STIX TAXII 2 & Beyond

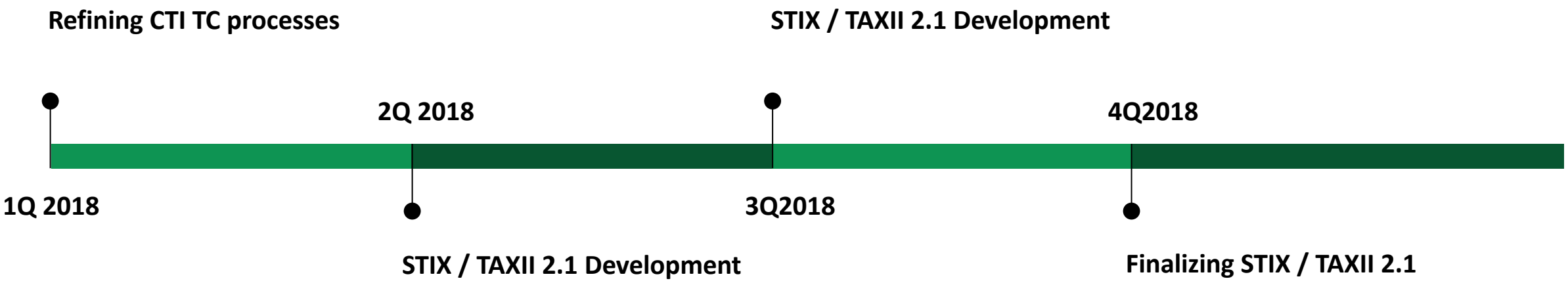
June 2018

Beyond Introduction

- Roadmap
- STIX Data Model Changes
- TAXII Changes
- STIXPreferred Changes

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Current Timeline



Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

STIX 2.1 and Beyond

New Feature: Confidence

- A new, optional property on all STIX Domain Objects.
- Definition: The **confidence** property identifies the confidence that the creator has in the correctness of their data. The confidence value **MUST** be a number in the range of 0-100.
- Examples
  - An Indicator with a **confidence** value of 100 = high confidence that the indicator pattern detects the malicious activity that it claims to
  - A Campaign with a **confidence** value of 50 = medium confidence that the campaign is made up of a related set of adversarial behaviors
- STIX 2.1 includes a standard set of mappings between existing confidence scales and STIX confidence values (including range)
  - None/Low/Medium/High
  - 0-10 scale
  - Admiralty Credibility
  - Words of Estimative Probability (WEP)
  - DNI Scale

WEP	STIX Confidence Value	Range of Values
Impossible	0	0
Highly Unlikely/Almost Certainly Not	10	1-19
Unlikely/Probably Not	30	20-39

Example WEP Mappings

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

New Feature: Internationalization

- Multi-faceted goal:
  - Allow STIX content to be translatable into different languages so that you can have publishers creating content in several languages and third party translation services for STIX content.
  - Allow for the identification of which language specific STIX content is in.
- New optional **lang** property on all STIX SDOs: indicates what language the content is in.
  - For example: a campaign object could be published with a **lang** value of Japanese to indicate that the name, description, and other human text fields are in Japanese.
- New optional **lang** property in the granular-marking type: indicates that certain fields in the object are in a particular language.
  - For example: certain fields in an object are in English while others are in Japanese.
- New language-content object: provide additional languages (translations) for other STIX objects.
  - For example: one could publish a campaign in Japanese and then provide a language-content object with that same text in English.

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

New SDO: Location

A Location represents a geographic location. The location may be described as any, some or all of the following: region, civic address, or latitude and longitude.

Examples

- North America
- New York, USA
- 38.833882, -104.821363

Relationships

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

New SDO: Note

A Note is a comment or note containing informative text to help explain the context of one or more STIX Objects or to provide additional analysis that is not contained in the original object.

Examples

- A Note indicating the steps used by an analyst to investigate a particular Campaign
- A Note stating that a particular Indicator was automatically generated by a malware sandbox

Relationships

- N/A – there are no top-level relationships between the Note Object and other Objects.
- Instead, the Note Object has an embedded relationship that can point to any STIX Object (including other relationships).

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

New SDO: Opinion

An Opinion is an assessment of the correctness of the information in another STIX Object.

Examples

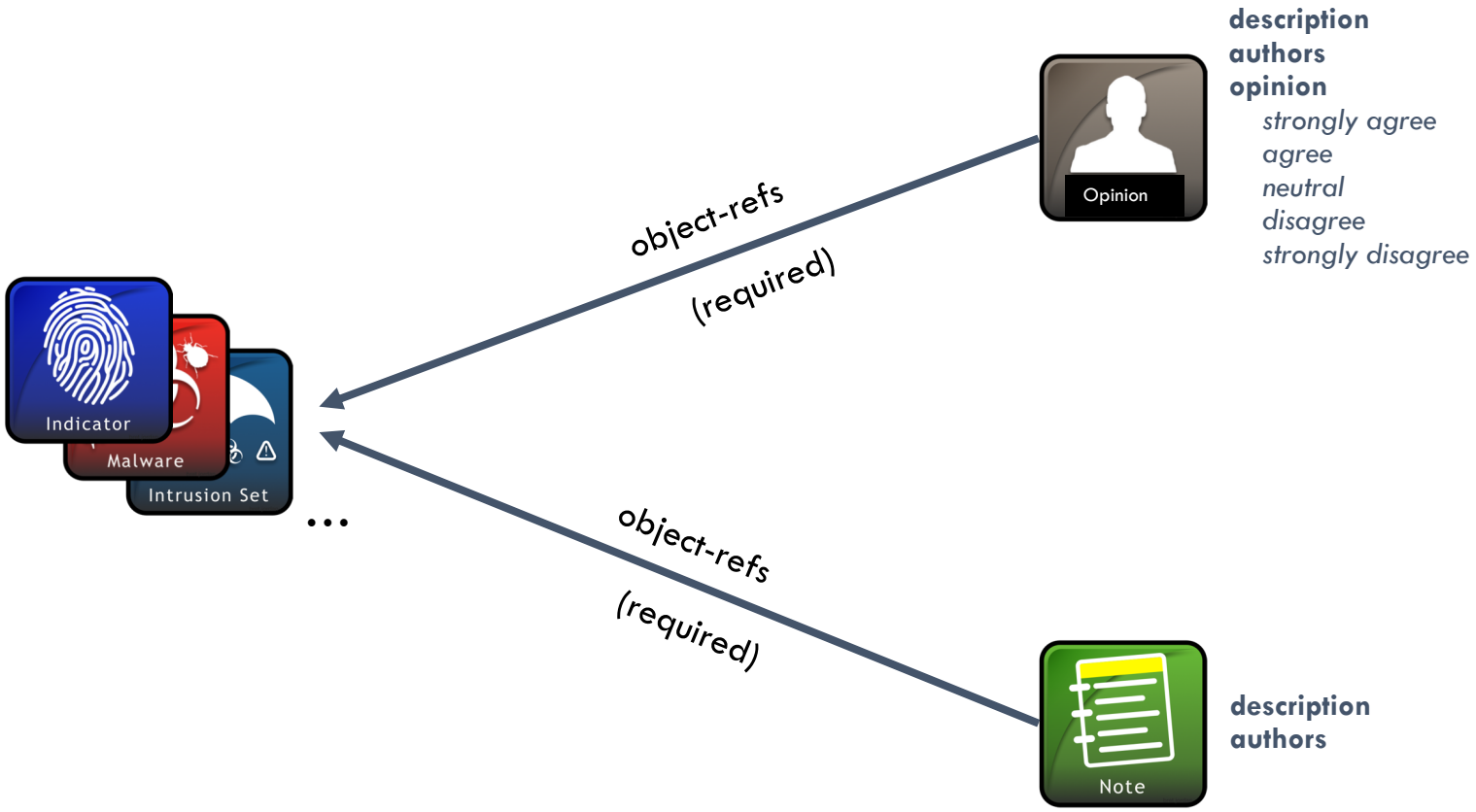
- An Opinion about Indicator Foo, stating that it does not detect what it claims to
- An Opinion about Campaign Bar, stating that it was based on false assumptions

Relationships

- N/A – there are no top-level relationships between the Opinion Object and other Objects.
- Instead, the Opinion Object has an embedded relationship that can point to any STIX Object (including other relationships).

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Using Opinions and Notes



Opinion

- MITRE "strongly disagrees" with that indicator
- MITRE "agrees" with that indicator

Note

- MITRE believes that the behavior this indicator detects is being seen in the energy sector in addition to the finance sector

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Updated SDO: Malware

Malware characterizes Malware Instances or Malware Families, including identifying information, metadata, and data that may be derived from various forms of malware analysis.

- The STIX 2.0, the Malware SDO was a stub that could only capture malware names
- For STIX 2.1 the Malware SDO has been updated to natively capture:
  - Sample metadata (e.g., file hashes, etc.)
  - Field data (first seen/last seen)
  - Execution & Implementation metadata
  - Static analysis results
  - Dynamic analysis (i.e., sandboxing) results
  - AV classification results
  - High-level capabilities (e.g.,
- In addition, the STIX 2.1 Malware SDO allows for the differentiation of Malware Instances and Malware Families

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

TAXII 2.1 and Beyond

What's New and Planned

- Additional Endpoints
- Pagination
- Query
- TAXII Channels

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Versions by Object ID

- Get a list of versions for an object

- Example: https://ts01.example.com/api1/collections/91a7b528-80eb-42ed-a74d-c6fbd5a26116/objects/indicator--252c7c11-daf2-42bd-843b-be65edca9f61/versions/

- URL Filtering Parameters

```
- added_after  - a timestamp              (e.g., ?added_after=...)
- version      - the version of an object (e.g., ?match[version]=...)
```

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Versions by Object ID

- GET Resource Response

```
HTTP/1.1 200 OK
Content-Type: application/taxii+json;version=2.1
X-TAXII-Date-Added-First: 2018-05-12T03:05:09.15811Z
X-TAXII-Date-Added-Last: 2018-05-12T03:05:17.275544Z

{
  "versions": [
    "2016-11-03T12:30:59.000Z",
    "2016-11-03T12:31:00.000Z”
  ]
}
```

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Delete an Object

- TAXII 2 needs the ability for a client to tell a server to remove an object from a Collection

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Pagination

- TAXII 2.0 “item” based pagination
- This proved to not work
- Item based pagination was removed for TAXII 2.1
- Investigating alternative solutions

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Query

- Phase 1
  - Find indicators that match this observation
  - Find observations that match this indicator pattern
  - Find relationships to or from this object ID
  - Automatically dereference embedded object references

- Phase 2
  - Find objects with a defined combination of property values
  - Graph traversal, return if these two objects are related

OASIS

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Channels

- Enable Publish / Subscribe
- Allow services to listen for and emit results
- Enable new workflows
  - Analyst to analyst
  - Machine to machine

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

STIXPreferred Future Challenges

Training Module #5

Module #5: Future Challenges

- Things that you will learn…
  - How will STIX 2.0 and STIX 2.1+ products be tested for interoperability
  - What future tests will be added to STIXPreferred
  - The meaning of life…

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Future STIXPreferred Testing - TAXII (2 Examples)

- TAXII 2.0 vs TAXII 2.1 interoperability
  - TAXII 2.1 has introduced a new mechanism for discovery that is not compatible with TAXII 2.0 clients
    - We will verify that clients and servers both advertise the versions they support correctly and are able to detect incompatible combinations

- Filters and paging
  - A substantial feature that many systems require when handling large scale distribution of intelligence
  - Verify that both servers and clients are able to handle larger scale publication and distribution of intelligence

OASIS

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Future STIXPreferred Testing - STIX (3 Examples)

- Malware
  - Has been substantially revised in STIX2.1 and the new schema supports many different use cases including sandboxing output sharing; malware repository collaboration environment
    - Tests will introduce higher level tests for technologies that are connected to sandboxes or leverage malware repositories to query information or post information on malware

- Campaigns, attack-patterns, intrusion-sets, actors, ttps and beyond…
  - STIXPreferred will introduce tests to verify the tradecraft of intelligence used across analyst teams beyond simple intelligence constructs (e.g. indicators)

- (More) Advanced Patterning
  - Verification of patterning has focused on simple use of pattern grammar
  - More sophisticated patterns useful for forensic analysis, combinatorial logic across both network and host based systems is necessary

OASIS

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Module #5: Checking In

Q1: Name one item that will be verified between a STIX/TAXII v2.0 system running against a STIX/TAXII v2.1 system?

Q2: Name one STIX SDO introduced in STIX2.1 that did not exist in STIX 2.0?

Q3: Where can interested parties learn more about STIXPreferred and STIX/TAXII v2 Interoperability on the Internet?

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Learn More…

- …on standards: **OASIS**
  - Membership https://www.oasis-open.org/
  - Events https://www.oasis-open.org/events/calendar

- …on CTI Interoperability: **STIX/TAXIIv2 Interoperability Subcommittee**
  - https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti-interoperability

- …on CTI: **STIX/TAXII Subcommittee**
  - https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Thank You