CTI-TC Interop Working Session

Meeting Date: March 21, 2018
Time: Noon US EDT/9:00 a.m. US PDT
Purpose: Weekly CTI TC Interoperability Meeting

Attendees:
- Allan Thomson – Moderator
- Richard Struse
- Jane Ginn - Recorder
- Philip Royer

Agenda:
- Review of Parts 1 & 2

Meeting Notes

Allan Thomson

I want to go through some of the comments.
Let’s deal with some of Phil’s comments

Philip Royer

[Discussion on TMS testing comment on Part 1 & Part 2]

Allan Thomson

[Made adjustments in the document to address Philip’s comment]
Went into Draft Part 2 to address the comments – [Shared Screen]
https://docs.google.com/document/d/11MocPK3s8im8O5-7rgZhtVHoXO72aQicjj2v-HDx-Q8/edit#heading=h.4do73o99e2l7

Philip Royer

[Made additional comments on tests that were referenced in the 3.5 tables]
[Presented position on Identity object and how it works within Interop]

[Referenced email that went out earlier this week – Both Jason and Bret
Have opinions on this... we’ll have to go through
Went through slide deck on what the Use Cases would be
Use Cases – coming from the Spec

STIX 2.0 Identity Use Cases

• Use Case #1: Identity of **Intel Provider** (individual or org)

• Use Case #2: Identity of **Target** of Attack Pattern | | Campaign |
  Intrusion Set | | Malware | | Threat Actor | | Tool

• Use Case #3: Identity of **Associated/Related** Threat Actor

Showed slide Copied from Spec to refresh everyone’s understanding

Identity Specification

• **Identities can represent actual individuals, organizations, or groups** (e.g., ACME, Inc.) as well as classes of individuals, organizations, or groups (e.g., the finance sector).

• **The Identity SDO can capture basic identifying information, contact information, and the sectors that the Identity belongs to. Identity is used in STIX to represent, among other things, targets of attacks, information sources, object creators, and threat actor identities.**

  • Embedded/Common Relationships

  • Named relationships

[Posed a question about how entities identify **Identity** (person or org)]

Interoperability Part 1 and Part 2 Use Of Identity

• Interop Part 1 and Part 2 test Use Case #1 (currently)

  • Provider:
    • We test a provider’s ability to generate intelligence where that provider identifies itself (organization or group or individual) and shares both the identity and the associated intelligence

  • Consumer:
    • We also test a consumer’s ability to read that identity and associate that identity with the intelligence being consumed

• However...

Richard Struse

Created_by_ref is an optional property – But intelligence that does not
Say where it comes from is not very useful

[Differentiated between ‘Anonymous’ and ‘Anonamized’]

  My way of saying – Identity is an essential characteristic of intel

Philip
Most of the time we are going to want it – you might check the Identity of the provider before taking action on it

Allan

I was at a CISO Conference last night – I asked them

Almost 100% of the room said: Without knowing where intel comes from, it is almost garbage

For the majority of systems we are building – we don’t have the time

Our focus must be on the Majority Use Case

There is a reason by the Identity was made optional... but, for Interop,

It is very important

*****************************

Question 2

* Question #2: If you agree to Q1 is yes, then how will identity be provided in products?

* Choice #A: Once per *intelligence publication* where

  * An intelligence publication is one or more bundles pushed to a TAXII server where an intelligence publication is a set of data that may not fit into a single bundle or spans a period of time where the identity of all related intelligence does not change

* Choice #B: Once per bundle for each identity referenced in the bundle

  * So if N objects are provided by N producers then there would be N identities in that bundle

* Choice #C: Other?

Allan Thomson

Bret and Jason have a concern in TAXII – If you publish Intel on Day 1

Then, on Day 7, you publish new Intel, but don’t change Day 1

But, if you pull data from Day 7, but Identity object is assoc.

With Day 1

Other option, in TAXII – we do an explicit object look-up

This type of thing is much more real world – and up to product choices

That is a very complicated set of conditions –

Richard Struse

[From Chat]

What is the argument against Identity in this context?

Isn’t this a more general question that relates to more objects than Identity?

I’m reluctant to complicate this too much –

You need to do that per Bundle – If the reference is not in it

In that case, a lot of our assumptions will be broken

If there is no way to chase down a reference – a lot of our assumptions

Need to be questions

Philip Royer

[Posed question about Bundle vs. Collection]

Allan Thomson

Bundle is not a persistent object

Philip Royer

In that case, shouldn’t that Identity object be in the Collection – not Bundle

Allan

Interesting thought – ok, here is a test Collection

[Described how the Interop Test doc could be updated]
Richard

You could provide two different tests – One with Identity is in the Collection
And the other with a Look-up

Allan

What Jason and Bret were concerned about was that the latter case
Is more reflective of the real world
I think we should have both tests
Drew... do, you have a view on this?

Drew

I don’t like the idea of adding special context to the Bundle
Plus, there is always asynchronous order for delivery
To TAXII clients

Allan

I’m going to change the Spec to capture some of these thoughts

2.2.3.1 Indicator IPv4 Address

Verify the following data is in collection : X

```
"objects": [
  {
    "type": "identity",
    "id": "Identity::f431fe90-377b-45e0-a12c-3a4751ae6f09",
    "identity_class": "organization",
    "name": "AME Corp., Inc.",
    "modified": "2018-01-17T11:11:13.002Z"
  },
  {
    "type": "indicator",
    "id": "Indicator::54f2ab-636c-4d4d-8b0c-7d0fdd0ad5e0",
    "name": "Bad IP!",
    "description": "STIX TAXII 2.0 Interoperability Part 1, §2.2.3.1, Indicator IPv4 Address",
    "created_by_ref": "Identity::f431fe90-377b-45e0-a12c-3a4751ae6f09",
    "created": "2018-01-17T11:11:13.002Z",
    "modified": "2018-01-17T11:11:13.002Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "labels": ["malicious-activity"],
    "pattern": "[ipv4-addr: value = '198.51.50.1']"
  }
]
```

The Object Referral Test we could add to Part 2

[Given example of a time-based look-ups]
We intend to do that as a part of a future Part 3

I could see us proposing a change in this Spec to ‘Collection’

Question 3

• Question #3: Based on answer to Q2 how should be test in interop identity of intelligence providers?

  • Choice A: As is currently done. No changes required.
  • Choice B: Remove identity and separate into its own bundle and update all tests to reflect changes.
  • Choice C: Remove identity from most tests and add a separate test around identity of intel provider as a specific test area and make it mandatory/optional per persona
  • Choice D: Change all tests to refer to collections instead of bundles but keep the test case including identity with the intel
[Took a Poll on the Call – Unanimous on Choice #D]
I’ll write this up for the rest of the Community

Drew

[Brought up the API Root issue]

Allan

The right place to discuss it is on the Tue call
So, I think we’ve finished what we have on for today – Thanks for joining us

Meeting Terminated

*******************************************************************************