Cyber Threat Intelligence: Technical Committee (CTI TC)

Monthly Meetings – **16 November**
Session #1 & Session #2

STIX™ & TAXII™

Agenda

Moderating: Richard Struse - Chair, CTI TC

- STIX update
  - Status of 2.1 Data Objects
- Observables update
  - Ongoing discussions + Patterning
- TAXII update
  - Discussions on Version 2.1
- Interop update
  - Plans for Upcoming Plugfest
- Update on Salt Lake City F2F

STIX Subcommittee Update

John Wunder and Sarah Kelley – Co-Chairs

- Assertion
  - Had two working calls, one left if necessary.
  - The proposal is mostly done, found here: https://docs.google.com/document/d/15qD9KBQcVcY4FlG9n_VGhqacaeiLlNcQ7zVEjc8l3b4/edit#heading=h.qxvz3vox3ksj
  - Bret sent a list to potentially use for `assertion-category-ov`
- Grouping
  - One call left to discuss it (if needed)
  - Open question is over the values in `grouping-context-ov`
  - https://docs.google.com/document/d/15qD9KBQcVcY4FlG9n_VGhqacaeiLlNcQ7zVEjc8l3b4/edit#heading=h.t56pn7elv6u7

STIX Subcommittee Update

John Wunder and Sarah Kelley – Co-Chairs

- Infrastructure
  - 3 calls left for discussion (if needed)
  - Need to do modeling exercises
  - Open questions: Do we need the object? How does it relate to Observed Data/Indicators? Should it have external or embedded relationships?
  - https://docs.google.com/document/d/15qD9KBQcVcY4FlG9n_VGhqacaeiLlNcQ7zVEjc8l3b4/edit#heading=h.maky5z1n51ds

STIX Subcommittee Update

John Wunder and Sarah Kelley – Co-Chairs

- IEP
  - We seem to have consensus to add it with a caveat saying we’re adding it to facilitate interchange but not defining how to implement it in tools
  - https://docs.google.com/document/d/1wiG6RoNEFaE2lrblfgjpu3RTAJZOK2q0b5OxXCaCV14/edit#heading=h.8tzg8tq7p9du
- COA
  - Jyoti has sent the proposal to the list for possible inclusion in 2.1.
  - This was not built into our original time-boxed schedule, so opening this for discussion will require scheduling additional working calls.
  - https://docs.google.com/document/d/1VVeXcXsKHbfjjdglLo-mFQlXpjUhyGbGUBPSBFnSERY/edit#

Cyber Observables Subcommittee Update I

Trey Darley & Ivan Kirillov – Co-Chairs

- **Malware object moved from working concepts into STIX 2.1, Part 2**
  - https://docs.google.com/document/d/1bkMmU1PxlwlAwjrMmyWV147rvLcRs2x62FicHbpH2gU/edit#heading=h.cabdb5lryb9q
- **DNS objects need review**
  - https://docs.google.com/document/d/1PHRpmizbMGOwAu_TwRj5ofwnUEOIoM__vIDCDZGf4Sk/edit#heading=h.rxnh1v7ak6vl
  - DNS Query
  - DNS Response
  - DNS Record
- **We've been investigating DNS-based patterns**

```
[network-traffic:protocols[*] = 'dns' AND network-traffic:extensions.'dns-query-ext'.qname_ref.value = 'badstuff.example.com' AND network-traffic:extensions.'dns-query-ext'.qtype = 'TXT']
```

Cyber Observables Subcommittee Update II

Trey Darley & Ivan Kirillov – Co-Chairs

- **We've proposed an enhancement to Patterning for 2.1**
  - https://docs.google.com/document/d/12ZcuQWzNmPdpOJSNgvQFn59AgPAOorCW6ymQScxzdkM/edit#heading=h.tqad81km2lrm
- **There is a need for specifying that element of a pattern MUST match on the same item in a list**
  - **E.g., the list of values under a Registry Key**

```
[win-registry-key:values[s].data MATCHES '^\d+$' AND
win-registry-key:values[s].name = 'ImagePooth')]
```

Interoperability Subcommittee Updates

Allan Thomson & Jason Keirstead – Co-Chairs

- **No active work on Interoperability documents until after F2F in Jan**
  - **Test Document Part 1 Approved**
  - **Test Document Part 2 Committee considers complete but pending edits/ballot after plugfest**
  - **OASIS STIX Preferred logo and brand in progress**

- **Plugfest (Jan 30 2018)**
  - **TC Participants: 11 orgs/individuals**
  - **Planning document has been completed 90%**
    - **Tests cover persona (TXS, DFP, TIP, TMS, TDS, SIEM)**
    - **Basic connectivity, sharing and collaboration**
  - **All remaining meetings for 2017 are not required**
  - **Participants agreed to reconvene early January to finalize last minute details on setup**

Salt Lake City CTI TC F2F

Bret Jordan of Symantec – Host

Wednesday January 31st & Thursday February 1st, 2018

High Level Agenda:

- PlugFest DeBrief
- STIX 2.1 topics + STIX 2.2 Roadmap
- TAXII 2.1
- Interoperability for STIX 2.1 Planning

Register ASAP on EventBrite!

http://bit.ly/SLC-CTI_TC_F2F

Hackathon @ FIRST/OASIS Event in Prague

Richard Struse

- Friday, December 8th
- Provide participants with a corpus of STIX 2 data and a set of suggested challenges/problems to solve
- We will have STIX2 data from a variety of sources!

Q & A

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

Cyber Threat Intelligence
Technical Committee