STIXPreferred Training

June 2018

Training Introduction

- Training Module #1: Key Concepts & Objectives
- Training Module #2: Interoperability Setup
- Training Module #3: Data Sharing
- Training Module #4: Intelligence Collaboration
- Training Module #5: Future Challenges

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

Training Module #1

Key Concepts & Objectives

Module #1: Key Concepts & Objectives

- Things that you will learn…
  - Understanding the rationale and justification why Interoperability certifications are important
  - Understand and explain what is STIXPreferred
  - Understand and explain what are STIXPreferred Persona
  - Understand and explain how STIXPreferred tests are organized and performed

OASIS

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

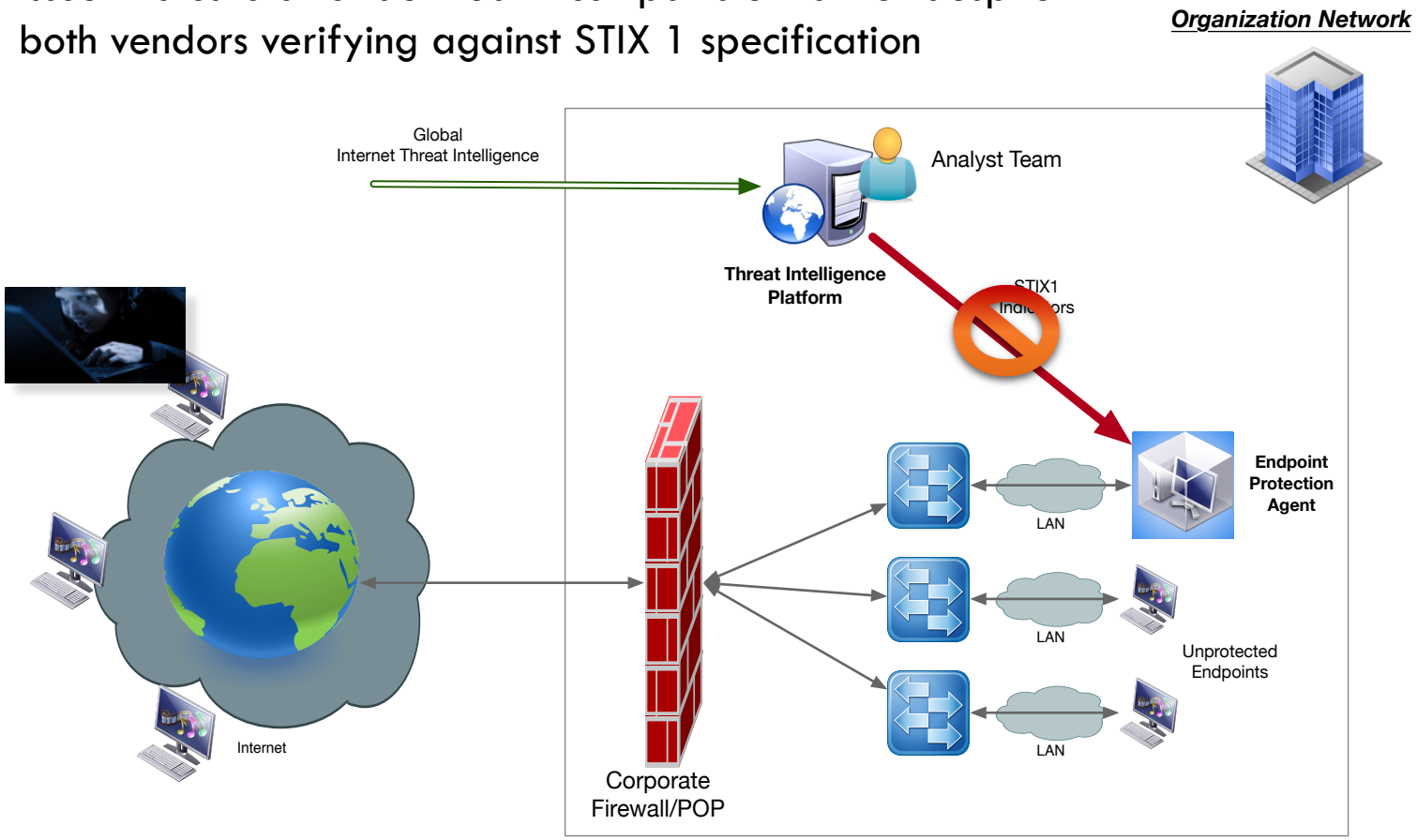
Interoperability and why it matters…

- Effective Cyber Defense requires
  - Multiple Systems
    - Typically different vendors
  - Different Functions & Tasks
  - Coordinated Actions
  - Easy Plug & Play

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

Too Often The Reality…

Issue: Indicators not defined in compatible manner despite both vendors verifying against STIX 1 specification



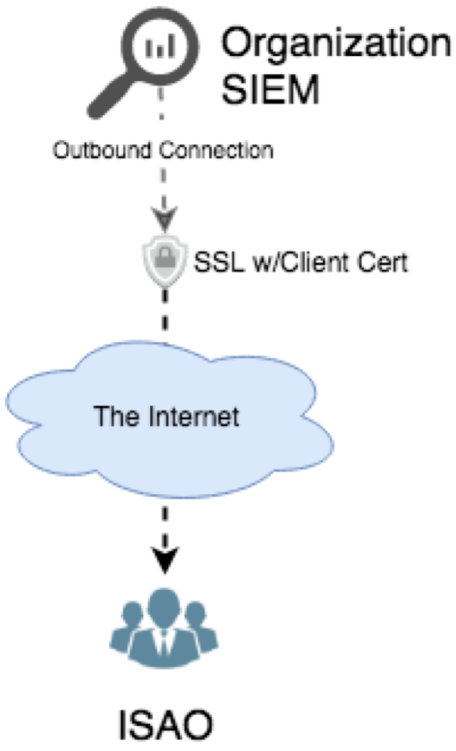
- **Organization: Large Multinational Media Company**
  - 10000s of Windows endpoints
  - Mature Security Analysis and Operations Team
- **Vendor A: Threat Intelligence Platform**
  - Aggregates global Internet Threat Intelligence feeds
  - Claims support of STIX Version 1 Indicators
- **Vendor B: Endpoint Protection Agent**
  - Inspects for malware, correlates against global Indicators
  - Claims support of STIX Version 1 Indicators

Result: Organization failed to debug problem, both vendors support/engineering teams involved

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

Too Often The Reality #2…

Issue: SIEM unable to connect to ISAO to receive indicators; both vendors verifying against STIX 1 specification



Result: Organization failed to debug problem, both vendors support/engineering teams involved

- **Organization: Large financial services organization**
  - Fortune 100 enterprise, tens of thousands of employees
  - SIEM consumes upwards of 1-2M EPS daily
- **Vendor A: SIEM Platform**
  - Consumes threat intelligence indicators to watch for them in logs, flows, and other data
  - Claims support of STIX 1 Indicators
- **Vendor B: Large ISAO with TAXII service**
  - Thousands of clients around the globe
  - Provides TAXII feed service based on commercial offering
  - Claims support of STIX 1 Indicators

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

Lack Of Interoperability Has Organizational Impact

- Expertise & Human Resources
  - To understand technically what is working
- Time & Costs
  - Multiple days/weeks to make it 'work'
  - Multiple orgs involved
- Lack of Capability
  - Unexpected results
  - Undermines protection
- Result is … Adversaries WIN

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

STIX TAXII 2 Preferred Certification

"Vendors want to proclaim some notion of us [the CTI TC] endorsing their support for STIX."

"We want to be able to say 'we support STIX' and have some kind of weight behind that."

"Evidence shows the market **does** care; otherwise, we wouldn't be getting these continual requests for endorsement."

"We want to allow vendors to very simply indicate, 'we have submitted an interoperability test, and you can find it registered on the CTI website.'"

"Self-certification is more than sufficient for what we need now."

- OASIS STIX/TAXIIv2 Self Certification Program
- Increase interoperability of cyber industry products
- Increase quality and success of CTI Collaboration

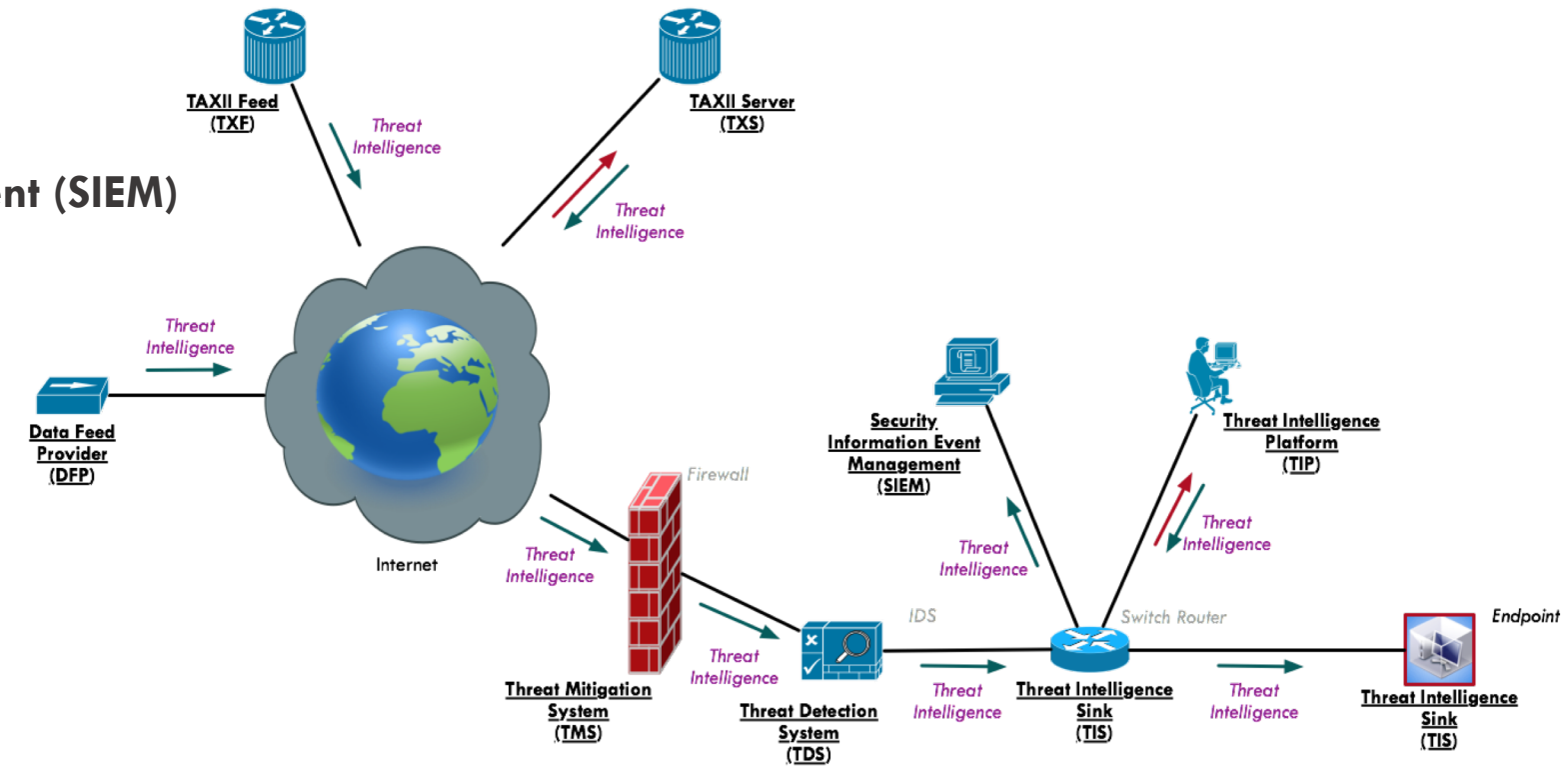
STIX2 PREFERRED

STIX2 TAXII 2 PREFERRED

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

STIX TAXII 2 Preferred - Persona

- Data Feed Provider (DFP)
- Threat Intelligence Platform (TIP)
- Security Incident and Event Management (SIEM)
- TAXII Server (TXS)
- TAXII Feed (TXF)
- Threat Mitigation System (TMS)
- Threat Detection System (TDS)
- Threat Intelligence Sink (TIS)



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

Part 1: Persona Definitions #1

- **Data Feed Provider (DFP)**
  - Software instance that acts as a producer of STIX 2.0 content.

- **Threat Intelligence Platform (TIP)**
  - Software instance that acts as a Producer and/or Respondent of STIX 2.0 content primarily used to aggregate, refine and share intelligence with other machines or security personnel operating other security infrastructure.

- **Security Incident and Event Management system (SIEM)**
  - Software instance that acts as a producer and/or Respondent of STIX 2.0 content. A SIEM that produces STIX content will typically create incidents and indicators. A SIEM that consumes STIX content will typically consume sightings, indicators.

OASIS

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

Part 1: Persona Definitions #2

- **Threat Mitigation System (TMS)**
  - Software instance that acts on courses of action and other threat mitigations such as a firewall or IPS, Endpoint Detection and Response (EDR) software, etc.

- **Threat Detection System (TDS)**
  - Software instance of any network product that monitors, detects and alerts such as Intrusion Detection Software (IDS), Endpoint Detection and Response (EDR) software, web proxy, etc.

- **Threat Intelligence Sink (TIS)**
  - Software instance that consumes STIX 2.0 content in order to perform translations to domain specific formats consumable by enforcement and/or detection systems that do not natively support STIX 2.0.

OASIS

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

Interoperability Certification Tests Organization

- **STIX Sharing (independent of TAXII) Tests – Part 1 Interoperability**
- **STIX over TAXII Sharing - Part 2 Interoperability**
- Each part defines
  - 1) A set of tests to performed and data
  - 2) A set of expected results & behaviors
  - 3) Checklists define mandatory and optional tests for each persona

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

Interoperability Certification Part 1 Focus

Description	Producer Personas	Respondent Personas
Indicator Sharing	DFP, TIP	TMS, TIS, TDS, TIP, SIEM
Sightings Sharing	DFP, TIP, TMS, TDS	TIP, SIEM
Versioning	All	All
Data Markings	All	All
Custom Objects & Properties	All	All
Course of Action Sharing	DFP, TIP	TIP, TMS, TIS, TDS

OASIS

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

Interoperability Test Component #1: Data

- Each part defines
  - A set of tests to performed and data for producer and consumer

To TXS	From TXS

POST
/api1/collections/91a7b528-80eb-42ed-a74d-bd5a2116/objects/ HTTP/1.1
Host: 10.1.1.10
Accept: application/vnd.oasis.taxii+json; version=2.0
Authorization: Basic dGVzdDoxMjPCow==
Content-Type: application/vnd.oasis.stix+json; version=2.0
 	
{
"type": "content from test table below...",
}
	HTTP/1.1 202 Accepted
	Content-Type: application/vnd.oasis.taxii+json; version=2.0
	
	{
	"id": "2d086da7-4bdc-4f91-900e-d77486753710",
	"status": "complete",
	"request_timestamp": "2016-11-02T12:34:34.12345Z",
	"total_count": 4,
	"success_count": 4,
	"successes": [
	"List of objects defined in the Part1 bundle test cases"
	],
	"failure_count": 0,
	"pending_count": 0
	}

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

Interoperability Test Component #2: Behavior

- A set of expected results & behaviors

Setup B Behavior - Read-Write Collection

1. Producer does a get on the Read-Write collection `https://10.1.1.10/api1/collections/91a7b528-80eb-42ed-a74d-bd5a2118`
2. Verify at the Producer that the TXS responds with the following information:
   a. **HTTP Response Code** is 200 OK
   b. **id** is `91a7b528-80eb-42ed-a74d-bd5a2118`
   c. **title** is "Read-Write Collection 1"
   d. **description** is "This is Read-Write Collection 1"
   e. **can_read** is true
   f. **can_write** is true
   g. **media_types** is `"application/vnd.oasis.stix+json; version=2.0"`
3. For each section described in Part1: Indicator Sharing Producer Test Cases the Producer will allow an analyst to create an Indicator in the user interface of Producer product and then publish the content to the TXS at `https://10.1.1.10/api1/collections/91a7b528-80eb-42ed-a74d-bd5a2118/objects` where the TXS component will not respond to the post until all objects within the bundle have been processed
4. Verify the TXS accepts the content by verifying the following on the Producer:
   a. **HTTP Response code** is 202 Accepted
   b. **id** represents a unique identifier for each post
   c. **status** is complete
   d. **request_timestamp** represents the time of the post
   e. **total_count** represents the number of objects in the bundle test case
   f. **success_count** is the same as total_count
   g. **successes** is an array of the object identifiers in the submitted bundle and matches the identifiers posted for each indicator
   h. **failure_count** is 0
   i. **pending_count** is 0
5. Verify that the Producer shows that the content shared to the TXS is visually shown to the user that the content was accepted successfully by the TXS.

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

Interoperability Test Component #3: Checklists

- Checklists define mandatory and optional tests for each persona

Table 3.3.1 - Threat Intelligence Platform (TIP) Part 1 Test Verification List

Use Case	Test	Verification	Results
Indicator Sharing	Indicator IPv4 Address	Mandatory	<fill in>
Indicator Sharing	Indicator IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	Indicator with IPv6 Address	Optional	<if supported, fill in>
Indicator Sharing	Indicator with IPv6 Address CIDR	Optional	<if supported, fill in>
Indicator Sharing	Indicator FQDN	Mandatory	<fill in>
Indicator Sharing	Indicator URL	Mandatory	<fill in>
Indicator Sharing	Indicator URL or FQDN	Mandatory	<fill in>
Indicator Sharing	Indicator File hash with SHA256 or MD5 values	Mandatory	<fill in>
Sighting Sharing	Producer Test Case Data	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with IPv4 Address	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with IPv4 Address Matching CIDR	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with IPv6 Address Matching CIDR	Optional	<if supported, fill in>
Sighting Sharing	Sighting + Indicator with NO observed data	Mandatory	<fill in>

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

Part 2: Persona Definitions #3

- Persona introduced as part of Part 2 tests

- TAXII Feed (TXF)
  - Software instance that publishes STIX data as a read-only TAXII Server where respondents may receive the STIX data from the TXF.

- TAXII Server (TXS)
  - Software instance that acts as a TAXII Server enabling the sharing of STIX 2.0 content among producers and respondents.

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

Module #1: Checking In

- Q1: What is a persona?
- Q2: Name at least 3 persona and their roles?
- Q3: Name one objective for testing interoperability of CTI products?
- Q4: Can systems certify for STIXPreferred if they share STIXv2 content over Email?
- Q5: Are all tests in STIXPreferred persona SIEM mandatory?

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

Training Module #2

Interoperability Setup

Module #2: Interoperability Setup

- Things that you will learn…
  - What TAXII configurations are important for interoperability verification
  - What are important differences between TAXII server persona
  - What interoperability exists between STIX/TAXII v1 and v2

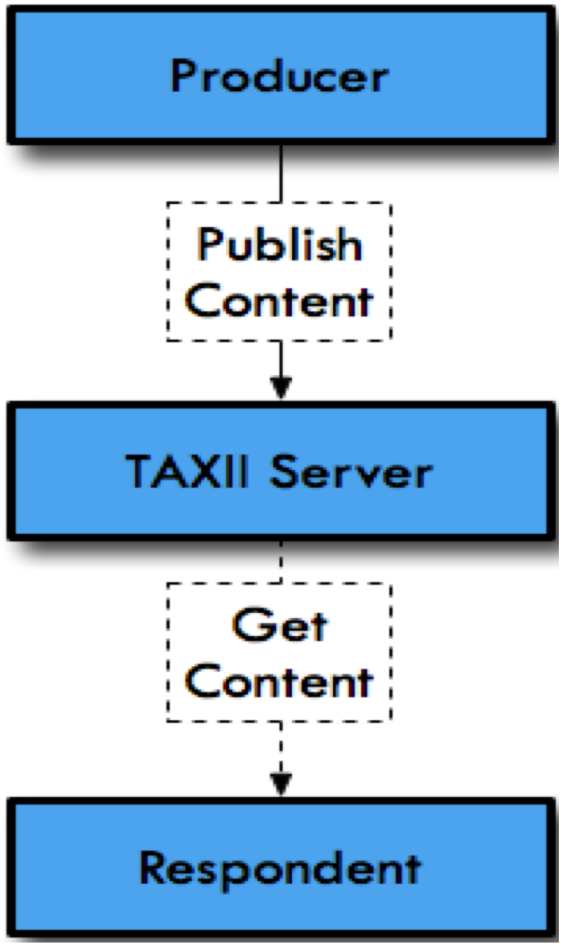
Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

TAXII Interoperability

- An organization's software product under test may implement multiple personas

- It is conceivable that a single software product instance supports
  - a TAXII Server
  - the producer
  - the respondent personas

- For Interoperability test case documents, each specific persona verification and expected behavior is called out separately.



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

TAXII Configuration Setup

- The following TAXII configuration parameters must be used
  - IP Address
  - HTTPS (not HTTP)
  - HTTP Basic Authentication (and associated credentials)

Connectivity consistency across components
- Secure transport
- Secure Authentication

- Server Information including
  - Name of server
  - Description
  - Contact
  - Default root
  - List of roots

Allows clients to learn about the server they connect to.
- Important for operational use
- API roots advertise where the data is

- API Root including
  - URL of root
  - Name of root
  - Description of root
  - Versions supported
  - Max Content supported

Identifies specific sharing communities
- Max content an important consideration for compatibility

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

TAXII Basic Connectivity Tests Covered

- Verify that all servers and clients can communicate on a basic level and handle errors

- Tests include:
  - Basic Get Request & Get Response
  - Basic API Get Request & Get Response
  - Missing Authorization Parameter Request & Response
  - Incorrect Authorization Parameter Request & Response
  - Incorrect API Root Info Get Returns Not Found Request & Response
  - Incorrect Collection Info Get Request & Response

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

TAXII Server Persona Differences

- There are 2 persona defined (see Module #1)
  - TXF: Read only server
  - TXS: Read write server

- Differences?
  - TXF only ever publishes intelligence
    - NO writes via TAXII endpoints

  - TXS allows producers to post intelligence and read intelligence

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

TAXII Collection Tests

- 3 Collection Setups
  - Setup A: Read Only Collection; Write Only Collection
  - Setup B: Read-Write Collection
  - Setup C: Read-Only Collection

Separate collections
- Unvetted data vs vetted data

Sharing Communities that allow publication and collaboration

Intelligence publication only

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

TAXII v1 & TAXII v2 Interoperability

- There is NO interoperability between STIX/TAXII version 1 & STIX/TAXII version 2
  - STIX/TAXII v1 is completely unrelated to STIX/TAXII v2

- A vendor can support TAXII v1 and TAXII v2 on the same product instance

- Be careful of clients and how they connect to TAXII v1 vs v2 endpoints

OASIS

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

Module #2: Checking In

Q1: What authentication method is verified for interop tests?

Q2: What error should be returned when an unauthenticated account is used to connect to a TAXII server?

Q3: Should all TAXII servers support collections that are both read and write?

Q4: Can an org support a TAXII server that has both TAXII v1 and TAXII v2 on the same system?

OASIS

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

Training Module #3

Data Sharing

Module #3: Data Sharing

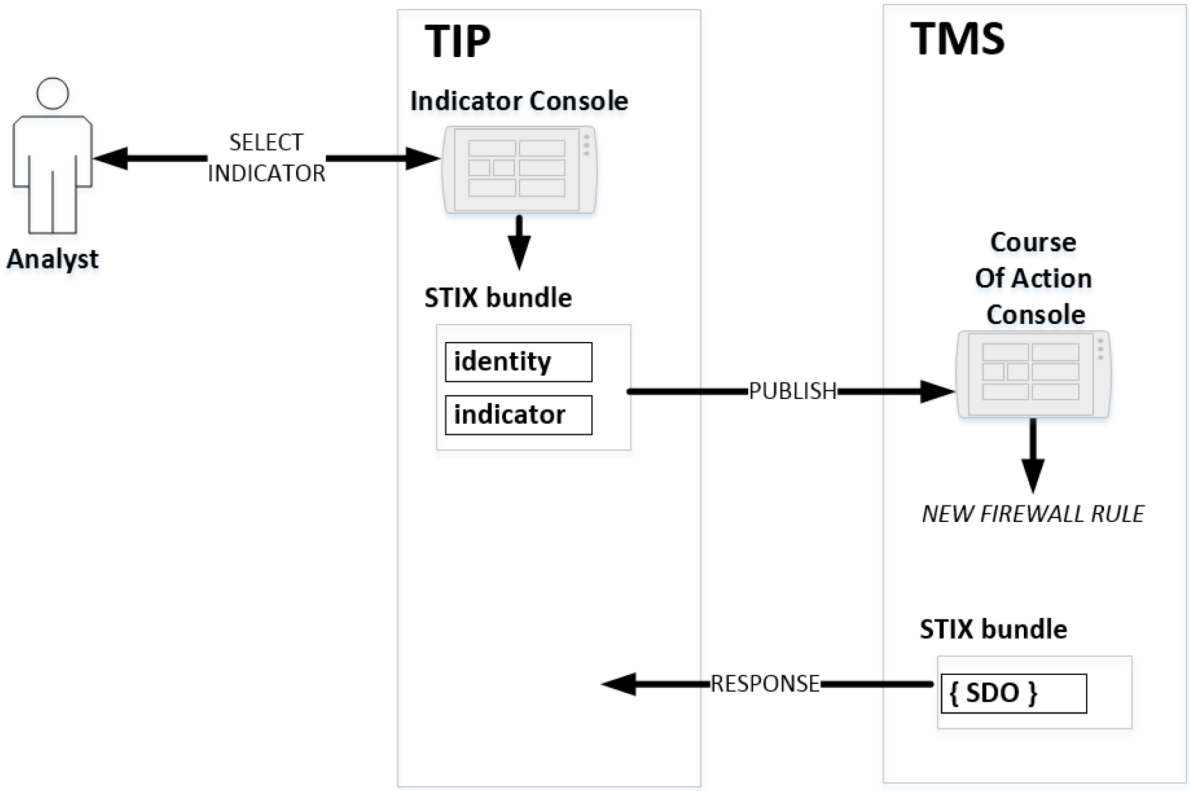
- Things that you will learn…
  - What are important considerations for **Indicator & sighting sharing** across a producer and a consumer
  - What are important considerations for **versioning intelligence** across a producer and a consumer
  - What are important considerations for **data marking on intelligence** across a producer and a consumer
  - What are important considerations for **customized intelligence** across a producer and a consumer

OASIS

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

Indicator Sharing Use Case

- Very common use case
- Producers define what threats to look for
  - Technical indicators can be IP; URLs; Domains; Hashes…etc
- Consumers act on those indications
- IMPORTANT Tests support for new STIX2pattern grammar basic support



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

Indicator Sharing – Verification

- Goal:
  - A) Verify how a producer (DFP & TIP) of Indicator intelligence generates the data correctly
  - B) Verify how a respondent (TIP; TMS; TDS; TIS) of Indicator intelligence correctly handles data not just parse it

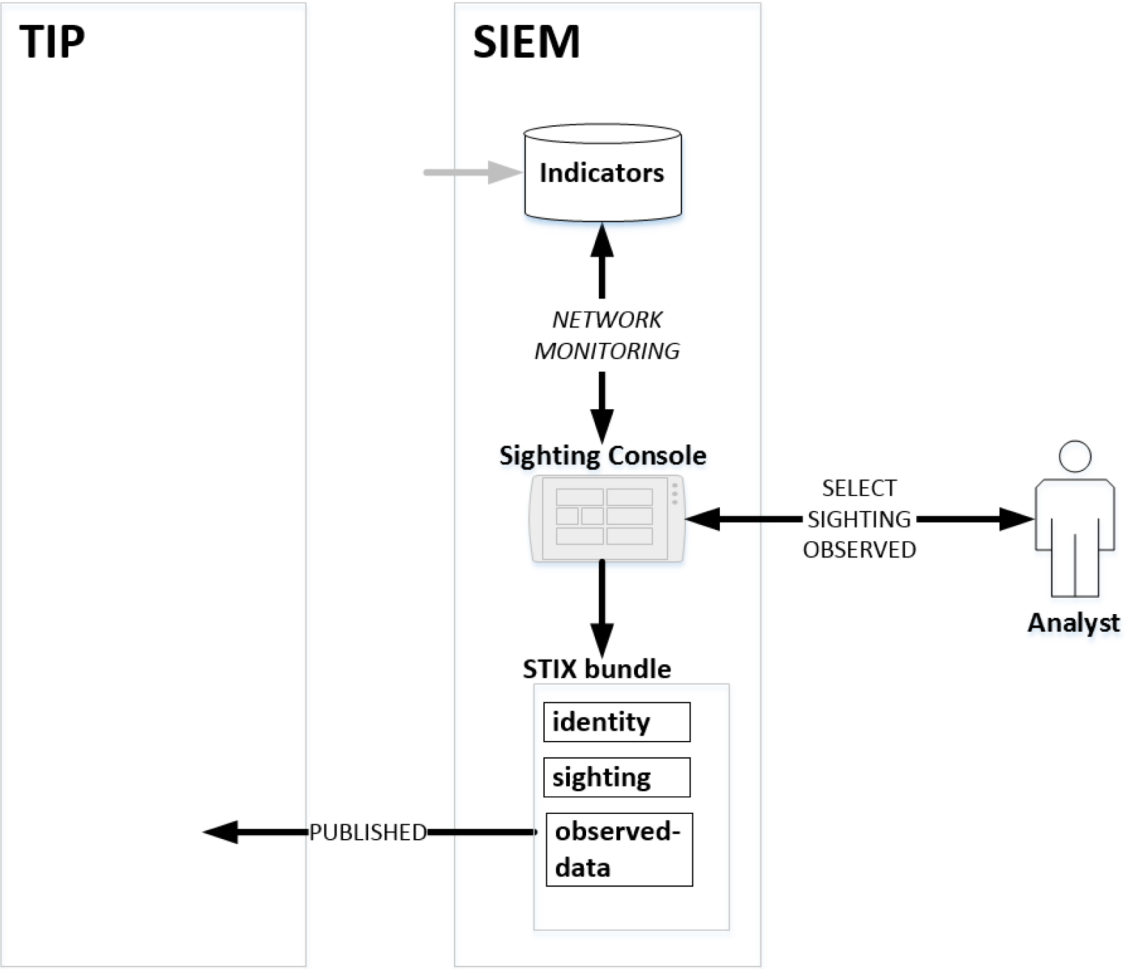
- Content verified:
  - Schema Version information
    - To ensure payload is correctly identifying the version of STIX being used
  - Created_by & Identity attribution
    - To ensure payload can be attributed to an intelligence source/org/team and respondent connects identity to intel
  - Created/Modified information
    - To ensure producer is publishing correct information for versioning of an object
  - Valid_from
    - To ensure producers are publishing dates that indicators are valid to consider
  - Pattern
    - To ensure the producer is able to construct correct patterns for common base indicators including: IP; FQDN; Hash; URL…etc INCLUDING simple combinatorial patterns

OASIS

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

Indicator & Sighting Sharing Use Case

- Very common use case
  - Builds on indicator sharing
- Producers define what threats were observed based on indicators previously shared
  - Sightings include which specific observed data matched which indicators
- Consumers act on those sightings
- IMPORTANT Tests support for new STIX2pattern grammar basic support



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

Sighting Sharing – Verification

- Goal:
  - A) Verify how a producer (DFP & TIP) of Indicator intelligence generates the data correctly (same as Indicator tests)
  - B) Verify how a respondent (SIEM; TIP; TMS; TDS; TIS) receives Indicator intelligence and is able to produce Sighting intelligence correct that matches those indicators

- Sighting & Observed_Data content verified:
  - Schema Version information
    - To ensure payload is correctly identifying the version of STIX being used
  - Created_by & Identity attribution
    - To ensure payload can be attributed to an intelligence source/org/team and respondent connects identity to intel
  - Created/Modified information
    - To ensure producer is publishing correct information for versioning of an object
  - First_seen; last_seen; first_observed; last_observed; number_observed
    - To ensure respondents are publishing dates & counts that sightings including observed_data were seen during
  - Sighting_of_ref
    - To ensure the respondent is connecting the indicator to the sighting correctly

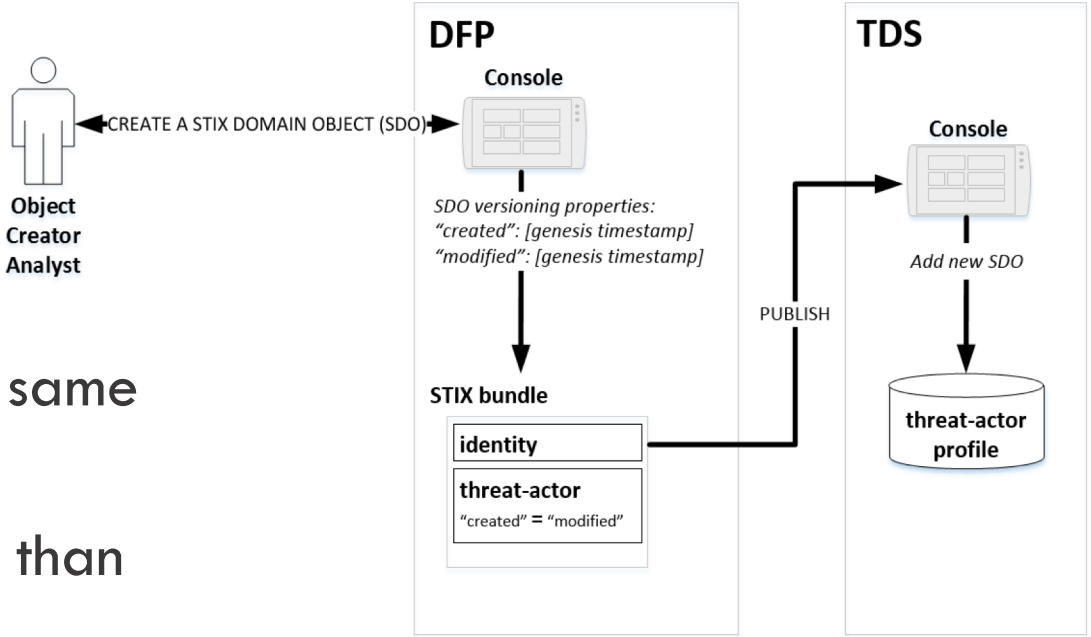
OASIS

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

Versioning Verification Use Case

- Required for all producers and respondents to handle versioning

- Verification on the use of
  - First time created objects
    - Checks that both created and modified are same
  - Modification to existing objects
    - Checks that modified is updated and newer than created
  - Revocation to existing objects
    - Checks that revoked is set and modified is updated

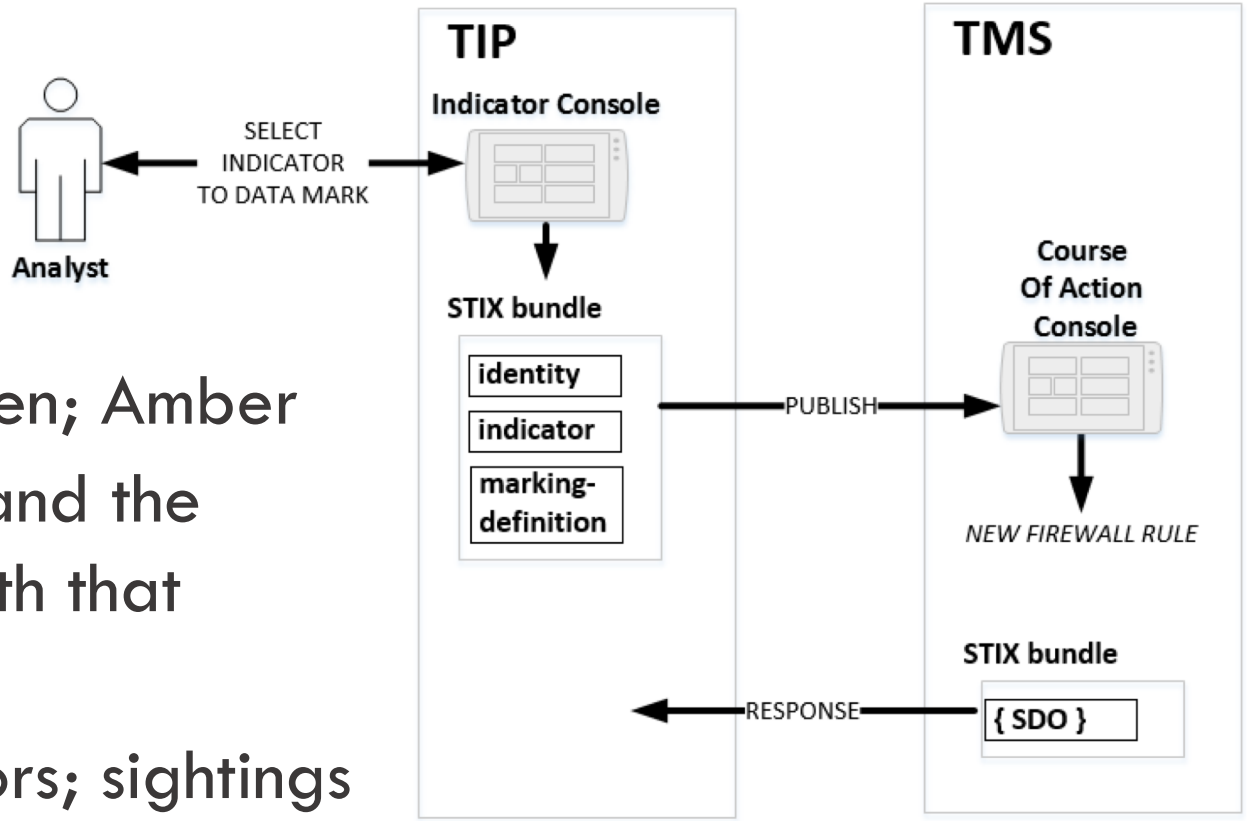


Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Data Marking Verification Use Case

- Required for all producers and respondents to handle data marking

- Verification on the use of
  - Creation of a marking object
    - Specifically TLP levels Red; Green; Amber
  - Reference to that marking object and the covered intelligence associated with that markings
  - Tests across intelligence of indicators; sightings



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

Customization Verification Use Case

- Required for all producers and respondents to handle custom objects and properties *without* crashing
  - There is no mandate for a respondent to act on the custom object beyond not crashing

- Verification on creation, modification of a custom objects and/or properties
  - Mandatory common properties are present and validated
  - Respondent handles the inclusion of custom objects in a bundle received from a producer without crashing

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

Module #3: Checking In

Q1: As a data feed provider, what are some of the verification steps to perform?

Q2: What must a producer of an intel object do before publishing a new version of an intel object they've previously published?

Q3: Is a consumer of an intel object allowed to modify or change an intel object from another provider?

Q4: What must be done to share related objects from one vendor vs original vendor?

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

OASIS

Training Module #4

Intelligence Collaboration

Module #4: Intelligence Collaboration

- Things that you will learn…
  - The basic requirements and verification steps for **setup and connect** to share intelligence via a TAXII 2.0 server
  - The requirements and verification for producers who create intelligence to **share as a feed** to other respondents and how the respondent should handle such data
  - The requirements and verification for **intelligence collaboration where teams create, modify and revoke intelligence** in a collaborative environment

OASIS

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

Data Sharing – Collection Verification Setups

- 3 Use Cases identified for TAXII exchange
  - Applied to both data and intelligence collaboration tests

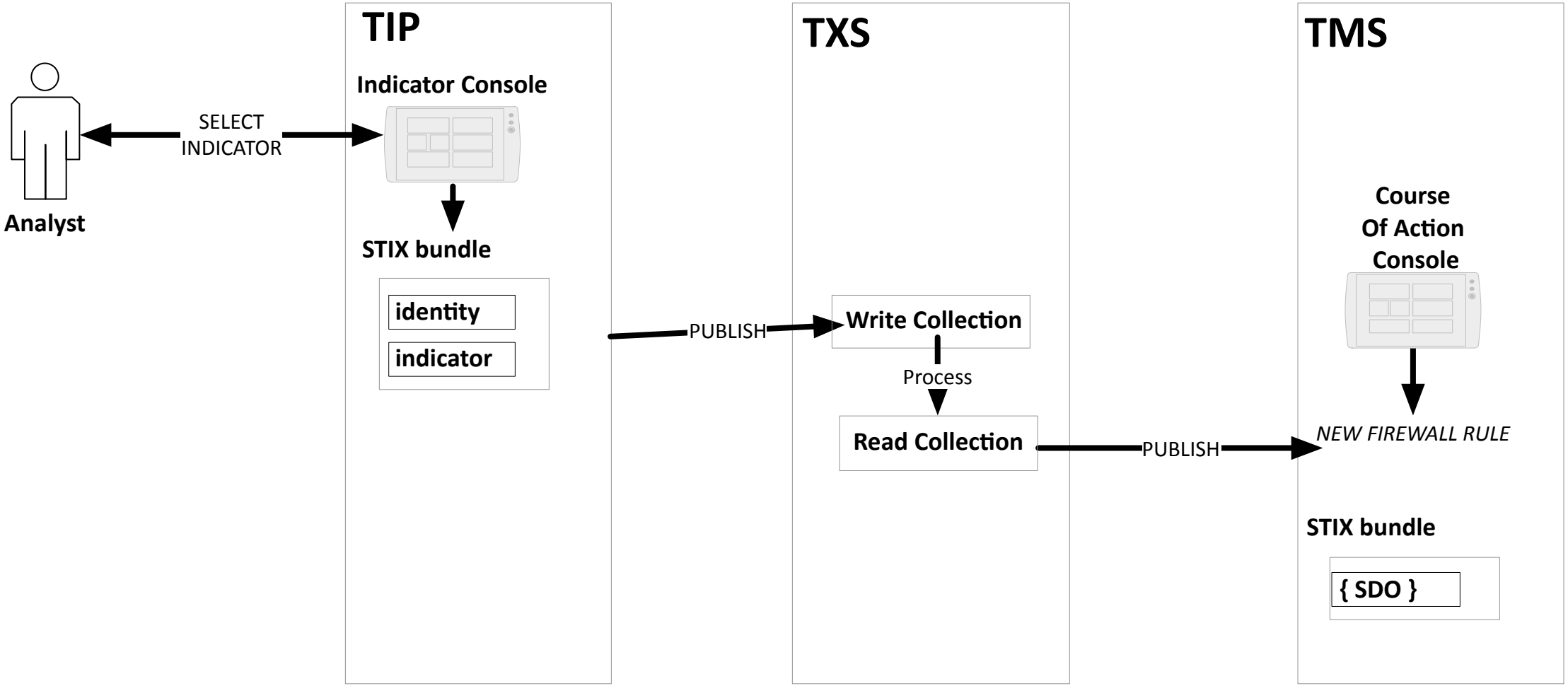
- **Setup A: Read & Write Separate Collections**
  - Supports providers that can post content to a product or community that verifies content before republishing the content to others

- **Setup B: Read & Write Same Collection**
  - Supports providers and respondents that publish and use intelligence without verification of the intelligence at the TAXII server

- **Setup C: Read Only Collection**
  - Supports providers that wish to publish content but do not allow any feedback on that published content or allow additional content to be pushed

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

Separate Read + Write Collection Setup



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

Producer – Separate Read & Write Collection Verification

- **Goal: Verify producers handle collection permissions and post data correctly**
  - Personas Tested: DFP, TIP, SIEM, (TXS)
  - Check #1: Able to check Write collection is available & allows write permissions with appropriate media
  - Check #2: Able to publish all Indicator sharing test cases
  - Check #3: Verify that all counts returned from TXS as expected
  - Check #4: Appropriate HTTP codes (success & error) are correct

OASIS

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

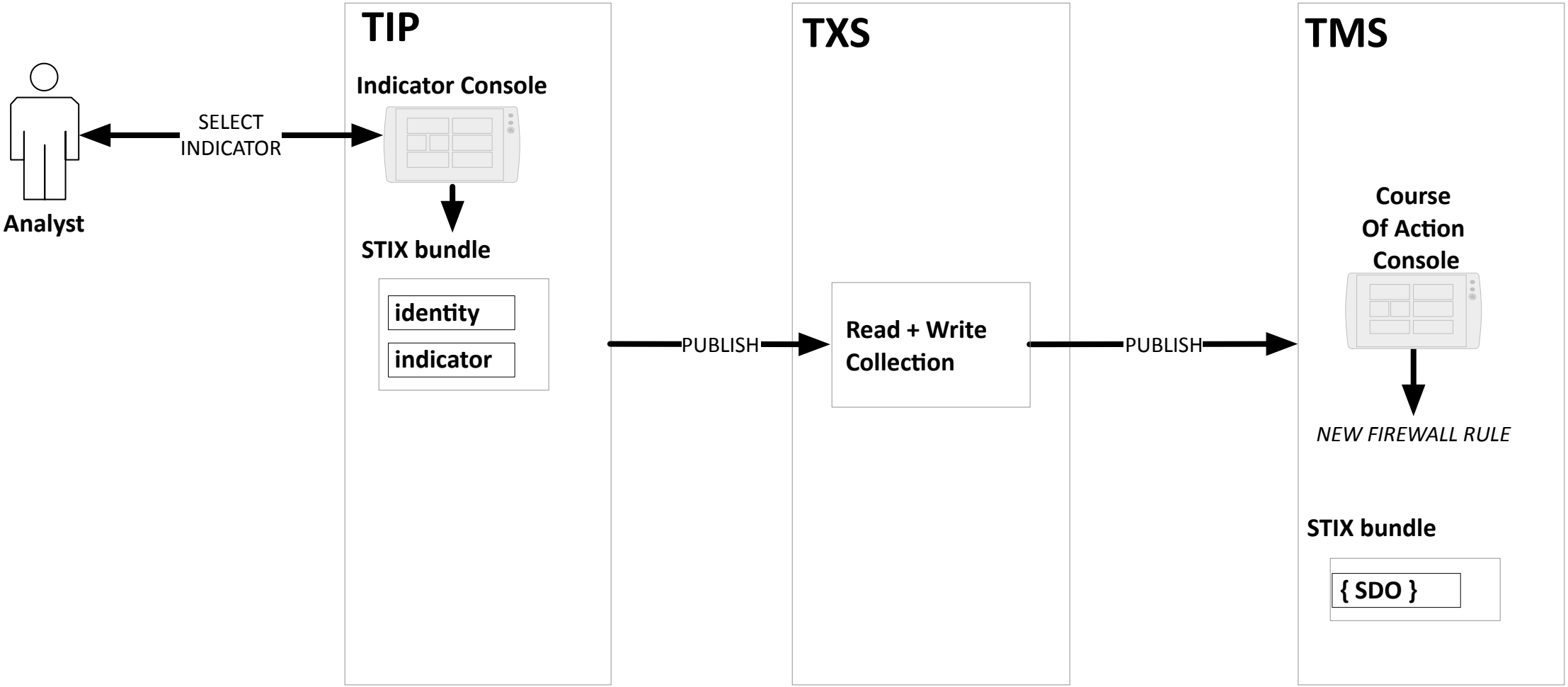
Respondent – Separate Read & Write Collection Verification

- **Goal: Verify respondents handle collection permissions and read data correctly**
  - Personas Tested: TIP, SIEM, TMS, TDS, TIS, (TXS)
  - Check #1: Able to check Read collection is available & allows read permissions with appropriate media
  - Check #2: Able to **read** all Indicator sharing test cases
  - Check #3: Verify that all data & counts returned from TXS as previously posted to Write Collection
  - Check #4: Appropriate HTTP codes (success & error) are correct

OASIS

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

Same Read + Write Collection Setup



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

Same Read & Write Collection Verification

- **Producer Goal:** Verify producers handle collection permissions and post data correctly **when collection has both read & write permissions**
  - Persona: DFP, TIP, SIEM

- **Respondent Goal:** Verify respondents handle collection permissions and read data correctly **when collection has both read & write permissions**
  - Persona: TIP, SIEM, TMS, TDS, TIS

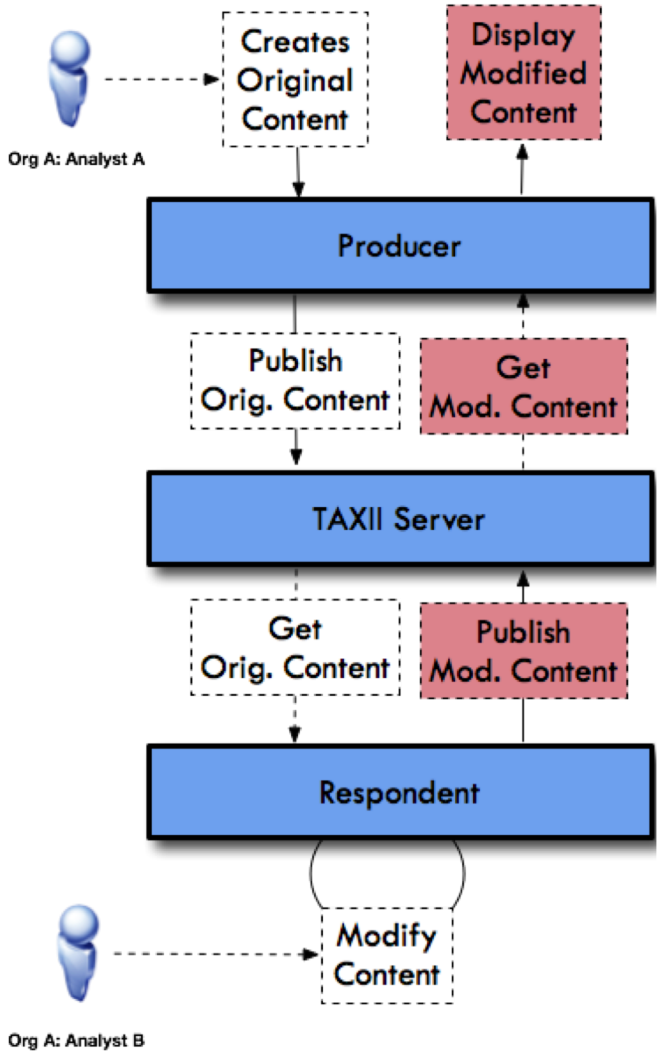
- Both producer and respondent checks are same as prior tests

OASIS

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

Intelligence Collaboration - Use Case #1

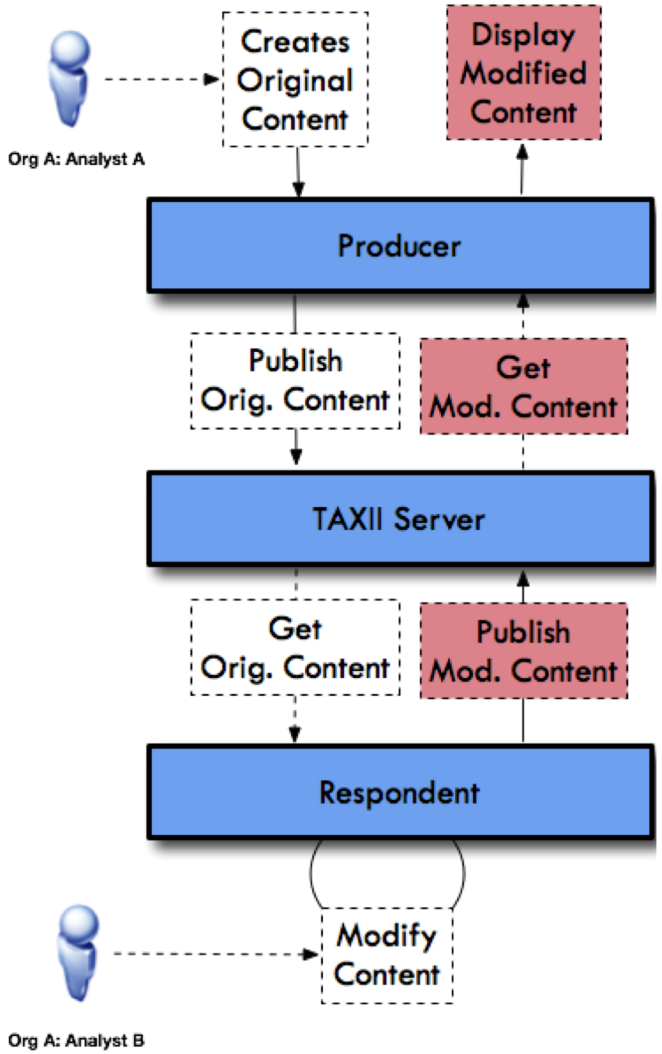
- **Same organization** sharing and modifying **common** intelligence between two analysts using two systems
  - First analyst creates an intelligence element that they wish to share with other analysts within the same organization
  - Second analyst receives the intelligence from the first analyst and then proceeds to modify the existing intelligence and reshares back to the first analyst



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

Verification Steps - Use Case #1

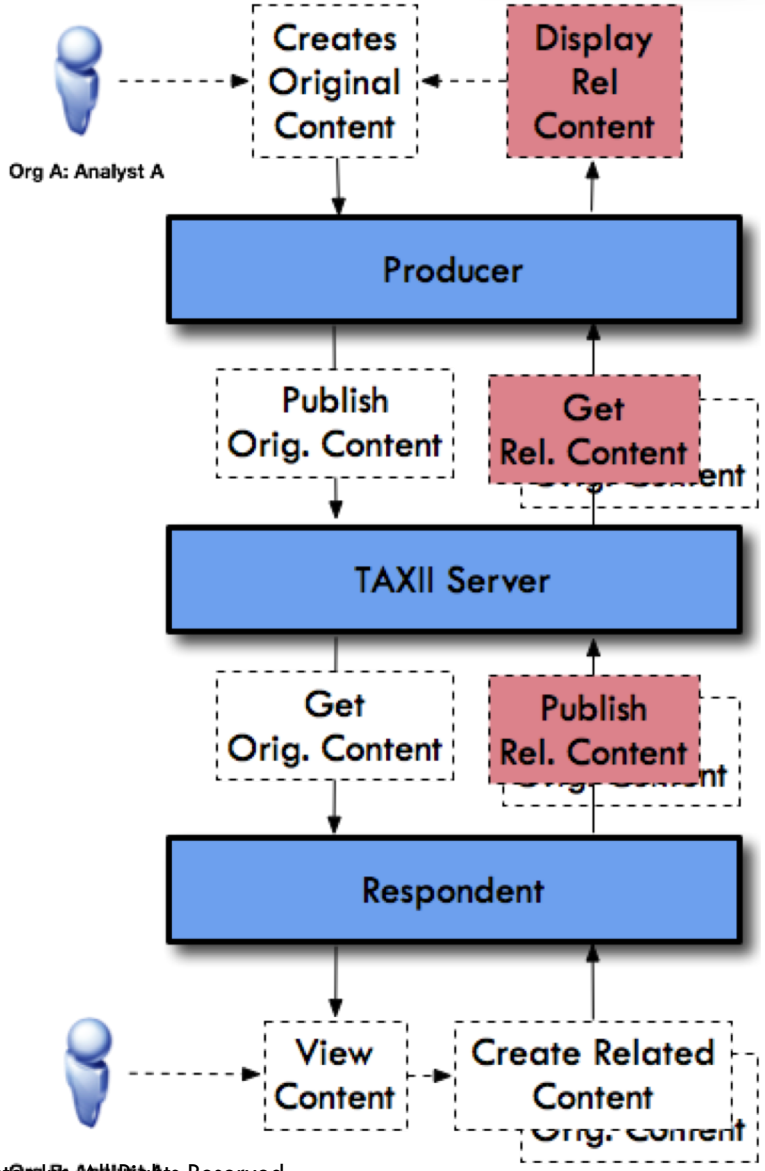
- Producer verification steps
  - Same as Indicator data sharing initially for creation tests
- Respondent verification steps
  - Checks that the intelligence is modified correctly and republishes via TXS back to original producer
- Producer verification steps
  - Is able to handle the updated intelligence received from the respondent and correctly handles the updates to the intel objects the producer had originally had produced back into its systems



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

Intelligence Collaboration Verification – Use Case #2

- **Different organizations** sharing and modifying **related** intelligence between two analysts using two systems
  - First analyst creates an intelligence element that they wish to share with another set of analysts in a sharing community
    - The other analysts in this sharing community belong to different organizations
  - Second analyst receives the intelligence from the first analyst and then proceeds to find some new content that they believe is related to the original intelligence
    - They proceed to then share the new intelligence back to the sharing community, including the relationship that connects the intelligence together



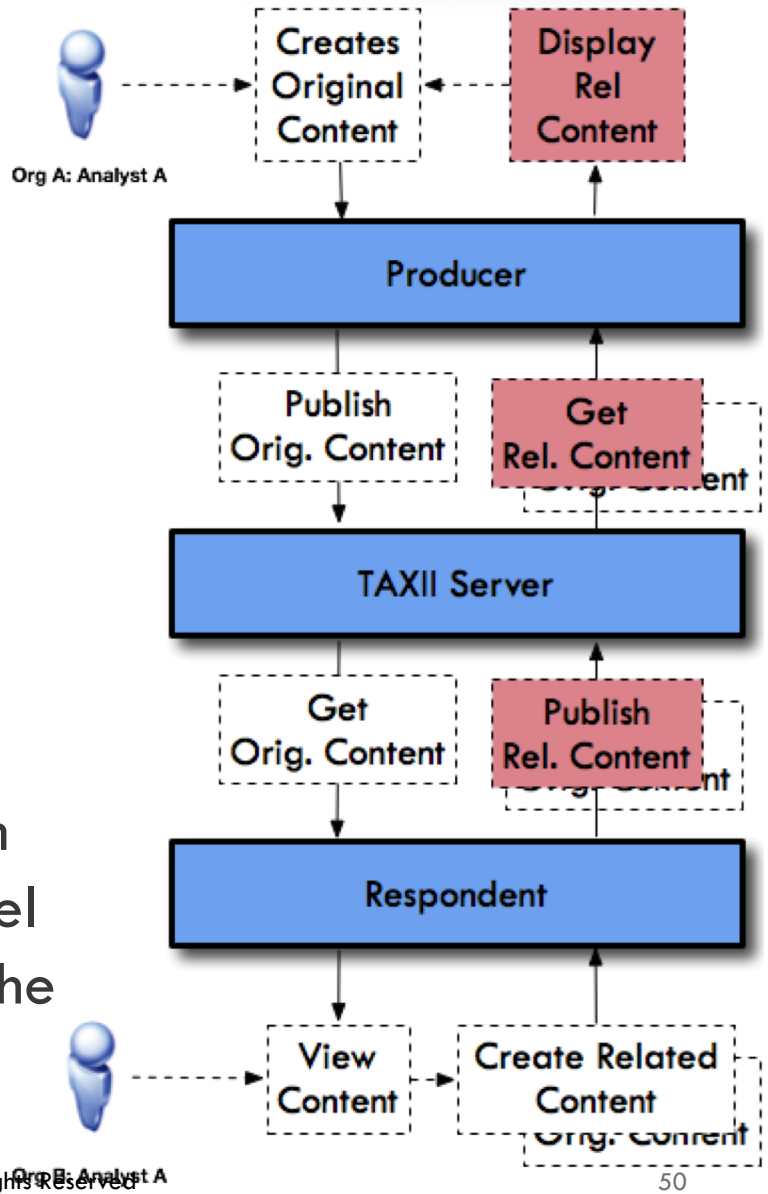
Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Verification Steps – Use Case #2

- Producer verification steps
  - Same as Indicator data sharing initially for creation tests

- Respondent verification steps
  - Checks that the intelligence is created (and not modified) correctly including relationships constructed correctly and republishes via TXS back to original producer

- Producer verification steps
  - Is able to handle the new related intelligence received from the respondent and correctly handles the updates to the intel objects that have been related by the respondent back to the producer had originally had produced back into its systems



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

Intelligence Collaboration Verification – Use Case #3

- **Analysts/Groups within the same organization** sharing and modifying **related** intelligence between two analysts using two systems where the analyst has their own **created_by** identity
  - These analysts/groups would serve different missions within the same organization
  - First analyst creates an intelligence element that they wish to share with another set of analysts in a sharing community within the same organization. Additionally, the organization wants to track each individual analyst's contributions
  - Second analyst receives the intelligence from the first analyst and then proceeds to find some new content that they believe is related to the original intelligence. They proceed to share the new related content back to the sharing community, including the relationship that connects the intelligence together

OASIS

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

Module #4: Checking In

Q1: Name one aspect that is verified differently for Separate Read & Write collections vs Same Read-Write collection test cases?

Q2: Should a data feed provider certify their product for Intel Collaboration?

Q3: Name two collection setups that are verified as part of Intelligence Collaboration tests?

Q4: Name two of the 3 user-level scenarios that intel collaboration verifies? (Hint: Name both org and teams involved)

OASIS

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

Training Module #5

Future Challenges

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?

OASIS

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