfest
  - TC Members only
  - Focused on interoperability
- Day 2: Training
  - Focused on developers & analysts
  - Open to non-TC members

June 6, 2018 - Reston, VA

Allan Thomson

Day 2 Training Agenda

- Overview on STIX/TAXII & History
- Data Model Foundations
- TAXII2 & Interop Foundations
- STIX2/TAXII2 in Practice
  - Leveraging STIX2 for Modelling
  - Using Python STIX2

Call for Plugfest/ F2F/ Training Hosts

Rich Struse

- Fall 2018 - Europe?
- Winter 2019 - U.S. West Coast?
- Call for Volunteer Trainers
  - Ideas for Exercises
  - Training Artifacts (e.g. STIX2 Card Deck)

Working calls

- As we focus on finalizing CSDs and developing implementations, the pace of working calls is slowing :)
- Tuesday working calls and Wednesday interoperability calls will be merged
  - Topics for any given Tuesday working call may be specification or interop

Path Forward for 2.1 Release

Rich Struse

Key Question:

How do we release STIX 2.1 in a timely manner while also minimizing the likelihood that new features have latent issues, in the worst case requiring backward-breaking changes to address in 2.2+?

Options:

1. **Require CS Verification (by Implementation)**
   Follow the consensus from the SLC F2F, with a few tweaks based on subsequent discussion of the implementation details.

2. **Release 2.1 CS As-Is**
   Begin working on STIX 2.2, starting with incomplete work originally slated for 2.1.

Proposal 1: Require CS Verification

Mark Davidson

1. We will release a series of TC approved CSDs, where each CSD has a 2 week ballot period.
2. Each CSD may have some fixes that require breaking changes to previous CSDs as required
3. A feature has 185 days (6 months) post CSD ballot approval to show that it meets the definition of done; If it does not meet the definition of done it will be scoped out of the next CSD.
4. Before we do a CS we will ensure that all changes and new features meet the definition of "done".
    1. At least 2 organizations will have running POC code with real data that can interoperate
    2. We will have fully defined specification text
    3. The feature is covered by one or more interop tests, either new or existing
5. A CS will be submitted for TC approval no later than 185 days (6 months) **(or longer if agreed to by the TC)** after the last CSD that the TC approved. However, if something has to be removed we will reissue a CSD with only components that were approved and shown to be done in a previous CSD.

Proposal 1: Require CS Verification

1. STIX 2.1 CSD 01 shall include:
    1. 2.0 Breaking Changes
    2. Confidence
    3. i18n
    4. Location
    5. Malware
    6. Intel Note
    7. Opinion
2. STIX 2.1 CSD-Future-TBD (**Where the specific CSD for each feature may change depending on the specification text being complete for that feature)**
    1. IEP
    2. Grouping
    3. COA
    4. Assertion
    5. Patterning fixes
    6. Infrastructure
    7. STIX "Extension" mechanism
3. **Informationally note the risk that organizations take when implementing draft specifications**
    1. **Text on next slide**

Example Text to Add On Implementation Risk

TC EDITORS: PLEASE REMOVE THIS SECTION BEFORE CS BALLOT

While the eventual version indicator for this version of the specification will be "2.1", implementations of draft versions (CSDs) of this specification SHOULD instead advertise "2.1-draftXX" in all places where the specification version is referenced (for example, spec_version property, API-roots, media types, etc).

This allows pre-final implementations to safely negotiate with each other, even if they would otherwise be incompatible. When this specification is marked as final by the Technical Committee, having advanced to either a CS (committee specification) or an OASIS Standard, implementations MUST only advertise "2.1" to represent this specification. Any content that was used prior to this specification becoming final, and has a designation of "-draftXX) MAY be converted to the final version or deleted.

NOTE: XX = current draft number

Proposal 2: Release 2.1 CS As-Is

Rich Piazza

1. Declare STIX 2.1 to be "done", and start the process for it to be released as the 2.1 CS: release a CSD, do one or more public comment periods, vote to approve CS
2. Each "text-complete" feature will be voted on, and only ones approved by the TC will be included.
    1. 2.0 Breaking Changes
    2. Confidence
    3. i18n
    4. Location
    5. Malware
    6. Intel Note
    7. Opinion
3. Development of dropped features and others will continue with STIX 2.2 using the new approved process as discussed in the January F2F.

Proposal Pros/Cons

Proposal #1: Require CS Verification

- **Pros**
  - Ensures completeness and implementation confidence of features
- **Cons**
  - No timeframe for 2.1 CS
  - Additional process will slow progress
  - Running code is not a cure-all for breaking changes, especially in a data model specification like STIX (does not apply to TAXII).

Proposal #2: Release 2.1 CS As-is

- **Pros**
  - Some 2.1 feature specifications sooner
  - Follows the process we had when we started 2.1 and we called features "completed"
- **Cons**
  - Missing key feature specifications needed by market and use cases
  - Lacks support of extension mechanism
  - Lacks implementation verification
  - No verified or definition of interoperability of features/behaviors

Process Preferences Ballot

Moderating: Richard Struse - Chair, CTI TC

Ballot will be published ASAP to determine TC decision

TC Voters this means YOU!!!!!!!

Choose one of the two options presented

Q & A

Richard Struse – Chairman, CTI TC
Jane Ginn - Secretary, CTI TC

Cyber Threat Intelligence
Technical Committee