CTI-TC Monthly Meeting: Session #2

Meeting Date: **November 15, 2018**
Time: **Session #2 – 9:00 PM US EST**
Purpose: **Monthly CTI TC Meeting**
Attendees:

Name	Company	Role
Kai Li	360 Enterprise Security Group	Voting Member
Kyle Maxwell	Accenture	Voting Member
Jane Ginn	Cyber Threat Intelligence Network, Inc.	Secretary
Toshitaka Satomi	Fujitsu Limited	Voting Member
Kunihiko Yoshimura	Fujitsu Limited	Voting Member
Elysa Jones	Individual	Voting Member
Terry MacDonald	Individual	Member
Allan Thomson	Looking Glass	Voting Member
Jonathan Baker	Mitre Corporation	Member
Sarah Kelley	Mitre Corporation	Voting Member
Nicole Parrish	Mitre Corporation	Member
John Wunder	Mitre Corporation	Voting Member
Richard Struse	Mitre Corporation	Co-Chair
John-Mark Gurney	New Context Services, Inc.	Voting Member
Christian Hunt	New Context Services, Inc.	Voting Member
Bret Jordan	Symantec Corp.	Voting Member
Richard Shok	U.S. Bank	Voting Member

Agenda:

- Interop Update | PlugFest Update | COA SDO Update
- Community Development Corner: Visualizer
- Subcommittee Updates
- Face-to-Face in January in California – Fujitsu
- Change in date for Dec. meeting

Meeting Notes:

Richard Struse

Opened meeting and asked all to register participation

Allan Thomson

Both Part 1 and Part 2 have been approved by Ballot
If you have comments on the STIXpreferred Portal, please add to the document
https://docs.google.com/document/d/1MCnrLR4m1CnkqZcLM0FcIzgJrvId3on3GTkqcwtdH1I/edit#heading=h.i3o6gvkwteti
We are going to plan out a Launch with OASIS
This is the first Certification process that OASIS has ever done

Allan Thomson

[*Gave update on status of next PlugFest*]

Will be postponed for another date in the future
We need more commonality across companies that want to test features
We'll keep a list and have a rolling sign-up
We want to build of pipeline to gauge interest
https://docs.google.com/document/d/1V7zAg2rl-QOkIFbZjv4mgDZ-Z2_GRTjGsoI2ZUi99bk/edit?ts=5bec471c#heading=h.r4ruh38j0l6

Allan Thomson

[*Gave an update on the Mini Group to sort out the best way to handle*]
Cyber Observables
Let Trey or I know if you want to get involved
[*Summarized key points – Status*]
Mini-group have agreement on use cases and needs for the use cases
A compromise concept *in principle* is being discussed in mini-group that has promise
o Call to get involved (reach out to Allan/Trey) to be added the meetings

a. Introduce a deterministic mechanism to identify cyber observables and directly reference those cyber observables from objects
b. Support a mechanism for semantic equivalence of cyber observables
c. Introduce options on relationships that supports objects and cyber observables connections

Richard Struse

[Made some points about how Allan has tried to facilitate reaching a Use Case
To address most of the key points]
We want stability with respect to STIX2 – We want to reach a consensus
That is not unanimity – We need to make progress, we need to move forward
What is the best approach? We want to identify solutions for the majority of the TC
Update on the Visualizer:

CTI STIX Visualizer has been updated to support visualization of custom objects

- Configurable via JSON
  - Allows users to specify which property should be used for node labels of that type in the graph and which icon image to use
  - By default, displays a ? icon

```
{
    "x-example-com-customobject": {
            "display_property": "something_custom",
            "display_icon": "customobject.png"
    }
}
```

https://github.com/oasis-open/cti-stix-visualization

Sarah Kelley

[*Gave update on the COA object*]
STIX 2.1 COA Object Update
Allows for the capture of a structured COA
Big upgrade on the existing stub!
Updated proposal has been discussed (with good consensus)

now merged into the working draft of the next CSD

Some remaining questions/discussion around the context of "action_os_versions" capture the operating system versions that the action is applicable to https://docs.google.com/document/d/1bkMmU1PxlwlAwjrMmyWV147rvLcRs2x62FicHbpH2gU/edit#heading=h.a925mpw39txn

[*Gave update on POC Sponsorship*]

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!

Bret Jordan

Update on TAXII2 changes – Working Draft 4 should go out tomorrow

- TAXII 2.1 Working Draft 04 will be released tomorrow
  - 2-week review period ending November 30th
  - Depending on feedback, move to CSD
- Working Draft 04 includes
  - TAXII Envelope
  - Some URL Parameters (limit, spec_versions)
  - Wordsmithing and document cleanup
  - More tightly coupled to STIX

Richard Struse

Thanks Bret for all your work…and all on TAXII2

[*Gave update on January Face-to-Face*]

January 29-30 2019 at Fujitsu in Sunnyvale, CA USA
GCDP North Café
Fujitsu Sunnyvale Campus
1250 E. Arques Avenue
Sunnyvale, CA 94085-5401

[*Gave update on change in schedule for December meeting*]

It will be the 2nd Thursday during December – Dec. 13th, 2 session

Meeting Terminated
****