CTI-TC Threat Actor Open Repository User Group

Meeting Date: August 2, 2019
Time: 11:00 AM US EDT
Purpose: Kick-off Meeting

Attendees:

Name	Company
Jane Ginn	Cyber Threat Intelligence Network
Ryan Hohimer	Darklight
Shawn Riley	Darklight
Marlon Taylor	Department of Homeland Security
Preston Werntz	Department of Homeland Security
Catlin Huey	EclecticIQ
Chris O'Brian	EclecticIQ
Sergey Polzunov	EclecticIQ
Sean Barnum	FireEye
Paul Patrick	FireEye
Tim Casey	Intel Corporation
Javier Garcia Robles	LookingGlass
Ivan Kirillov	Mitre Corporation
John Wunder	Mitre Corporation
Bret Jordan	Symantec
Robert Keith	Symantec
David Girard	TrendMicro

Agenda:

- Harmonizing Threat Actor Concepts
- Discuss Framework & Coordination
- Discuss Resources

Meeting Notes:

Jane Ginn

Gave background on issue – noted discussion on Slack that led to the meeting

STIX 2.1 Threat Actor SDO Summary

SDO	Required Common Properties	Optional Common Properties	Not Applicable Common Properties	Threat Actor Specific Properties
Threat Actor	type spec_version id created modified	created_by_ref revoked labels confidence lang external_references object_marking_refs granular_markings	defanged extensions	name description threat_actor_types aliases first_seen last_seen roles goals sophistication resource_level primary_motivation secondary_motivation personal_motivations

Noted existing resources:

- Florian Roth et. al. Matrix https://docs.google.com/spreadsheets/u/1/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/pubhtml
- ATT&CK 'Groups' https://attack.mitre.org/groups/
- MISP-Galaxy https://github.com/MISP/misp-galaxy/blob/master/clusters/threat-actor.json
- ThaiCERT Cards
- CERT.be
- Other???

Noted use of Open Repository for governance as a User Group

- Authorization
  - OASIS TC Open Repository Policies
    - https://www.oasis-open.org/policies-guidelines/open-repositories
  - Membership
    - CTI TC Members & non-Member Contributors
      - All must sign an OASIS Contributor License Agreement (CLA) https://www.oasis-open.org/resources/open-repositories/cla/

First Order of Business

Must be approved by Ballot by the CTI TC

"Each TC Open Repository should have a purpose statement, indicating its intended contents or topic, declared by the TC that creates it, as part of its approval action."

Noted Resources

- **CTI TC Ad Hoc Meeting Link**
  - https://newcontext.zoom.us/j/332585406
- Github?
  - "OASIS initially will create TC Open Repositories as either distinct GitHub projects, or distinct Subversion repositories."

Sean Barnum

Asked for clarification on purpose –

pointed out usefulness for building on STIX 2.1 framework

Noted that harmonizing existing frameworks more problematic

Tim Casey

Noted origins of Threat Actor properties came from his team

This could be useful to help members of community to tell the story of the threat actor

John Wunder

Noted that ATT&CK Groups was developed only to help describe TTPs not as Threat Actor DB

Ryan Hohimer

Looking at it from technical POV – Should be a graph database that will allow individual schemas – could be viewed through the lens of STIX 2.1

Sean Barnum

Becomes a "named graph" – different fields represent different levels of assertion

A vision statement for moving forward

Should be referenceable as "linked data"

Ryan Hohimer

I could support this

Jane Ginn

Asked if CVE was "lined database"

Sean Barnum

Clarified that it is not – It is a structured DB

Bret Jordan

Pointed out the STIX 2.1 is a data model for transport

A lot of innovation will be taking place as we move forward with work of TC

Jane Ginn

Laid out next steps:

1. Develop Statement of Purpose
2. Begin dialogue with OASIS Management
3. Run a TC Ballot to approve
4. Set-up a separate Slack group (OASIS members and non-members – All sign CLA)
5. Set-up meeting schedule – 2 times a month
6. Doddle Poll - Find time on Tues., Wed. or Thurs

Marlon Taylor

Noted that some people that are interested in User Group may not be at meeting

Jane Ginn

Noted announcements about the User Group will go out to full TC

Noted some of the community resources specific to the Threat Actor SDO:

Icons

https://github.com/freetaxii/stix2-graphics/tree/master/icons/png/stix2-adversary-icons-png

Open Vocabularies are in the Spec

NOTE: If you are interested in being part of the TA Open Repository User Group and you were not able to attend, please send an email to Jane Ginn (jg@ctin.us) to be included on follow-up correspondence

Meeting Terminated

****