CTI-TC Monthly Meeting: Session #1

Meeting Date: October 17, 2019
Time: Session #1 – 11:00 AM US EDT
Purpose: Monthly CTI TC Meeting

Attendees:

Name	Company	Role
Coderre, Robert	Accenture	Voting Member
Maxwell, Kyle	Accenture	Voting Member
Ginn, Jane	Cyber Threat Intelligence Network, Inc.	Secretary
Darley, Trey	CERT.be	Co-Chair
Hohimer, Ryan	DarkLight, Inc.	Voting Member
Riley, Shawn	DarkLight, Inc.	Voting Member
Roberts, Ian	DarkLight, Inc.	Voting Member
Rosa, Michael	DHS Office of Cybersecurity & Communications	Observer
Taylor, Marlon	DHS Office of Cybersecurity & Communications	Voting Member
Huey, Caitlin	EclecticIQ	Voting Member
O'Brien, Christopher	EclecticIQ	Voting Member
van Belkum, Aukjan	EclecticIQ	Voting Member
Morris, John	IBM	Voting Member
Ratliff, Emily	IBM	Voting Member
Williams, Ron	IBM	Voting Member
Casey, Tim	Intel Corporation	Voting Member
Aviles, Jorge	Johns Hopkins U. Applied Physics Lab	Observer
Pumo, Beth	Kaiser Permanente	Voting Member
Applegate, Alex	LookingGlass	Member
Hostetler, Dennis	LookingGlass	Voting Member
Pladna, Matt	LookingGlass	Voting Member
Serban, Vlad	LookingGlass	Voting Member
Stewart, Justin	LookingGlass	Member
Thomson, Allan	LookingGlass	Voting Member
Kirillov, Ivan	Mitre Corporation	Voting Member
Lenk, Chris	Mitre Corporation	Voting Member
Piazza, Richard	Mitre Corporation	Voting Member
Struse, Richard	Mitre Corporation	Co-Chair
Vargas-Gonzalez, Emmanuelle	Mitre Corporation	Voting Member
Butt, Michael	NC4	Voting Member
Davidson, Mark	NC4	Voting Member
Dye, Daniel	NC4	Voting Member
Hunt, Christian	New Context Services, Inc.	Voting Member
Jordan, Bret	Symantec Corp.	Voting Member
Keith, Robert	Symantec Corp.	Voting Member
Kostrosky, Curtis	Symantec Corp.	Voting Member
Merchant, Aubrey	Symantec Corp.	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

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)

TAXII update

- 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)

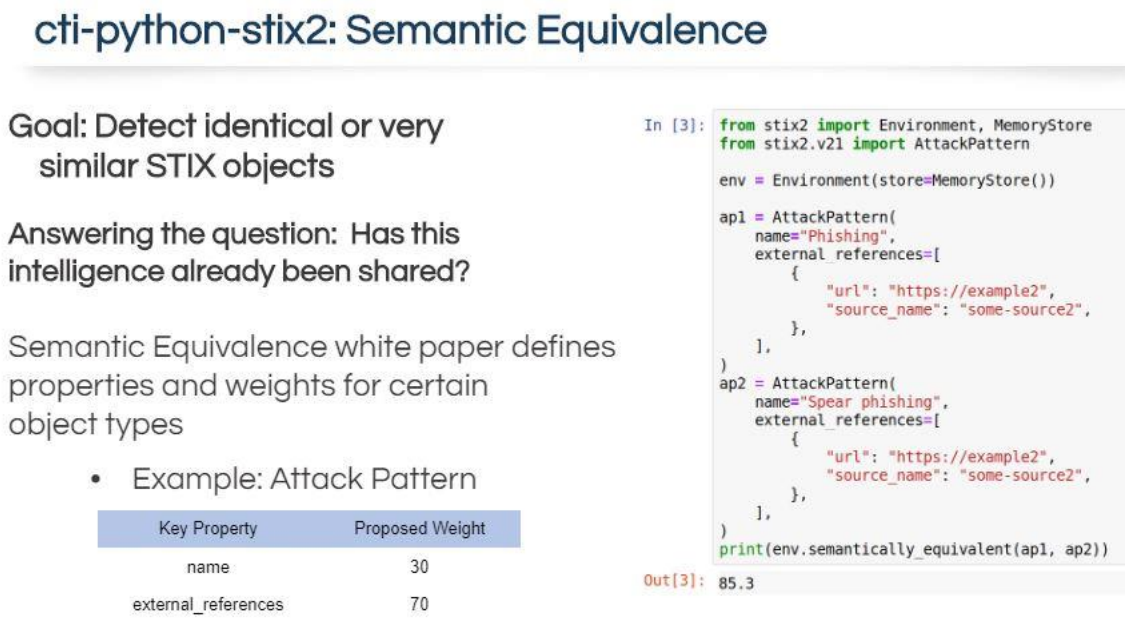
Richard Struse

Interoperability Subcommittee

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

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

****