CTI-TC Monthly Meeting: Session #2

Meeting Date: October 17, 2019
Time: Session #2 – 9:00 AM US EDT
Purpose: Monthly CTI TC Meeting

Attendees:

Name	Company	Role
Thompson, Dean	Australia and New Zealand Banking Group (ANZ)	Voting Member
Ginn, Jane	Cyber Threat Intelligence Network, Inc. (CTIN)	Secretary
Joyce, Ryan	DarkLight, Inc.	Voting Member
Satomi, Toshitaka	Fujitsu Limited	Voting Member
Yamada, Koji	Fujitsu Limited	Voting Member
Yoshimura, Kunihiko	Fujitsu Limited	Voting Member
Takami, Yutaka	Hitachi, Ltd.	Voting Member
Keirstead, Jason	IBM	Voting Member
Lenk, Chris	Mitre Corporation	Voting Member
Struse, Richard	Mitre Corporation	Co-Chair
Kakumaru, Takahiro	NEC Corporation	Voting Member
Gurney, John-Mark	New Context Services, Inc.	Voting Member
Riedel, Daniel	New Context Services, Inc.	Voting Member
Storms, Andrew	New Context Services, Inc.	Voting Member
Varner, Drew	NineFX, Inc.	Voting Member
Jordan, Bret	Symantec Corp.	Voting Member
Girard, David	Trend Micro	Voting Member

Agenda:

- Introduction & Welcome
- Sub-Committee Updates
  - STIX
  - TAXII
- Community Development Corner
  - Chris Lenk - Python STIX2 Library

Meeting Notes:

Richard Struse

Welcome to monthly meeting

Bret Jordan

Went through updates needed – and process

We do need some Sponsors

STIX update

- Currently working on an update to Patterning based on public review feedback
- Watch for ballots for another round of CSDs and Public Reviews
- Sponsors needed

- Trial Office Hours under development

Still Need Sponsors

Current Status

- Course of Action (Cisco,)
- Grouping
- Infrastructure (New Context,)
- Malware
- Malware Analysis
- SCOs as top-level objects (LookingGlass,)
- SCO relationships (LookingGlass,)
- Deterministic IDs (MITRE, LookingGlass)

Important to prove that the spec is complete and they examples are clear

TAXII update

Gave some background on revised pagination – gave some schedule updates

- Pagination functionality added
- We will try and send out a new working draft for final review today
- Watch for ballots for another round of CSDs and Public Reviews

Sponsors needed

- Pagination refactoring (FreeTAXII,)
  - next URL parameter
  - limit URL parameter
  - envelope changes
- Delete Endpoint added (FreeTAXII, MITRE)
- Versions Endpoint added (FreeTAXII, MITRE)

Richard Struse

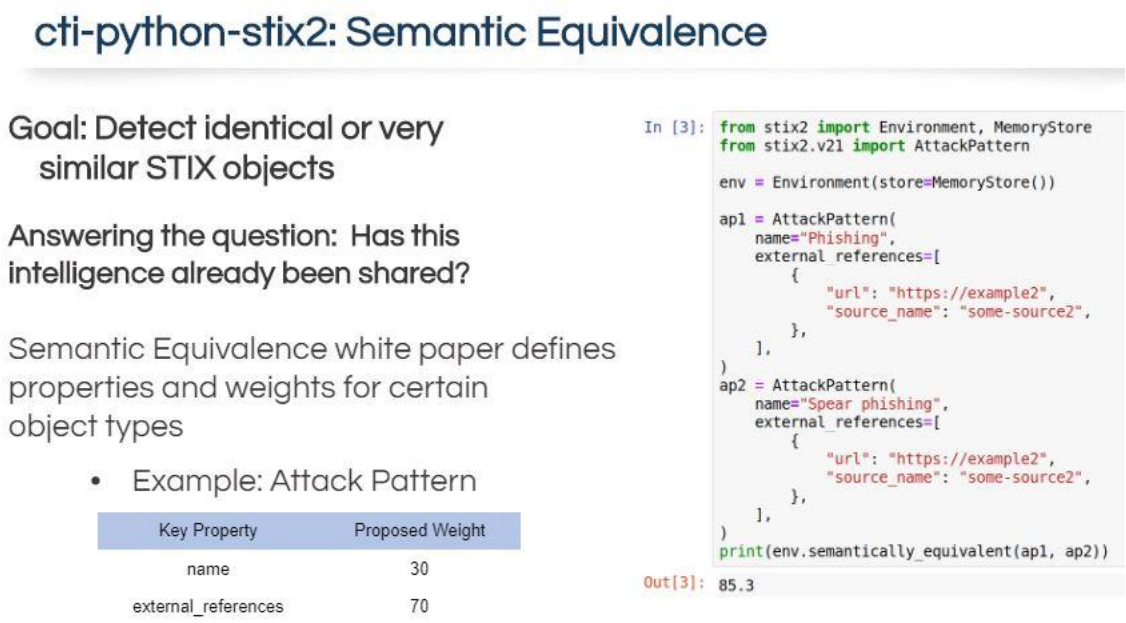
Interoperability Subcommittee

Please welcome our newest co-chair of the Interoperability Subcommittee:
Justin Stewart from **LookingGlas**s

Relatively new Co-Chairs – have continued support from Allan and Jason
A lot of work done on STIXPreferred program – to address problems with STIX 1.x
This will help us – We learned from our mistakes
This gives us a way for companies to perform tests on their own
Work with the Co-Chairs – in 2020 – Plan for PlugFests
If you are interested in getting involved – reach out to Rich, Trey or Jane
And Co-Chairs
We are all Ambassadors to the Community
I'll be posting on LinkedIn – I want to tell the story
All of us should feel empowered to tell your story

Chris Lenk

Community Development Corner



- Currently only some SDOs defined
- Only takes into account properties actually present on the objects
- Can be configured:
  - Weights
  - How properties are compared
  - Additional object types
- Documentation and examples: https://stix2.readthedocs.io/en/latest/guide/equivalence.html

Richard Struse

Thanks everyone – we'll have another session this evening at 9:00 pm US EDT

Meeting Terminated

****