CTI-TC Monthly Meeting: Session #2

Meeting Date: **December 13, 2018**
Time: **Session #2 – 9:00 PM US EDT**
Purpose: **Monthly CTI TC Meeting**
Attendees:

Name	Company	Role
Jonathan Baker	Mitre Corporation	Member
Jane Ginn	Cyber Threat Intelligence Network, Inc.	Secretary
John-Mark Gurney	New Context Services, Inc.	Voting Member
Ryusuke Masuoka	Fujitsu Limited	Voting Member
Toshitaka Satomi	Fujitsu Limited	Voting Member
Vlad Serban	LookingGlass	Voting Member
Richard Shok	U.S. Bank	Voting Member
Natalie Suarez	NC4	Voting Member
Dean Thompson	Australia and New Zealand Banking Group	Voting Member
Allan Thomson	LookingGlass	Voting Member
Koji Yamada	Fujitsu Limited	Voting Member
Kunihiko Yoshimura	Fujitsu Limited	Voting Member

Agenda:

- Introduction & Welcome (Trey & Rich)
  - TAXII Ballot (Bret)
  - STIXPreferred Update (Allan)
- Update on Cyber Observables Mini-Group (Allan)
  - Background & Motivation
  - Use Cases for 95% & Current Proposals
  - Update on Status
- Sub-Committee Updates
  - STIX (Sarah & Ivan)
  - TAXII (Bret) + CDC Demo
- F2F Update - Sunnyvale (Rich, Trey & Ryu)

Meeting Notes:

Richard Struse

Welcome and please record your attendance

Bret Jordan

Update on the TAXII Ballot – Formal Standards approach – Need for formal Ballots

- Committee Specification Draft 02 (Working Draft 05)
  - Editorial changes and User-Agent description
  - Please vote
- Proposed Schedule Post CSD 02 (if it passes)

- 30-day Public Review Period
- CSD 03 based on Working Draft 06 (changes from PRP)
- 15-day Public Review Period
- Ballot to make TAXII 2.1 a Committee Specification

Allan Thomson

- STIXPreferred Launch Planning
  - Mini-group formed on STIXPreferred launch tasks
    - Chet, Carol and Dee (OASIS)
    - Allan, Jason, Rich, Trey, (CTI TC)
- Pre-Launch Activities (now to Feb 15th)
  - Committee review team alias updates/operational checks
  - Define & Review rules of review committee operation
  - Test examples posted for use by vendors
- Phase 1 Launch Targeting Vendors (now to Mar 31st)
  - Outreach to orgs that wish to be included in the initial launch activity announcements including press release, social presence...etc.
  - Must have at least 1 approved STIXPreferred certified product
- Phase 2 Launch Market/Vendors (April 2019)
  - Press release; Social media; Web-site updates
  - Webinar

Allan Thomson

Update on PlugFest Sign-up

- Future plugfests sign-up sheet

https://docs.google.com/document/d/1V7zAg2rl-QOkIFbZjv4mgDZ-Z2_GRTjGsoI2ZUi99bk/edit?ts=5bec471c#heading=h.r4ruh38j0l6

We will hold the next one when there is enough interest

It is intended to be a developer-friendly environment

Please, no marketing or sales

Allan Thomson

Went over the Agenda for the Cyber Observables Mini-Group Discussion

- Status
- Background – How we got here
- High-level Requirements of the New Feature
- Summary Proposal
  - Standard IDs
  - Org Customizable IDs
- Where we stand
- Next Steps

INTRODUCTION & STATUS

- Mini-group has been working on this proposal for multiple weeks
  - Some agreement and progress has been achieved but open questions remain
- If no agreement and supporting text shared with TC by 31st Jan 2019 then we will revert to Malware definition contained in following document for 2.1 (and vote on inclusion)

https://docs.google.com/document/d/1xZLjT4kpjQRuCo_CXh9xUAOfO3-lQfiWo5VhJ7MsnxQ/edit

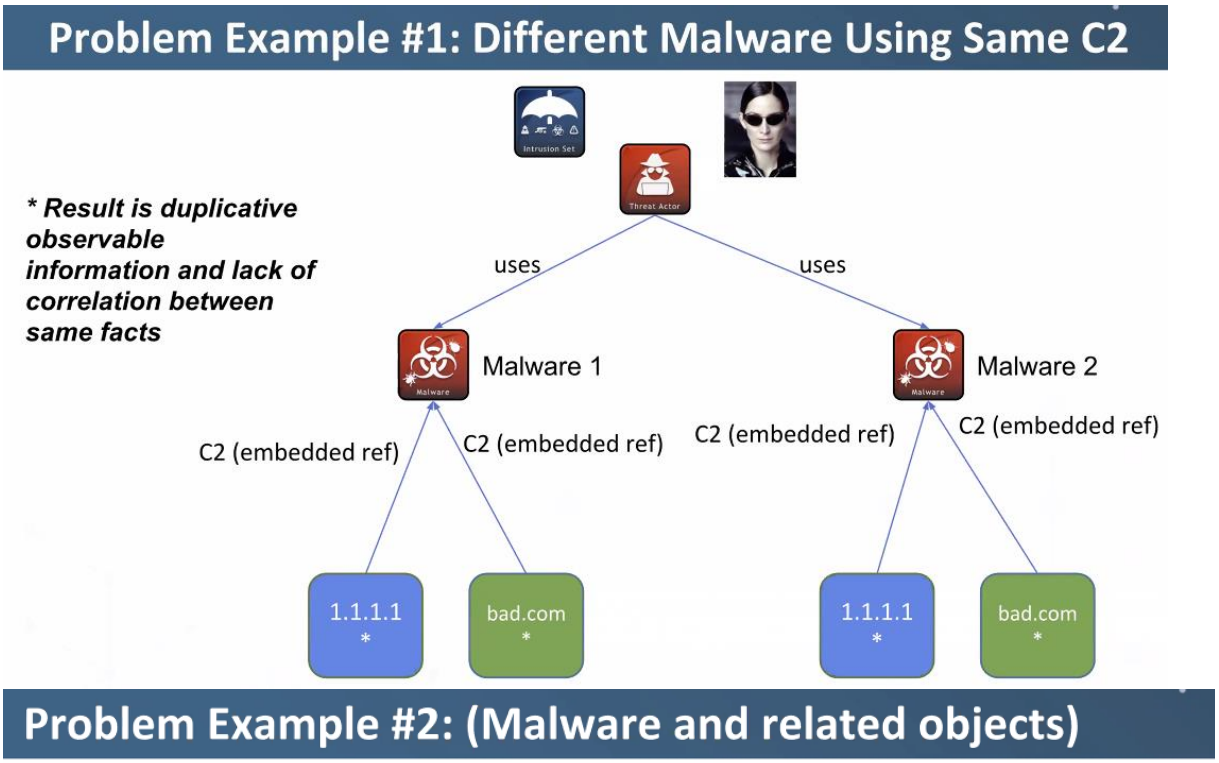
[*Allan asked a question was asked about whether there were any objections to the approach*]

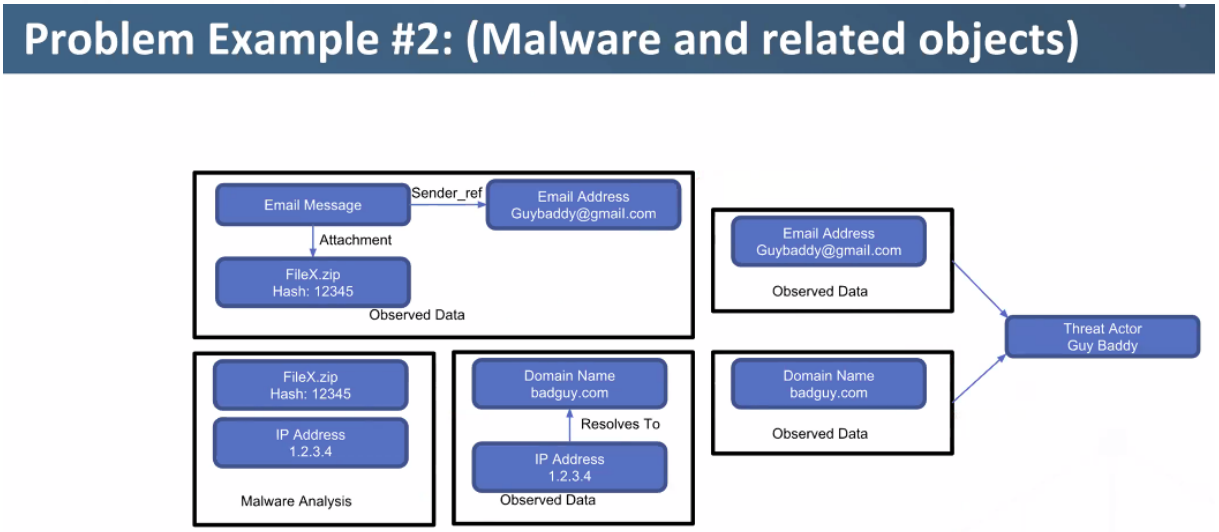
There were no objections

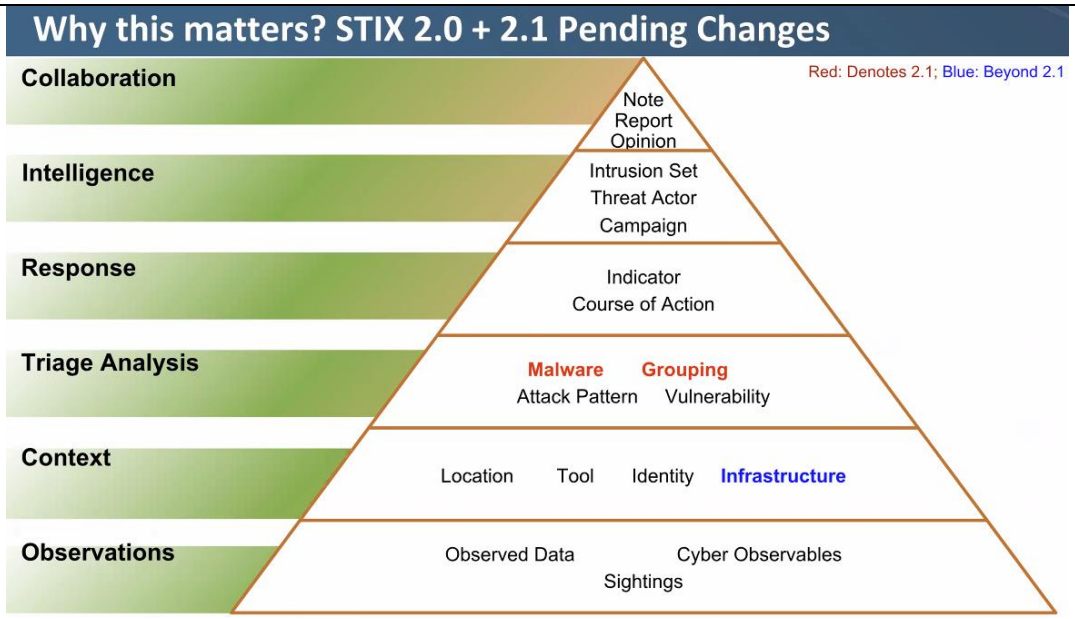
BACKGROUND

- There have been multiple use cases identified that require the data captured currently within Cyber Observables must be referred to or included with TLOs such as malware
  - Future TLOs such as infrastructure would also benefit from this capability
- In many cases ineffective or inadequate data modelling using Observed Data containing Cyber Observables referred from Malware would work in some cases but not in others
  - NOTE: Many use cases previously defined for Observed Data continue to be valid

- There is a strong desire to find an approach that can support as many of the problematic use cases as possible while supporting the previous work leveraging Observed Data



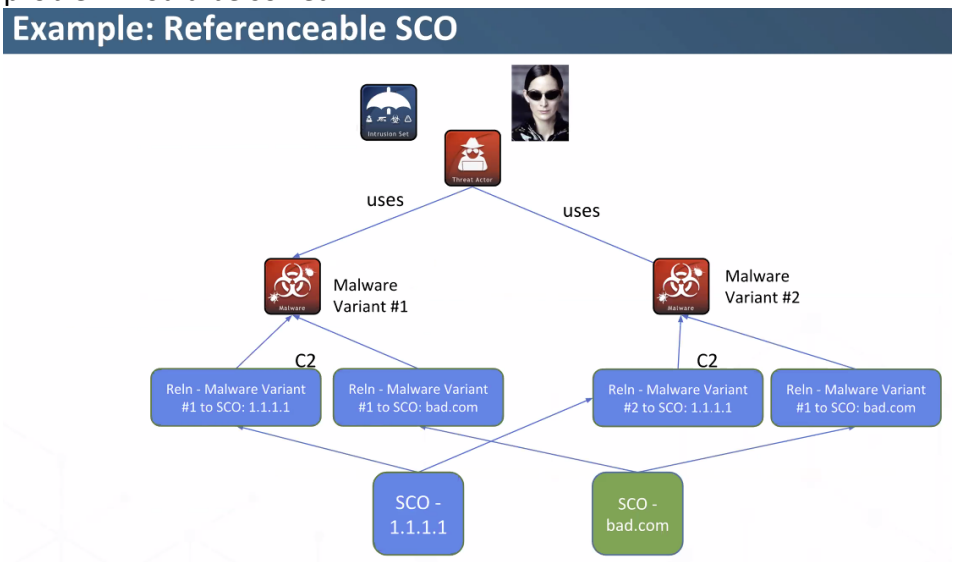




KEY REQUIREMENTS

- MUST have a way to represent objects like Malware (future: Infrastructure) including all associated meta-data that includes facts/cyber observables
    - MUST be able to include supporting facts (i.e. cyber observables) and create relationships between facts and associated TLOs
- Easily creatable and should be able deterministic IDs enable scalable CTI applications especially when handling billions of facts
- CTI producers MUST be able to inform their consumers on how data correlates across both objects and facts
- CTI consumers and producers SHOULD be able to reference/correlate objects & facts from other producers

Allan noted that if we do adopt this approach, the following diagram shows how the problem would be solved



PROPOSED SOLUTION: Part 1 – Standard SCO IDs

- Introduce ID property for SCO (STIX Cyber Observable)
- Will define a **subset** of cyber observable properties per cyber observable that make up the ID for that cyber observable
- Will update relationships to allow references between SDO/SRO/SCO
- Introduce ID-creation-mapping property
    - Absence of property and default will be standard defined in spec
- Will define standard mapping for ID creation property
- Compliance:
    - Will add statement on orgs **SHOULD** use the defined approach for SCO ID creation
    - STIXPreferred Interoperability will be updated to include testing for specific persona

PROPOSED SOLUTION: Part 2 – Organization Custom SCO IDs

- Producers MAY define their own ***separate*** method for creating an ID on a per-object basis
    - **Used instead of standard ID creation method**
- Producers **MUST** publish those ID creation definitions in a CTI OASIS defined schema if non-standard approach
- Producers and Consumers MAY BE ABLE generate an org-specific IDs
- Secondary Org MAY reference Original Producer's objects provided ID

PROPOSED SOLUTION: SCO ID Creation

- Will use version of Digital Signature proposal with modifications
- Add text to STIX2.1 draft text instead of SEP
- Update to state how it is used for SCO properties
- Update to include none (i.e. missing property)
- Update to consider Hash algorithm (do we really need 512 when considering the impact on amount/size of SCOs)
- **TC Question: Any objections to taking a 2 part approach (standard IDs & org specific IDs) leveraging an updated digital signature mechanism for the SCO properties including in the ID?**

[*Allan paused to give an opportunity for debate – No objections shown*]

Jane Ginn

[Noted that this represents a compromise from some very diametrically opposed views]

WHERE MINI-GROUP CURRENTLY STANDS

- We **agree** that an ID is required for SCOs with the following properties
    - It should be possible to deterministically compute on both creation (producer side) and useful for search (consumer side)
    - It's easy to create (for both sides)
    - It can be referenced by relationships across transactional/individual units of intel (i.e. bundles)
    - The ID will be computed on a subset of SCO properties <- mini-group consensus last week
- We **need to work** on
    - A) Finalize text on all changes including ID creation, referencing and SCO updates

Richard Struse

Thanks to Allan for working towards a compromise on this very important issue

Sarah Kelley

- Sponsor updates - Confidence/Note/Opinion
- Documents:
  - Confidence: https://docs.google.com/document/d/1-Bl7dEYIbepKHunc6Narcpa79IaRIePb28wv8IbHJtY/edit#heading=h.gjdgxs
  - Opinion: https://docs.google.com/document/d/17hEBdomv6zqUCQTXnmXRzhX5mLqrSgsX3Vc5ZqNoJu4/edit#heading=h.gjdgxs
  - Note: https://docs.google.com/document/d/11piq3g99fTDbiKpXrO1V3WV0581VjKlxJejm908cJd4/edit#heading=h.gjdgxs
- Documents will include
  - Specific use cases that were tested
  - If use case POC code demonstrates Producer or Respondent
  - Interop tests

We still need a Sponsor for the Location SDO – We will drop it from the Spec

If we don't get that 2nd Sponsor

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

[*Noted that there are some potential supporters for the Location object moving forward*]

Jane Ginn

[*Gave shout-out to all of those that are participating in the current Sponsor groups*]

Bret Jordan

Reminder to Vote on the TAXII Ballot

https://www.oasis-open.org/apps/org/workgroup/cti/ballot.php?id=3283

Discussion on What Constitutes "Done" for TAXII

- Should TAXII have similar requirements to STIX for measuring its DONE-ness?
- What should those be?
  - Specification Text (obviously)
  - Interoperability Tests
  - Working Proof of Concept Code
- What constitutes a features that needs to be assessed?
  - In STIX this generally means new objects but not really changes or additions to objects.

TAXII Process Approach

- How should we determine in TAXII:

- If a feature or enhancement should be worked on / added to the specification?
- Which proposal we should adopt if there is more than one?
- When a feature or enhancement is deemed complete or shippable by the TC?

- How should we handle requests when the TC is either
  - contentious about a feature or
  - apathetic about a feature

Bret Jordan

Community Development Corner (CDC)

- Demo of TAXII 2.1 compliant features
  - New envelope and Pagination
  - Media Type Changes
  - New Versions Endpoint

https://test.freetaxii.com:8000/taxii2/

Richard Struse

[*Gave Update on the Face-to-Face & Welcome from Ryu*]

January 29-30 2019 at Fujitsu in Sunnyvale, CA USA

GCDP North Café
H Building - Fujitsu
Sunnyvale Campus
1250 E. Arques Avenue
Sunnyvale, CA 94085-5401

Go to Front Desk of H Building to be escorted to the Meeting Room

Register here:
https://www.eventbrite.com/e/oasis-cyber-threat-intelligence-f2f-tc-meeting-january-2019-registration-53540053742

Dean Thompson

[*Asked for some training materials – Sarah provided a link to the GitHub site*]

Richard Struse

Thank you all – See you next month at our regular time.

Meeting Terminated

****