OASIS Committee Note

STIX/TAXII™ 2.0 Interoperability Test Document: Part 2 Version 1.0

Committee Note 01

05 November 2018

Specification URIs

This version:

https://docs.oasis-open.org/cti/stix-taxii-2-interop-p2/v1.0/cn01/stix-taxii-2-interop-p2-v1.0-cn01.docx (Authoritative)

https://docs.oasis-open.org/cti/stix-taxii-2-interop-p2/v1.0/cn01/stix-taxii-2-interop-p2-v1.0-cn01.html

https://docs.oasis-open.org/cti/stix-taxii-2-interop-p2/v1.0/cn01/stix-taxii-2-interop-p2-v1.0-cn01.pdf

Previous version:

N/A

Latest version:

https://docs.oasis-open.org/cti/stix-taxii-2-interop-p2/v1.0/stix-taxii-2-interop-p2-v1.0.docx (Authoritative)

https://docs.oasis-open.org/cti/stix-taxii-2-interop-p2/v1.0/stix-taxii-2-interop-p2-v1.0.html

https://docs.oasis-open.org/cti/stix-taxii-2-interop-p2/v1.0/stix-taxii-2-interop-p2-v1.0.pdf

Technical Committee:

OASIS Cyber Threat Intelligence (CTI) TC

Chair:

Richard Struse (Richard.Struse@HQ.DHS.GOV), DHS Office of Cybersecurity and Communications (CS&C)

Editors:

Allan Thomson (athomson@lookingglasscyber.com), LookingGlass

Jason Keirstead (Jason.Keirstead@ca.ibm.com), IBM

Related work:

This document is related to:

- *STIX/TAXII™ 2.0 Interoperability Test Document: Part 1 Version 1.1*. Edited by Allan Thomson and Jason Keirstead. Latest version: https://docs.oasis-open.org/cti/stix-taxii-2-interop-p1/v1.1/stix-taxii-2-interop-p1-v1.1.html.
- *STIX™ Version 2.0. Part 1: STIX Core Concepts*. Edited by Rich Piazza, John Wunder, and Bret Jordan. Latest version: http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part1-stix-core.html.
- *STIX™ Version 2.0. Part 2: STIX Objects*. Edited by Rich Piazza, John Wunder, and Bret Jordan. Latest version: http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part2-stix-objects.html.
- *STIX™ Version 2.0. Part 3: Cyber Observable Core Concepts*. Edited by Ivan Kirillov and Trey Darley. Latest version: http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part3-cyber-observable-core.html.

- *STIX™ Version 2.0. Part 4: Cyber Observable Objects*. Edited by Ivan Kirillov and Trey Darley. Latest version: http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part4-cyber-observable-objects.html.
- *STIX™ Version 2.0. Part 5: STIX Patterning*. Edited by Ivan Kirillov and Trey Darley. Latest version: http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part5-stix-patterning.html.
- *TAXII™ Version 2.0.* Edited by John Wunder, Mark Davidson, and Bret Jordan. Latest version: http://docs.oasis-open.org/cti/taxii/v2.0/taxii-v2.0.html.

Abstract:

This is Part 2 of the Interoperability test documents which supplement the five-part Structured Threat Information Expression (STIX 2.0) and TAXII 2.0 specifications developed by the Cyber Threat Intelligence Technical Committee (CTI TC) of the Organization for the Advancement of Structured Information Standards (OASIS). This test document provides detailed requirements on how producers of products within the threat intelligence ecosystem may self-certify and demonstrate that their software is interoperable with other systems implementing STIX/TAXII 2.0.

There are eight personas detailed in this specification. These are: Data Feed Provider (DFP), Threat Intelligence Platform (TIP), Threat Mitigation System (TMS), Threat Detection System (TDS), Security Incident and Event Management (SIEM), Threat Intelligence Sink (TIS), TAXII Feed (TXF) and TAXII Server (TXS).

This Interoperability test document defines tests of the following test cases: common connection, basic data sharing, and basic threat intelligence collaboration. For each of these test cases the document defines what the Producer[1], TAXII Server and Respondent[2] need to support to satisfy each test case.

Status:

This is a Non-Standards Track Work Product. The patent provisions of the OASIS IPR Policy do not apply.

This document was last revised or approved by the OASIS Cyber Threat Intelligence (CTI) TC on the above date. The level of approval is also listed above. Check the "Latest version" location noted above for possible later revisions of this document.

Technical Committee (TC) members should send comments on this document to the TC's email list. Others should send comments to the TC's public comment list, after subscribing to it by following the instructions at the "Send A Comment" button on the TC's web page at https://www.oasis-open.org/committees/cti/.

Citation format:

When referencing this document the following citation format should be used:

[STIX-TAXII-Interop-p2-v1.0]

STIX/TAXII™ 2.0 Interoperability Test Document: Part 2 Version 1.0. Edited by Allan Thomson and Jason Keirstead. 05 November 2018. OASIS Committee Note 01. https://docs.oasis-open.org/cti/stix-taxii-2-interop-p2/v1.0/cn01/stix-taxii-2-interop-p2-v1.0-cn01.html. Latest version: https://docs.oasis-open.org/cti/stix-taxii-2-interop-p2/v1.0/stix-taxii-2-interop-p2-v1.0.html.

[1] Definition of this term may be found in Part 1 v1.1 Section 1.1 Terminology

[2] Definition of this term may be found in Part 1 v1.1 Section 1.1 Terminology

Notices

Table of Contents

1 Introduction

This document defines additional test cases and personas for STIX/TAXII 2.0 Interoperability Test Cases and is supplementary to Part 1 v1.1.

1.1 IPR Policy

This specification is provided under the Non-Assertion Mode of the OASIS IPR Policy, the mode chosen when the Technical Committee was established. For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC's web page (here).

1.2 Terminology

Please refer to Part 1 v1.1 Section 1.1 Terminology.

Within Part 2 the following amended definition of Respondent is used. Future revisions of Part 1 Terminology will be updated to reflect this change.

Respondent - A software instance that reads STIX 2.0 content and performs some action on that received data ***and may send data back to the original Producer to support the particular use case and exchange of intelligence between the systems***.

1.3 References

[RFC7230] Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing, June 2014

[RFC5246] The Transport Layer Security (TLS) Protocol Version 1.2, AUGUST 2008

[RFC7617] The 'Basic' HTTP Authentication Scheme, SEPTEMBER 2015

1.4 Overview

This document focuses on testing interoperability of software instances that support STIX and TAXII exchange. It leverages Part 1 v1.1 test cases, and augments them by adding a TAXII Server to facilitate the exchange of STIX bundled content detailed in Part 1 v1.1.

1.4.1 Part 2 Personas

The following system personas are used throughout this document.

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

- 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.
- TAXII Feed (`TXF`)
    - Software instance that publishes STIX content from a read-only TAXII Server where Respondents are only allowed to receive the STIX content 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.
- Threat Detection System (`TDS`)
    - Software instance of any network product that monitors and/or detects such as Intrusion Detection Software (IDS), Endpoint Detection and Response (EDR) software, web proxy, etc. A TDS will typically ingest STIX content and may emit events or reports that indicate the TDS has detected traffic or behaviors matching the STIX 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.
- 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. These consumers may or may not have the capability of reporting sightings. A `TIS` will typically consume intelligence identified in the STIX content but will not produce any STIX content itself.
- Threat Mitigation System (`TMS`)
    - Software instance that acts on course of actions and other threat mitigations such as a firewall or IPS, Endpoint Detection and Response (EDR) software, etc.

For an organization to receive OASIS STIXPreferred certification, the software instances must adhere to persona behavior and prescribed message contents as detailed in the Required Persona/Profile Support section of each test case.

For each persona checklist and test requirements please refer to Section 3 Persona Checklist.

2 Test Case Details

This Test Document defines a set of mandatory and optional test cases identified by persona. All test cases require the use of a TAXII Server (TXS) used in concert with the Producer and Respondent persona components as shown below.

A software product under test may implement multiple personas. Therefore, it is conceivable that a single software product instance may support a TAXII Server persona, the producer and the respondent personas in that instance. However, for the purposes of this test case document, each specific persona verification and expected behavior is called out separately.

The following figure provides a simplified uni-directioinal workflow of data to highlight the relationship between a Producer, a TAXII Server and a Respondent.

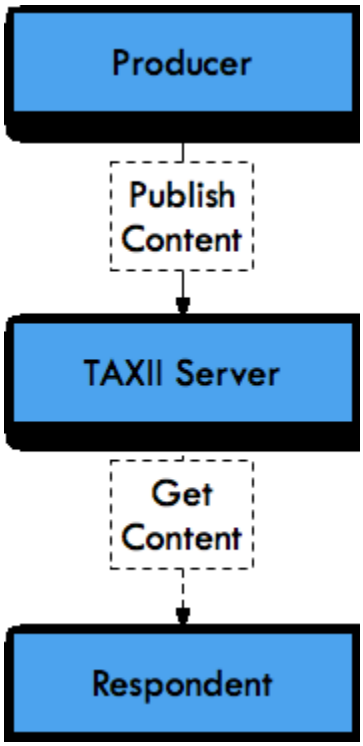

Figure 2: Basic Intelligence Data Flow

This document details the following test cases.

Table 2.0 — List of TAXII Interoperability Test Categories

Description	Producer Personas	Respondent Personas
Common Connection and Error Handling	All	All
Basic Feed Sharing	DFP, TIP; SIEM, TXF	TMS, TDS, TIP, SIEM, TIS

Basic Intel Collaboration	DFP, TIP, TMS, TDS; SIEM, TXF	TIP, SIEM

2.1 Common Test Case Requirements

The following common test case requirements apply to Part 2 tests.

1. The HTTPS over IPv4 protocol must be used for all test cases in this document.
    a. Future versions of this document may introduce testing HTTPS over IPv6 as the TAXII transport protocol.
    b. There are no defined tests that exclude IPv6 support if an organization wishes to execute those tests with HTTPS over IPv6.
2. Bundles
    a. STIX 2.0 specification allows object references that are not distributed within the same Bundle. However, for simplicity and test purposes only, this specification chooses to define all test data without the Bundle wrapper so that organizations may test support of the creation or import of the data across a single bundle or multiple bundles.
    b. Future tests may verify additional cross-Bundle object references.
    c. Unless otherwise specified by a test description, all objects created and referenced by that test case should be contained within at least one Bundle produced by the persona under test.

2.2 Common Connection Test Cases

2.2.1 Description

The test cases in this section apply to all personas that connect to a TAXII Server (TXS) or TAXII Feed (TXF).

To ensure baseline interoperability between every Producer, every Respondent and the TAXII Server that connects those persona together, every test in this section must be completed. For further details on all required tests please refer to Section 3: Persona Checklist.

Recommendation: Advancing to Basic Feed Sharing and Basic Intelligence Collaboration test cases should not be attempted until the test cases in this section are completed successfully.

This set of tests are summarized as follows:

Test Number	Description
P2-CC-1	Test retrieval of Discovery Resource
P2-CC-2	Test retrieval of API-Root Resource

P2-CC-3	Test missing authorization parameter
P2-CC-4	Test incorrect authorization parameter
P2-CC-5	Test incorrect API-Root
P2-CC-6	Test incorrect Collection ID

2.2.2 Required TXS/TXF Configuration

For all tests in this section the TXS/TXF must be configured as follows:

1. Server IPv4 Address: 10.1.1.10[3]
2. Server configured to support client connections via HTTPS [RFC7230] and TLS 1.2 [RFC5246]
3. Server configured for HTTP Basic Authentication [RFC7617]
4. Server configured to authorize a client with the following credentials
    a. Username: test, Password: Passw0rd!
    b. HTTP Authentication Value (Base 64 encoded): "`Authorization: Basic dGVzdDpQYXNzdzByZCE=`"
5. Test Data #1: Discovery Resource Configuration
    a. `URL:` `10.1.1.10:443/taxii/`
    b. `Title:` "TAXII [Server | Feed] Under Test"
    c. `Description:` "This is a TAXII [Server | Feed] under test"
    d. `Contact:` "Admin Contact 1-800-111-1111"
    e. `Default:` "`https://10.1.1.10/api1/`"
    f. `Api_roots:` ["`https://10.1.1.10/api1/`"]
6. Test Data #2: API-Root Resource Configuration
    a. `URL:` `10.1.1.10/api1/`
    b. `Title:` "Sharing Group 1"
    c. `Description:` "This sharing group shares intelligence"
    d. `Versions:` ["taxii-2.0"]
    e. `MaxContentLength:` `104857600`
7. Test Data #3: Error Resource Configuration
    a. `Title:` "Incorrect API Root Get"
    b. `Description:` "An incorrect URL for an API root was accessed"
    c. `Error_id:` `<vendor specific id>`
    d. `Error_code:` `<vendor specific error code>`
    e. `HTTP_status:` `404`

[3] For all tests performed in this section, IP addresses may be substituted as required by the tester's environment. However, please ensure logs and other testing artifacts can prove support of the interoperability verification.

f. External_details: <url to vendor details>
g. Details: "apiroot": "/api2/"

2.2.3 Test Procedure

The systems under test (producer or respondent) must be able to connect to a TAXII Server (TXS) or TAXII Feed (TXF) and display the appropriate connection status as described in the tests below.

System Under Test (SUT): DFP; SIEM; TIP; TMS; TDS; TIS

Every organization submitting their SUT should verify the following behavior by examining log files and/or user interface display of the results:

1. SUT allows a user to select or specify the URL Address of the TXS or TXF to connect to as: https://10.1.1.10:443/taxii/
2. SUT connects to the TXS or TXF and gets the information associated with the TXS or TXF component and displays to the user the following information
    a. Get URL: https://10.1.1.10:443/taxii/
    b. The SUT must show that the returned data matches the setup data Test-Data #1: Discovery Service, as defined in Section 2.2.2.
3. SUT connects to the TXS or TXF API Root https://10.1.1.10/api1/ and gets the information associated with the TXS or TXF API Root as defined in Section 2.2.2 and displays to the user the following information:
    a. Get URL: https://10.1.1.10:443/api1/
    b. The SUT must show that the returned data matches the setup data Test-Data #2: API Root Service, as defined in Section 2.2.2.

2.2.4 Test Cases

All responses in this section must reflect what is configured in Section 2.2.2 TXS Configuration. For data responses that are not based on configured parameters, then the data responses shown are intended to be best practice examples only and judgement by the organization developing the solution should be used to follow those best practices.

2.2.4.1 Test P2-CC-1: Get Discovery Resource

This test will verify that all personas except TXS and TXF can correctly request a Discovery Resource, process the response from the TAXII Server, and display the resource correctly. For TXS and TXF personas, this test will verify that they can correctly process the request and deliver the appropriate response as defined in the table below.

Table 2.2.4.1 - Get Discovery Resource

Request Sent To TXS/TXF
GET /taxii/ HTTP/1.1

```
Host: 10.1.1.10
Accept: application/taxii+json;version=2.0
Authorization: Basic dGVzdDpQYXNzdzByZCE=
```

Response From TXS/TXF

```
HTTP/1.1 200 OK
Content-Type: application/taxii+json;version=2.0

{
  "title": "TAXII [Server | Feed] Under Test",
  "description": "This is a TAXII [Server | Feed] under test",
  "contact": "Admin Contact 1-800-111-1111",
  "default": "https://10.1.1.10/api1/",
  "api_roots": [
    "https://10.1.1.10/api1/"
  ]
}
```

2.2.4.2 Test P2-CC-2: Get API Root

This test will verify that all personas except TXS and TXF can correctly request an API-Root Resource, process the response from the TAXII Server, and display the resource correctly. For TXS and TXF personas, this test will verify that they can correctly process the request and deliver the appropriate response as defined in the table below.

Table 2.2.4.2 - GET API Root Request and Response

Request Sent To TXS/TXF

```
GET /api1/ HTTP/1.1
Host: 10.1.1.10
Accept: application/taxii+json;version=2.0
Authorization: Basic dGVzdDpQYXNzdzByZCE=
```

Response From TXS/TXF

```
HTTP/1.1 200 OK
Content-Type: application/taxii+json;version=2.0

{
  "title": "Sharing Group 1",
  "description": "This sharing group shares intelligence",
  "versions": [ "taxii-2.0"],
  "max_content_length": 104857600
}
```

2.2.4.3 Test P2-CC-3: Missing Authorization Parameter - Returns Unauthorized

This test will verify that TXS and TXF personas will correctly respond to requests that are missing the authorization parameter as defined in section 2.1. Further this tests will verify that all personas except TXS and TXF can correctly process and display the error response from the TAXII Server when the request was missing the authentication parameter.

Table 2.2.4.3 - Missing Authorization Request and Response

Request Sent To TXS/TXF
GET /api1/ HTTP/1.1 Host: 10.1.1.10 Accept: application/taxii+json;version=2.0
Response From TXS/TXF
HTTP/1.1 401 UNAUTHORIZED Content-Type: application/stix+json;version=2.0 WWW-Authenticate: Basic realm="taxii", type=1, title="Login to \"apps\"", Basic realm="simple"

2.2.4.4 Test P2-CC-4: Incorrect Authorization Parameter - Returns Unauthorized

This test will verify that TXS and TXF personas will correctly respond to requests that included an incorrect authorization parameter as defined in section 2.1. Further this tests will verify that all personas except TXS and TXF can correctly process and display the error response from the TAXII Server when the request included an incorrect authentication parameter.

Table 2.2.4.4 - Incorrect Authorization Parameter Request and Response

Request Sent To TXS/TXF
GET /api1/collections/170f24af-c685-411d-bd2a-f45248adb245/ HTTP/1.1 Host: 10.1.1.10 Accept: application/taxii+json;version=2.0 Authorization: Basic eererererere==
Response From TXS/TXF
HTTP/1.1 401 UNAUTHORIZED Content-Type: application/stix+json;version=2.0 WWW-Authenticate: Basic realm="taxii", type=1, title="Login to \"apps\"", Basic realm="simple"

2.2.4.5 Test P2-CC-5: Incorrect API Root Info - Returns Not Found

This test will verify that TXS and TXF personas will correctly respond to requests that use an incorrect API Root as defined in section 2.1. Further this tests will verify that all personas except TXS and TXF can correctly process and display the error response from the TAXII Server when the request included an incorrect API Root as defined in Test Data #1.3.

Table 2.2.4.5 - Incorrect API Root Info Request and Response

Request Sent To TXS/TXF
GET /api2/collections/170f24af-c685-411d-bd2a-f45248adb245/ HTTP/1.1 Host: 10.1.1.10 Accept: application/taxii+json;version=2.0 Authorization: Basic dGVzdDpQYXNzdzByZCE=
Response From TXS/TXF

HTTP/1.1 404 Not Found
Content-Type: application/taxii+json;version=2.0
{
"title": "Incorrect API Root Get",
"description": "An incorrect URL for an API root was accessed",
"error_id": "<vendor specific id>",
"error_code": "<vendor specific error code>",
"http_status": "404",
"external_details": "<vendor details>",
"details": {
"apiroot": "/api2/",
}
}

2.2.4.6 Test P2-CC-6: Incorrect Collection Info - Returns Not Found

This test will verify that TXS and TXF personas will correctly respond to requests that use an incorrect Collection ID as defined in section 2.1. Further this tests will verify that all personas except TXS and TXF can correctly process and display the error response from the TAXII Server when the request included an incorrect Collection ID.

Table 2.2.4.6 - Incorrect Collection Info Request and Response

Request Sent To TXS/TXF
GET /api1/collections/d021ecc8-ab8e-41ab-815e-911c7e329f88/ HTTP/1.1 Host: 10.1.1.10 Accept: application/taxii+json;version=2.0 Authorization: Basic dGVzdDpQYXNzdzByZCE=
Response From TXS/TXF

```
HTTP/1.1 404 Not Found
Content-Type: application/taxii+json;version=2.0
{
  "title": "Incorrect Collection Get",
  "description": "An incorrect URL for a collection was accessed",
  "error_id": "<vendor specific id>",
  "error_code": "<vendor specific error code>",
  "http_status": "404",
  "external_details": "<vendor details>",
  "details": {
       "collection": "/api1/collections/d021ecc8-ab8e-41ab-815e-911c7e329f88/",
  }
}
```

2.3 Basic Feed Sharing Test Cases

2.3.1 Description

Basic Feed Sharing provides for a Producer persona component to produce STIX content and share it with other Respondents via a TAXII Server. TAXII is the required mechanism to publish STIX content to a TXS. A TXF is a read-only TAXII server and provides no TAXII write functionality and as such how content gets to the TXF is out of scope.

This set of tests are summarized as follows:

Test Number	Description
P2-BF-1	Verify Write-Only; Read-Write & Read-Only Collection Sharing
P2-BF-2 to P2-BF-11	Verify Indicator sharing as a producer
P2-BF-12 to P2-BF-22	Verify Indicator sharing as a respondent

2.3.2 Required TXS or TXF Configuration

For all tests in this section the TXS or TXF must be configured with the configuration defined in *Section 2.2 Common Connection* as well as one of the following three configuration setups.

Numerous tests in this section refer to collection IDs during their execution. In these tests, the UUID defined in the Test Data sets is used to reference the collection under test. When performing the test, if the following IDs are not used, they **MUST** be substituted with UUIDs that actually exists in the TXS or TXF that meets the configuration requirements for the test being performed.

TXS Setup A: Demonstrate the use of a collection for adding data to the server and a separate collection for reading from the server.

1. Test Data #1: Write Only Collection
    a. ID: `1105e147-e4c1-4566-8fb1-1046d181fbf8`
    b. URL: `https://10.1.1.10/api1/collections/1105e147-e4c1-4566-8fb1-1046d181fbf8/objects/`
    c. Title: "Collection 1"
    d. Description: "This collection is write only"
    e. Can_read: false
    f. Can_write: true
    g. Media_types: [`"application/stix+json;version=2.0"`]

2. Test Data #2: Read Only Collection
    a. ID: `253900d3-b9dd-46df-8184-469380fae6d2`
    b. URL: `https://10.1.1.10/api1/collections/253900d3-b9dd-46df-8184-469380fae6d2/objects/`
    c. Title: "Collection 2"
    d. Description: "This collection is read only"
    e. Can_read: true
    f. Can_write: false
    g. Media_types: [`"application/stix+json;version=2.0"`]

TXS Setup B: Demonstrate the use of the same collection for adding and reading data to/from the server.

1. Test Data #3: Read-Write Collection
    a. ID: `378e5de7-84a4-45e4-8a34-c02a43d0b657`
    b. URL: `https://10.1.1.10/api1/collections/378e5de7-84a4-45e4-8a34-c02a43d0b657/objects/`
    c. Title: "Collection 3"
    d. Description: "This collection is read-write"
    e. Can_read: true
    f. Can_write: true
    g. Media_types: [`"application/stix+json;version=2.0"`]

TXF Setup C: Demonstrate the use of a single read-only collection for reading from the server.

3. Test Data #2: Read Only Collection
    a. ID: `253900d3-b9dd-46df-8184-469380fae6d2`
    b. URL: `https://10.1.1.10/api1/collections/253900d3-b9dd-46df-8184-469380fae6d2/objects/`
    c. Title: "Collection 2"
    d. Description: "This collection is read only"

e. `Can_read:  true`
f. `Can_write:  false`
g. `Media_types:  [ "application/stix+json;version=2.0" ]`

2.3.3 Producer Test Procedure

The producer persona must be able to create all content according to *Part1: Indicator Sharing*. The following behavior describes the general data flow for each required test case, given below.

Producer Persona Under Test: `DFP; TIP; SIEM`

Step 1: Verify that each Producer and TXS under test can perform all Common Connection Test Cases successfully.

Step 2: Verify that each Producer under test can correctly discover the correct collection as defined in Setups A, B and C are that they are returned correctly to the Producer from the TXS under test.

Step 3: Verify that each Producer under test is able to generate and publish all test data defined in *Part1: Indicator Sharing Producer Test Cases* to the TXS under test and verify the TXS receives that data correctly in the Collection as defined in Step 2. For Setup A where the collection is write-only, verification of a successful write primarily relies on producing logs and status messages indicating that the data was successfully written by the Producer. For Setup B where the collection is read-write, verification can additionally be done by using a separate TAXII GET request to retrieve the data previously written.

Before each test is performed in this section **verify** that the Producer allows a user to select or specify the URL Address of the `TXS` to connect to (example https://10.1.1.10:443/) and performs the tests described in *Section 2.2: Common Connection* Test successfully.

2.3.3.1 Test P2-BF-1-A: Verify Write-Only Collection Information

This test will verify that the TXS will correctly respond to requests to a Write-Only Collection ID and the Producer sending the request verifies that it parses the permission flags correctly for publishing data to the collection.

This test case does not apply to a TXF persona.

Table 2.3.3.1 - Verify Write-Only Collection Request and Response

Request Sent To TXS

`GET /api1/collections/1105e147-e4c1-4566-8fb1-1046d181fbf8/ HTTP/1.1`
`Host: 10.1.1.10`
`Accept: application/taxii+json;version=2.0`
`Authorization: Basic dGVzdDpQYXNzdzByZCE=`

Response From TXS

HTTP/1.1 200 OK
Content-Type: application/taxii+json;version=2.0
 	
{
  "id": "1105e147-e4c1-4566-8fb1-1046d181fbf8",
  "title": "Collection 1",
  "description": "This collection is write only",
  "can_read": false,
  "can_write": true,
  "media_types": [
  "application/stix+json;version=2.0"
  ]
}

Verify on Producer:

1) Producer receives TXS response with the following information:
    a) **HTTP Content-Type** is "`application/taxii+json;version=2.0`"
    b) **HTTP Response Code** is 200 OK
    c) **id** is `1105e147-e4c1-4566-8fb1-1046d181fbf8`
    d) **title** is "Write Collection 1"
    e) **description** is "This is write collection 1"
    f) **can_read** is false
    g) **can_write** is true
    h) **media_types** is `"application/stix+json;version=2.0"`
2) Upon successful receipt of the TXS response, the Producer is able to proceed with publication tests defined in *P2-BF-2 to P2-BF-11: Indicator Publication* test section.

2.3.3.2 Test P2-BF-1-B: Verify Read-Write Collection Information

This test will verify that the TXS will correctly respond to requests to a Read-Write Collection ID and the Producer sending the request verifies that it parses the permission flags correctly for publishing data to the collection.

This test case does not apply to a TXF persona.

Table 2.3.3.2 - Verify Read-Write Collection Request and Response

Request Sent To TXS
GET /api1/collections/378e5de7-84a4-45e4-8a34-c02a43d0b657/ HTTP/1.1 Host: 10.1.1.10 Accept: application/taxii+json;version=2.0 Authorization: Basic dGVzdDpQYXNzdzByZCE=
Response From TXS
HTTP/1.1 200 OK Content-Type: application/taxii+json;version=2.0

```
{
  "id": "378e5de7-84a4-45e4-8a34-c02a43d0b657",
  "title": "Collection 3",
  "description": "This collection is read write",
  "can_read": true,
  "can_write": true,
  "media_types": [
    "application/stix+json;version=2.0"
  ]
}
```

Verify on Producer:

1) Verify at the Producer that the TXS responds with the following information:
    a) **HTTP Content-Type** is "`application/taxii+json;version=2.0`"
    b) **HTTP Response Code** is 200 OK
    c) **id** is `378e5de7-84a4-45e4-8a34-c02a43d0b657`
    d) **title** is “Read-Write Collection 1”
    e) **description** is “This is read-write collection 1”
    f) **can_read** is true
    g) **can_write** is true
    h) **media_types** is `"application/stix+json;version=2.0"`
2) Upon receipt of the TXS response that the Producer is able to proceed with publication tests.

2.3.3.3 Test P2-BF-1-C: Verify Read-Only Collection Information

This test will verify that the TXS will correctly respond to requests to a Read-Only Collection ID and the Producer sending the request verifies that it parses the permission flags and reports an appropriate message to an administrator or user that this collection does not allow publication to it.

This test case does not apply to a TXF persona.

Table 2.3.3.3 - Verify Read-Only Collection Request and Response

Request Sent To TXS

```
GET /api1/collections/253900d3-b9dd-46df-8184-469380fae6d2/ HTTP/1.1
Host: 10.1.1.10
Accept: application/taxii+json;version=2.0
Authorization: Basic dGVzdDpQYXNzdzByZCE=
```

Response From TXS

```
HTTP/1.1 200 OK
Content-Type: application/taxii+json;version=2.0

{
  "id": "253900d3-b9dd-46df-8184-469380fae6d2",
  "title": "Collection 2",
  "description": "This collection is read only",
  "can_read": true,
  "can_write": false,
  "media_types": [
```

```
    "application/stix+json;version=2.0"
  ]
}
```

Verify on Producer:

1) Verify at the Producer that the TXS responds with the following information:
    a) **HTTP Content-Type** is "`application/taxii+json;version=2.0`"
    b) **HTTP Response Code** is 200 OK
    c) **id** is `253900d3-b9dd-46df-8184-469380fae6d2`
    d) **title** is "Collection 2"
    e) **description** is "This collection is read only"
    f) **can_read** is true
    g) **can_write** is false
    h) **media_types** is `"application/stix+json;version=2.0"`
2) Upon receipt of the TXS response that the Producer reports an error that the collection is not writable and the Producer does not attempt any further write actions with that collection.

2.3.3.4 Tests P2-BF-2 to P2-BF-11: Indicator Publication

For each test case listed in this section, the general form of the POST and POST-RESPONSE are as follows.

1. The test organization must verify that the returned responses
    a. Match the content in the To TXS or From TXS cells in the table below, with the correct total count of objects.
    b. For each test case P2-BF-X there are 2 test cases P2-BF-X-A and P2-BF-X-B for Setup A and Setup B
    c. For each section described in Part1: Indicator Sharing Producer Test Cases the Producer will publish the content to the TXS at the appropriate collection where the TXS component will not respond to the post until all objects within the bundle have been processed.
    d. For each POST request sent, verify the TXS accepts the content by verifying the following was returned to the Producer:
        i. **HTTP Response code** is 202 Accepted
        ii. **id** represents a unique identifier for each post
        iii. **status** is complete
        iv. **request_timestamp** represents the time of the post
        v. **total_count** represents the number of objects in the bundle test case
        vi. **success_count** is the same as total_count
        vii. **successes** is an array of the object identifiers in the submitted bundle and matches the identifiers posted for each indicator
        viii. **failure_count** is 0
        ix. **pending_count** is 0
2. These tests do not apply to the TXF persona.

Table 2.3.3.4 - Indicator Publication POST Request and Response

** The UUID shown in this table is the one defined for the write-only collection. If the test is being performed for a write-read collection, then replace the UUID with an appropriate collection UUID.*

Request Sent To TXS

```
POST /api1/collections/1105e147-e4c1-4566-8fb1-1046d181fbf8/objects/ HTTP/1.1
Host: 10.1.1.10
Accept: application/taxii+json;version=2.0
Authorization: Basic dGVzdDpQYXNzdzByZCE=
Content-Type: application/stix+json;version=2.0

{
  "type": "content from test table below...",
}
```

Response From TXS

```
HTTP/1.1 202 Accepted
Content-Type: application/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
}
```

Table 2.3.4.3 - Test Case Total Object Count Requirement

**The total count of objects includes the identity object and the associated intelligence objects.*

Test Cases	Test Case Setups	Total Count*
P2-BF-2 Indicator IPv4 Address	P2-BF-2-A; P2-BF-2-B	2
P2-BF-3 Indicator IPv4 Address CIDR	P2-BF-3-A; P2-BF-3-B	2
P2-BF-4 Two Indicators with IPv4 Address CIDR	P2-BF-4-A; P2-BF-4-B	2
P2-BF-5 Indicator with IPv6 Address	P2-BF-5-A; P2-BF-5-B	2

P2-BF-6 Indicator with IPv6 Address CIDR	P2-BF-6-A; P2-BF-6-B	2
P2-BF-7- Multiple Indicators within the same bundle	P2-BF-7-A; P2-BF-7-B	3
P2-BF-8 Indicator FQDN	P2-BF-8-A; P2-BF-8-B	2
P2-BF-9 Indicator URL	P2-BF-9-A; P2-BF-9-B	2
P2-BF-10 Indicator URL or FQDN	P2-BF-10-A; P2-BF-10-B	2
P2-BF-11 Indicator File hash with SHA256 or MD5 values	P2-BF-11-A; P2-BF-11-B	2

2.3.4 Respondent Test Procedure

The Respondent persona must be able to get all content according *Part1: Indicator Sharing*. The following behavior describes the general data flow for each required test case, given below.

Respondent Persona Under Test: `TIP; SIEM; TMS; TDS; TIS`

Step 1: Verify all Common Connection Test Cases successfully pass for each Respondent under test and TXS or TXF under test.

Step 2: Verify for each Respondent under test that the correct readable collection for Setups A; B and C are discoverable and returned to the Respondent from the TXS/TXF under test.

Step 3: Verify for each Respondent under test that it is able to read all test data defined *Part1: Indicator Sharing Respondent Test Cases* to the TXS/TXF under test and verify the TXS/TXF returns that data correctly from the Collection defined in for Setups A; B and C to the Respondent.

2.3.4.1 Tests P2-BF-12 to P2-BF-21: Indicator Get

For each of the test cases listed in this section, the general form of the GET and GET-RESPONSE are as follows.

1. The test organization must verify that the returned bundle
    a. match the content in the To `TXS/TXF` or From `TXS/TXF` cells in the table below, with the correct total count of objects.

Table 2.3.4.1 - Basic GET Request and Response

Request Sent To TXS/TXF

```
GET /api1/collections/253900d3-b9dd-46df-8184-469380fae6d2/objects/ HTTP/1.1
Host: 10.1.1.10
Accept: application/stix+json;version=2.0
Authorization: Basic dGVzdDpQYXNzdzByZCE=
```

Response From TXS/TXF

```
HTTP/1.1 200 OK
Content-Type: application/stix+json;version=2.0

{
  "type": "bundle",
  ...
  "objects": [
    {
      "type": "indicator",
      ...
    }
  ]
}
```

Table 2.3.4.2 - Test Case Total Object Count Requirement

**The total count of objects include the identity object and the associated intelligence objects.*

Test Cases	Test Case Setups	Total Count*
P2-BF-12 Indicator IPv4 Address	P2-BF-12-A; P2-BF-12-B; P2-BF-12-C	2
P2-BF-13 Indicator IPv4 Address CIDR	P2-BF1-3-A; P2-BF-13-B; P2-BF-13-C	2
P2-BF-14 Two Indicators with IPv4 Address CIDR	P2-BF-14-A; P2-BF-14-B; P2-BF-14-C	2
P2-BF-15 Indicator with IPv6 Address	P2-BF-15-A; P2-BF-15-B; P2-BF-15-C	2
P2-BF-16 Indicator with IPv6 Address CIDR	P2-BF-16-A; P2-BF-16-B; P2-BF-16-C	2
P2-BF-17 Multiple Indicators within the same bundle	P2-BF-17-A; P2-BF-17-B; P2-BF-17-C	3
P2-BF-18 Indicator FQDN	P2-BF-18-A; P2-BF-18-B; P2-BF-18-C	2
P2-BF-19 Indicator URL	P2-BF-19-A; P2-BF-19-B; P2-BF-19-C	2
P2-BF-20 Indicator URL or FQDN	P2-BF-20-A; P2-BF-20-B; P2-BF-20-C	2
P2-BF-21 Indicator File hash with SHA256 or MD5 values	P2-BF-21-A; P2-BF-21-B; P2-BF-21-C	2

2.4 Basic Intelligence Collaboration Test Cases

2.4.1 Description

Basic Intelligence Collaboration provides for a Producer persona component to produce STIX content, typically initiated by a human analyst, and share that content via a TAXII Server with a Respondent persona component. That Respondent then may respond with further changes to the same or related intelligence content.

To certify interoperability, the following required test cases must be evaluated:

- **Test Case #1: Same organization** sharing and modifying **common** intelligence between two analysts using two systems
    - In this scenario the first analyst creates an intelligence element that they wish to share with other analysts within the same organization for their perspective and feedback.
    - The second analyst receives the intelligence from the first analyst and then proceeds to modify the existing intelligence, using the same organization's identity, and reshares back to the first analyst for their review and acknowledgement.
    - See Figure 2.4.1.a
- **Test Case #2: Different organizations** sharing and modifying **related** intelligence between two analysts using two systems.
    - In this scenario the 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.
    - The 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.
    - See Figure 2.4.1.b
- **Test 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
    - In this scenario the 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.
    - The 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.

- The data flow for Test Case #3 resembles Test Case #2 except that both analysts work for the same organization.

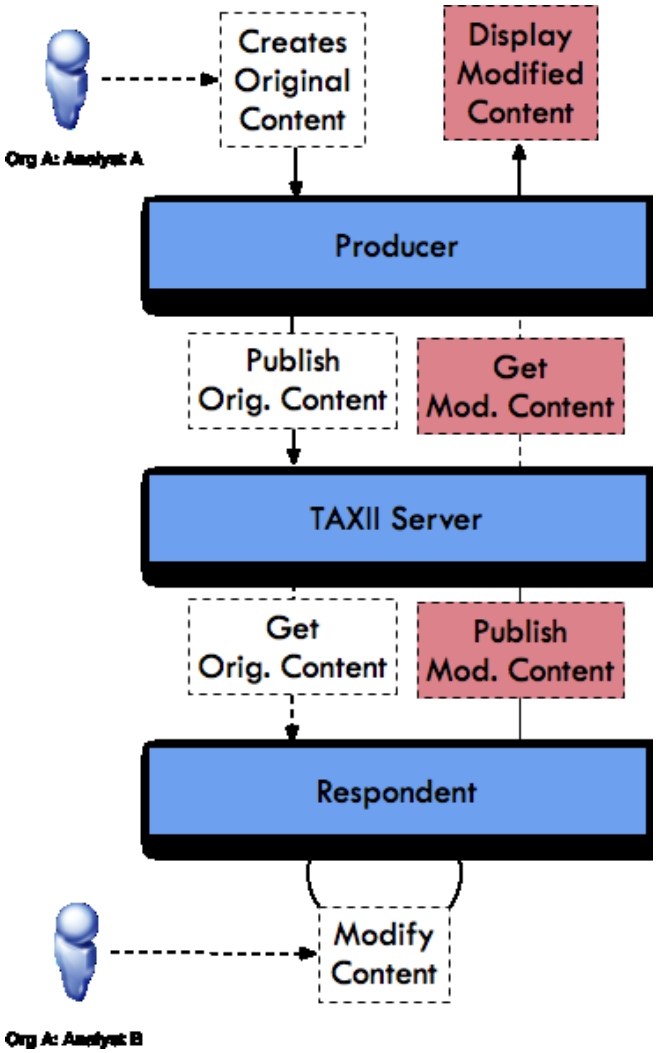

Figure 2.4.1.a: Same Organization - Collaboration Data Flow

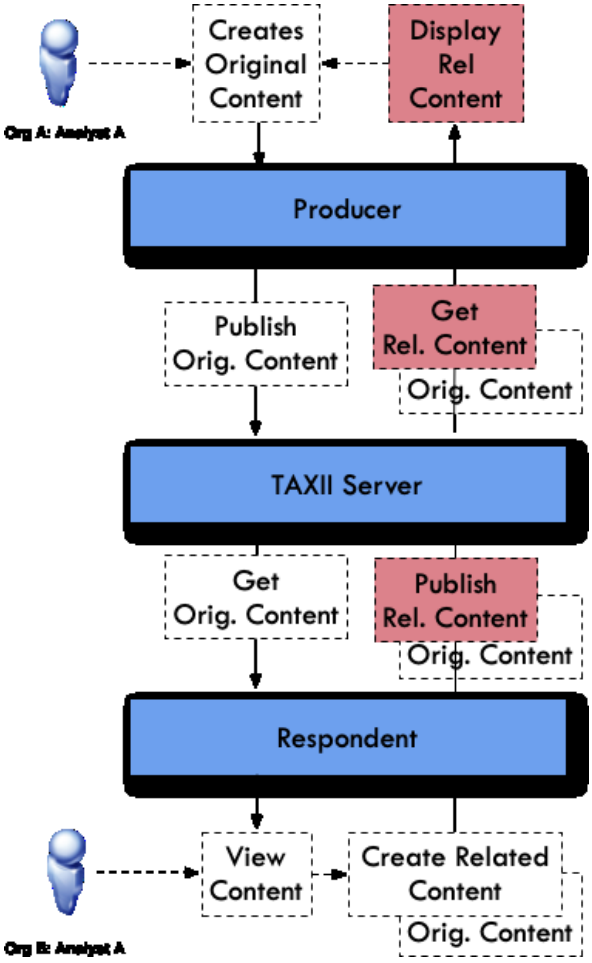

Figure 2.4.1.b - Different Organization - Collaboration Data Flow

This set of tests are summarized as follows:

Test Number	Description
P2-IC-1	Verify Write-Only; Read-Write Intelligence Collaboration Sharing
P2-IC-2 to P2-IC-11	Verify Indicator sharing as a producer
P2-IC-12 to P2-IC-21	Verify Indicator GET & Update Same Intelligence for Same Organization
P2-IC-22 to P2-IC-31	Verify Indicator GET & Create Related Intelligence for Different Organizations

2.4.2 Required TXS Configuration

For all tests in this section the `TXS` must be configured using a combination of the *Section 2.2: Common Connection* tests and the *Section 2.3: Basic Feed Sharing: Required TXS Configuration*. Refer to Table 2.3.2 for an illustration of combined configurations.

For Tests P2-IC-2 to P2-IC-21, both Producer and Respondent must be configured as the same **created_by** entity (i.e. the same organization entity) to ensure that both systems may modify the same intelligence shared between the Producer and Respondent.

For Tests P2-IC-22 to P2-IC-31, both Producer and Respondent must be configured with different **created_by** entity (i.e. different organization entities) to ensure that each system enforces rules on modification of intelligence consistent with the STIX specification that disallows modification of non-same organizational intelligence.

Numerous tests in this section **MUST** refer to collection IDs during their execution. In these tests several UUIDs are defined to reference the collection under test. When performing the test, this ID **MAY** be substituted with any UUID that exists in the TXS Server that meets the configuration requirements for the test.

2.4.3 Producer Test Procedure

The producer persona must be able to create all content according *Part1: Indicator Sharing*. The following behavior describes the general data flow for each test case.

Producer Persona Under Test: `TIP; SIEM`

Step 1: Verify that each Producer and TXS under test can perform all Common Connection Test Cases successfully.

Step 2: Verify that each Producer under test can correctly discover the correct writeable collection as defined in Setups A and B are that they are returned correctly to the Producer from the TXS under test.

Step 3: Verify that each Producer under test is able to generate and publish all test data defined in *Part1: Indicator Sharing: Required Producer Persona Support* to the TXS under test and verify the TXS receives that data correctly in the Collection as defined in Step 2.

2.4.3.1 Test P2-IC-1-A: Verify Write-Only Collection Information

This test will verify that the TXS will correctly respond to requests to the appropriate Write-Only Collection ID and the Producer sending the request verifies that it parses the permission flags correctly for publishing data to the collection.

This test case does not apply to a TXF persona.

Table 2.3.3.1 - Verify Write-Only Collection Request and Response

Request Sent To TXS

```
GET /api1/collections/1105e147-e4c1-4566-8fb1-1046d181fbf8/ HTTP/1.1
Host: 10.1.1.10
Accept: application/taxii+json;version=2.0
Authorization: Basic dGVzdDpQYXNzdzByZCE=
```

Response From TXS

```
HTTP/1.1 200 OK
Content-Type: application/taxii+json;version=2.0

{
  "id": "1105e147-e4c1-4566-8fb1-1046d181fbf8",
  "title": "Collection 1",
  "description": "This collection is write only",
  "can_read": false,
  "can_write": true,
  "media_types": [
    "application/stix+json;version=2.0"
  ]
}
```

Verify on Producer:

1) Producer receives TXS response with the following information:
    a) **HTTP Response Code** is 200 OK
    b) **id** is `1105e147-e4c1-4566-8fb1-1046d181fbf8`
    c) **title** is “Write Collection 1”
    d) **description** is “This is write collection 1”
    e) **can_read** is false
    f) **can_write** is true
    g) **media_types** is `"application/stix+json;version=2.0"`

2) Upon receipt of the TXS response that the Producer is able to proceed with publication tests.

2.4.3.2 Test P2-IC-1-B: Verify Read-Write Collection Information

This test will verify that TXS will correctly respond to requests to the appropriate Read-Write Collection ID and the Producer sending the request verifies that it parses the permission flags correctly for publishing data to the collection.

This test case does not apply to a TXF persona.

Table 2.3.3.2 - Verify Read-Write Collection Request and Response

Request Sent To TXS

```
GET /api1/collections/378e5de7-84a4-45e4-8a34-c02a43d0b657/ HTTP/1.1
Host: 10.1.1.10
Accept: application/taxii+json;version=2.0
Authorization: Basic dGVzdDpQYXNzdzByZCE=
```

Response From TXS

```
HTTP/1.1 200 OK
Content-Type: application/taxii+json;version=2.0

{
  "id": "378e5de7-84a4-45e4-8a34-c02a43d0b657",
  "title": "Collection 3",
  "description": "This collection is read write",
  "can_read": true,
  "can_write": true,
  "media_types": [
    "application/stix+json;version=2.0"
  ]
}
```

Verify on Producer:

3) Verify at the Producer that the TXS responds with the following information:
   a) **HTTP Response Code** is 200 OK
   b) **id** is `378e5de7-84a4-45e4-8a34-c02a43d0b657`
   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/stix+json;version=2.0"`
4) Upon receipt of the TXS response that the Producer is able to proceed with publication tests.

2.4.3.3 Tests P2-IC-2 to P2-IC-11: Indicator Publication

For each test case listed in this section, the general form of the POST and POST-RESPONSE are as follows.

1. The test organization must verify that the returned responses
   a. Match the content in the To TXS or From TXS cells in the table below, with the correct total count of objects.
   b. For each test case P2-IC-X there are 2 test cases P2-IC-X-A and P2-IC-X-B for Setup A and Setup B
   c. For each section described in *Part1: Indicator Sharing Producer Test Cases* the Producer will publish the content to the TXS at the appropriate collection where the TXS component will not respond to the post until all objects within the bundle have been processed.
   d. For each POST request sent, verify the TXS accepts the content by verifying the following was returned to the Producer:
      i. **HTTP Response code** is 202 Accepted
      ii. **id** represents a unique identifier for each post
      iii. **status** is complete
      iv. **request_timestamp** represents the time of the post
      v. **total_count** represents the number of objects in the bundle test case

vi. **success_count** is the same as total_count
vii. **successes** is an array of the object identifiers in the submitted bundle and matches the identifiers posted for each indicator
viii. **failure_count** is 0
ix. **pending_count** is 0

e. These tests do not apply to the TXF persona.

Table 2.4.3.3 - Indicator Publication POST Request and Response

Request Sent To TXS

```
POST /api1/collections/1105e147-e4c1-4566-8fb1-1046d181fbf8/objects/ HTTP/1.1
Host: 10.1.1.10
Accept: application/taxii+json;version=2.0
Authorization: Basic dGVzdDpQYXNzdzByZCE=
Content-Type: application/vnd.oasis.stix+json;version=2.0

{
  "type": "content from test table below...",
}
```

Response From TXS

```
HTTP/1.1 202 Accepted
Content-Type: application/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
}
```

**The total count of objects includes the identity object and the associated intelligence objects.*

Test Cases	Test Case Setups	Total Count Checks
P2-IC-2 Indicator IPv4 Address	P2-IC-2-A; P2-iC-2-B	2
P2-IC-3 Indicator IPv4 Address CIDR	P2-IC-3-A; P2-iC-3-B	2
P2-IC-4 Two Indicators with IPv4 Address CIDR	P2-IC-4-A; P2-iC-4-B	2

P2-IC-5 Indicator with IPv6 Address	P2-IC-5-A; P2-iC-5-B	2
P2-IC-6 Indicator with IPv6 Address CIDR	P2-IC-6-A; P2-iC-6-B	2
P2-IC-7 Multiple Indicators within the same bundle	P2-IC-7-A; P2-iC-7-B	3
P2-IC-8 Indicator FQDN	P2-IC-8-A; P2-iC-8-B	2
P2-IC-9 Indicator URL	P2-IC-9-A; P2-iC-9-B	2
P2-IC-10 Indicator URL or FQDN	P2-IC-10-A; P2-iC-10-B	2
P2-IC-11 Indicator File hash with SHA256 or MD5 values	P2-IC-11-A; P2-iC-11-B	2

2.4.4 Respondent Test Procedure

The Respondent persona must be able to get all content according *Part1:Indicator Sharing: Required Respondent Support* section. The following behavior describes the general data flow for each test case.

Respondent Persona Under Test: `TIP; SIEM`

Step 1: Verify that each Respondent and TXS under test can perform all Common Connection Test Cases successfully.

Step 2: Verify that each Respondent under test can correctly discover the correct readable & writeable collections as defined in Setups A and B are that they are returned correctly to the Respondent from the TXS under test.

Step 3: Verify that each Respondent under test is able to handle correct permission rules based on whether the organization that originally published the intelligence matches the organization of the Respondent or not. The following cases are tested:

a) modify existing intelligence read from a Producer and then re-publish the modified intelligence to the TXS server or

b) create related intelligence and associate that new intelligence with the previously published intelligence and publish the new related intelligence and associated relationships to the existing intelligence or

c) enforce STIX modification rules to ensure that non-allowed modifiable intelligence is protected

2.4.4.1 P2-IC-12 to P2-IC-21 Indicator Get & Update Intelligence (Same Org, Different Analysts)

The test organization must verify the following:

a) Match the content in the To TXS or From TXS cells in the table below, with the correct total count of objects.
b) For each test case P2-IC-X there are 2 test cases P2-IC-X-A and P2-IC-X-B for Setup A and Setup B
c) The Respondent must show in log files or via the user interface of the product that intelligence has been received from the Producer (via the TXS collection) and show in the log files or the user interface what intelligence including the following properties
   i) **Id** must include the UUID of the Indicator shared
   ii) **created_by_ref** must point to the identity of the **Producer**;
   iii) **created** and **modified** must match the timestamp to millisecond granularity of the original shared intelligence
   iv) **name** contains the name of the Indicator
   v) **description** contains the description field of the Indicator
   vi) **pattern** contains the pattern field of the Indicator
   vii) **valid_from** contains the date for the indicator valid_from
d) The Respondent must allow the Respondent analyst via the user interface to modify the **description** field value for each intelligence object to "Changed Indicator Description" and allow them to publish that Indicator back to the Producer
e) For each POST request sent, verify the TXS accepts the content by verifying the following was returned to the Producer:
   i. **HTTP Response code** is 202 Accepted
   ii. **id** represents a unique identifier for each post
   iii. **status** is complete
   iv. **request_timestamp** represents the time of the post
   v. **total_count** represents the number of objects in the bundle test case
   vi. **success_count** is the same as total_count
   vii. **successes** is an array of the object identifiers in the submitted bundle and matches the identifiers posted for each indicator
   viii. **failure_count** is 0
   ix. **pending_count** is 0
f. Verify after the Respondent posted the data to the TXS collection that the modified intelligence reflects the modified description fields on the TXS server
g. *Repeat the verification steps of the original Indicator but instead performing the test with Respondent of the changed description as the Producer*
h. These tests do not apply to the TXF persona

Table 2.4.4.1 - Indicator GET & Updated Modified Request and Response

Request #1 Sent To TXS
GET /api1/collections/91a7b528-80eb-42ed-a74d-bd5a2118/objects/ HTTP/1.1 Host: 10.1.1.10 Accept: application/stix+json;version=2.0

```
Authorization: Basic dGVzdDpQYXNzdzByZCE=
```

Response #1 From TXS

```
HTTP/1.1 200 OK
Content-Type: application/stix+json;version=2.0

{
  "type": "bundle",
  ...
  "objects": [
    {
      "type": "indicator",
      ...
    }
  ]
}
```

Request #2 Sent To TXS

```
POST /api1/collections/1105e147-e4c1-4566-8fb1-1046d181fbf8/objects/ HTTP/1.1
Host: 10.1.1.10
Accept: application/taxii+json;version=2.0
Authorization: Basic dGVzdDpQYXNzdzByZCE=
Content-Type: application/vnd.oasis.stix+json;version=2.0

{
  "type": "content from test table below with modified description fields for each
indicator...",
}
```

Response #2 From TXS

```
HTTP/1.1 202 Accepted
Content-Type: application/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
}
```

Table 2.4.4.2 - Test Case Total Object Count Requirement

**The total count of objects includes the identity object and the associated intelligence objects.*

Test Cases	Test Case Setups	Total Count
P2-IC-12 Indicator IPv4 Address	P2-IC-12-A; P2-iC-12-B	2
P2-IC-13 Indicator IPv4 Address CIDR	P2-IC-13-A; P2-iC-13-B	2
P2-IC-14 Two Indicators with IPv4 Address CIDR	P2-IC-14-A; P2-iC-14-B	2
P2-IC-15 Indicator with IPv6 Address	P2-IC-15-A; P2-iC-15-B	2
P2-IC-16 Indicator with IPv6 Address CIDR	P2-IC-16-A; P2-iC-16-B	2
P2-IC-17 Multiple Indicators within the same bundle	P2-IC-17-A; P2-iC-17-B	3
P2-IC-18 Indicator FQDN	P2-IC-18-A; P2-iC-18-B	2
P2-IC-19 Indicator URL	P2-IC-19-A; P2-iC-19-B	2
P2-IC-20 Indicator URL or FQDN	P2-IC-20-A; P2-iC-20-B	2
P2-IC-21 Indicator File hash with SHA256 or MD5 values	P2-IC-21-A; P2-iC-21-B	2

2.4.4.2 P2-IC-22 to P2-IC-31 Indicator Get & Create Related Intelligence (Different Org)

The test organization must verify the following:

a) Match the content in the To TXS or From TXS cells in the table below, with the correct total count of objects.
b) For each test case P2-IC-X there are 2 test cases P2-IC-X-A and P2-IC-X-B for Setup A and Setup B
c) The Respondent must allow the Respondent analyst via the user interface to create a new Indicator with all mandatory fields filled in and allow the user to associate the new Indicator with the previously received Indicator. The properties on the new Indicator should be:
    i) **Id** must include a new UUID of the Indicator being created
    ii) **created_by_ref** must point to the identity of the **Respondent**;
    iii) **created** and **modified** must match the timestamp to millisecond granularity of the original shared intelligence
    iv) **name** contains the name of the new Indicator
    v) **description** contains the description field of the new Indicator
    vi) **pattern** contains the pattern field of the new Indicator
    vii) **valid_from** contains the date for the indicator valid_from

d) The Respondent then should allow the analyst to publish that Indicator and the relationship between the new Indicator and the original Indicator back to the Producer

e) For each POST request sent, verify the TXS accepts the content by verifying the following was returned to the Producer:

   i) **HTTP Response code** is 202 Accepted

   ii) **id** represents a unique identifier for each post

   iii) **status** is complete

   iv) **request_timestamp** represents the time of the post

   v) **total_count** represents the number of objects in the bundle test case

   vi) **success_count** is the same as total_count

   vii) **successes** is an array of the object identifiers in the submitted bundle and matches the identifiers posted for each indicator

   viii) **failure_count** is 0

   ix) **pending_count** is 0

f) Verify after the Respondent posted the data to the TXS collection that the new intelligence reflects the new related intelligence on the TXS server

g) These tests do not apply to the TXF persona

Table 2.4.4.2 - Indicator GET & Create Related Intelligence Request and Response

Request #1 Sent To TXS

```
GET /api1/collections/91a7b528-80eb-42ed-a74d-bd5a2118/objects/ HTTP/1.1
Host: 10.1.1.10
Accept: application/stix+json;version=2.0
Authorization: Basic dGVzdDpQYXNzdzByZCE=
```

Response #1 From TXS

```
HTTP/1.1 200 OK
Content-Type: application/stix+json;version=2.0

{
  "type": "bundle",
  ...
  "objects": [
    {
      "type": "indicator",
      ...
    }
  ]
}
```

Request #2 Sent To TXS

```
POST /api1/collections/1105e147-e4c1-4566-8fb1-1046d181fbf8/objects/ HTTP/1.1
Host: 10.1.1.10
Accept: application/taxii+json;version=2.0
```

```
Authorization: Basic dGVzdDpQYXNzdzByZCE=
Content-Type: application/vnd.oasis.stix+json;version=2.0

{
  "type": "content from test table below with additional indicator and relationship...",
}
```

Response #2 From TXS

```
HTTP/1.1 202 Accepted
Content-Type: application/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
}
```

Table 2.4.6.3 - Test Case Total Object Count Requirement

**The total count of objects includes the Identity object and the associated new intelligence objects.*

Test Cases	Test Case Setups	Total Count
P2-IC-22 Indicator IPv4 Address	P2-IC-22-A; P2-iC-22-B	2
P2-IC-23 Indicator IPv4 Address CIDR	P2-IC-23-A; P2-iC-23-B	2
P2-IC-24 Two Indicators with IPv4 Address CIDR	P2-IC-24-A; P2-iC-24-B	2
P2-IC-25 Indicator with IPv6 Address	P2-IC-25-A; P2-iC-25-B	2
P2-IC-26 Indicator with IPv6 Address CIDR	P2-IC-26-A; P2-iC-26-B	2
P2-IC-27 Multiple Indicators within the same bundle	P2-IC-27-A; P2-iC-27-B	3
P2-IC-28 Indicator FQDN	P2-IC-28-A; P2-iC-28-B	2
P2-IC-29 Indicator URL	P2-IC-29-A; P2-iC-29-B	2

P2-IC-30 Indicator URL or FQDN	P2-IC-30-A; P2-iC-30-B	2
P2-IC-31 Indicator File hash with SHA256 or MD5 values	P2-IC-31-A; P2-iC-31-B	2

3 Persona Checklist

The following checklists summarize all tests that a persona (Producer or Respondent) must conform to within that persona for **both Part 1 and Part 2**. An organization must submit the results for their specific persona(s) to the OASIS CTI TC Interoperability SC to achieve confirmation of interoperability and to be listed on the OASIS website page showing the organization's compliance to STIX 2.0.

Results must be submitted to the STIX Interoperability sub-committee for verification via the STIXPreferred portal at https://oasis-stixpreferred.org/**.**

Part 1 checklists are duplicated for each persona within this document. Test results for both Part 1 and Part 2 must be provided if submitting results for a STIX/TAXII certification that is being submitted for Part2.

Results may be submitted as separate logs; documents; screenshots; any other proof such that the reviewers can assess whether the organization has successfully complied with STIX/TAXII 2.0 interoperability tests specified herein.

Instructions to organizations:

1) Fill in the section relevant to your instance
2) For each test, add a reference in the results column indicating what evidence documentation supports your compliance results.
3) Submit both the filled in section and all indicated supporting documentation.

After review and verification of your compliance demonstration submittal, the OASIS CTI TC Interoperability SC will post confirmation to the CTI TC website at: {URL here}. Your compliance listing will include the following:

1) Name, address and contact information of the company performing the demonstration,
2) Name of the conforming product, and
3) Summary of your compliance demonstration findings that substantiate interoperability conformance.

No independent testing will be performed by the Interoperability SC; rather compliance will be based solely on your self-verification testing, confirmed through your complete and accurate test results, accompanied by your indicated supporting documentation.

3.1 Performing Verification Tests and Recording Results

As a testing organization, you must/need to follow these procedures:

1) Identify one or more persona(s) that your software is being tested against. Go to the section and for each row in the verification tables (Part 1 and Part 2) perform self-certification tests that

prove that your software outputs the expected results and behaves according to the general test case data flows.

2) For each test, identify whether your software is a
    a) Producer, or
    b) Respondent, or
    c) TAXII Server (Part 2 test cases only).
3) For the identified role (e.g. Producer), perform the test in that row/role combination, capture evidence of your software's behavior, and paste that evidence into the table's Results column, confirming that the expected behavior is met. If your software has both roles for a test row, then record the results for each role separately.
    a) Example 1: Organization A wants to self-certify their Data Feed software product. They identify that they are producing threat intelligence and test their software as a Producer in both Part 1 and Part 2 test case tests.
    b) Example 2: Organization B wants to self-certify their Threat Intelligence Platform. They identify that their software is both a Producer and Respondent in the tests cases for Data Feed sharing and Basic Intelligence Collaboration. For each test, Organization B will perform and record the test results for each role.
        i) Test result #1, you record results as a Producer of the intelligence and Test result #2, you record results as a Respondent to the intelligence. For each test, you may choose to use your software as both Producer and Respondent in the test scenario or as a 3rd party that acts in those roles.
4) For test rows that identify numbered Test Cases (UC), perform that test for each UC# and provide results for each Test+UC server combination.

3.2 Data Feed Provider (DFP)

For the purpose of this document a DFP may be defined as a software instance that acts as a producer of STIX 2.0 content.

Any instance being qualified as a DFP must confirm test results for the following tests for both STIX/TAXII 2.0 Interoperability Test Documents Part 1 and Part 2.

Table 3.2.1 - Data Feed Provider (DFP) Part 1 Test Verification List

Test Case	Test	Verification	Results
Indicator Sharing	Part 1 - 2.2.3.1 Indicator IPv4 Address	Mandatory	<fill in>
Indicator Sharing	2.2.3.2 Indicator IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	2.2.3.3 Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	2.2.3.4 Indicator with IPv6 Address	Optional	<if supported, fill in>

Indicator Sharing	2.2.3.5 Indicator with IPv6 Address CIDR	Optional	<if supported, fill in>
Indicator Sharing	2.2.3.6 Multiple Indicators within the same bundle	Mandatory	<fill in>
Indicator Sharing	2.2.3.7 Indicator FQDN	Mandatory	<fill in>
Indicator Sharing	2.2.3.8 Indicator URL	Mandatory	<fill in>
Indicator Sharing	2.2.3.9 Indicator URL or FQDN	Mandatory	<fill in>
Indicator Sharing	2.2.3.10 Indicator File hash with SHA256 or MD5 values	Mandatory	<fill in>
Sighting Sharing	2.3.3 Producer Test Case Data	Optional	<if supported, fill in>
Sighting Sharing	2.3.5.1 Sighting + Indicator with IPv4 Address	Optional	<if supported, fill in>
Sighting Sharing	2.3.5.2 Sighting + Indicator with IPv4 Address Matching CIDR	Optional	<if supported, fill in>
Sighting Sharing	2.3.5.3 Sighting + Indicator with IPv6 Address Matching CIDR	Optional	<if supported, fill in>
Sighting Sharing	2.3.5.4 Sighting + Indicator with NO observed data	Optional	<if supported, fill in>
Sighting Sharing	2.3.5.5 Sighting + Indicator with URL	Optional	<if supported, fill in>
Sighting Sharing	2.3.5.6 Sighting + Indicator with File Hash	Optional	<if supported, fill in>
Versioning	2.4.3.1 Creation of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	2.4.3.2 Creation of a Sighting with Identity and Date	Mandatory	<fill in>
Versioning	2.4.7.1 Modification of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	2.4.7.2 Modification of a Sighting with Identity and Date	Mandatory	<fill in>

Versioning	2.4.11.1 Deletion of an Indicator with Identity; Dates	Mandatory	<fill in>
Versioning	2.4.11.2 Deletion of a Sighting and Associated Observed Data	Mandatory	<fill in>
Data Markings	2.5.3.1 TLP Green + Indicator with IPv4 Address	Mandatory	<fill in>
Data Markings	2.5.3.2 TLP Amber + Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Data Markings	2.5.3.3 TLP White and TLP Red + Indicator with IPv6 Address	Optional	<if supported, fill in>
Data Markings	2.5.3.4 TLP Red + Sighting and Indicator	Optional	<if supported, fill in>
Custom Object Creation	2.6.3.1 Custom Object Creation	Optional	<if supported, fill in>
Custom Property Creation	2.6.3.2 Custom Property Creation	Optional	<if supported, fill in>
Custom Ingestion	2.6.4 Required Respondent Support	n/a	n/a
Create COA	2.7.3.1 Create COA	Optional	<if supported, fill in>
Create COA Relationship	2.7.3.2 Create COA with Relationship	Optional	<if supported, fill in>

Table 3.2.2 - Data Feed Provider (DFP) Part 2 Test Verification List

Test Case	Test	Producer	Respondent
Common Connection	Get Discovery Resource	P2-CC-1: Mandatory	na
Common Connection	Get API Root	P2-CC-2: Mandatory	na
Common Connection	Missing Authorization Parameter	P2-CC-3: Mandatory	na
Common Connection	Incorrect Authorization Parameter Returns Unauthorized	P2-CC-4: Mandatory	na

Common Connection	Incorrect API Root Info Get Returns Not Found	P2-CC-5: Mandatory	na
Common Connection	Incorrect Collection Info Get Returns Not Found	P2-CC-6: Mandatory	na
Basic Feed Sharing	Verify Collection Information	Mandatory	na
Basic Feed Sharing	Indicator IPv4 Address	P2-BF-2-A & P2-BF-2-B: Mandatory	na
Basic Feed Sharing	Indicator IPv4 Address CIDR	P2-BF-3-A & P2-BF-3-B: Mandatory	na
Basic Feed Sharing	Two Indicators with IPv4 Address CIDR	P2-BF-4-A & P2-BF-4-B: Mandatory	na
Basic Feed Sharing	Indicator with IPv6 Address	P2-BF-5-A & P2-BF-5-B: Optional	na
Basic Feed Sharing	Indicator with IPv6 Address CIDR	P2-BF-6-A & P2-BF-6-B: Optional	na
Basic Feed Sharing	Multiple Indicators in same bundle	P2-BF-7-A & P2-BF-7-B: Mandatory	na
Basic Feed Sharing	Indicator FQDN	P2-BF-8-A & P2-BF-8-B: Mandatory	na
Basic Feed Sharing	Indicator URL	P2-BF-9-A & P2-BF-9-B: Mandatory	na
Basic Feed Sharing	Indicator URL or FQDN	P2-BF-10-A & P2-BF-10-B: Mandatory	na
Basic Feed Sharing	Indicator File hash with SHA256 or MD5 values	P2-BF-11-A & P2-BF-11-B: Mandatory	na
Basic Intel Collaboration	Verify Collection Information	P2-IC-1-A & P2-IC-2-B: Mandatory	na

Basic Intel Collaboration	Indicator IPv4 Address	P2-IC-2-A & P2-IC-2-B: Mandatory	na
Basic Intel Collaboration	Indicator IPv4 Address CIDR	P2-IC-3-A & P2-IC-3-B: Mandatory	na
Basic Intel Collaboration	Two Indicators with IPv4 Address CIDR	P2-IC-4-A & P2-IC-4-B: Mandatory	na
Basic Intel Collaboration	Indicator with IPv6 Address	P2-IC-5-A & P2-IC-5-B: Optional	na
Basic Intel Collaboration	Indicator with IPv6 Address CIDR	P2-IC-6-A & P2-IC-6-B: Optional	na
Basic Intel Collaboration	Multiple Indicators within the same bundle	P2-IC-7-A & P2-IC-7-B: Mandatory	na
Basic Intel Collaboration	Indicator FQDN	P2-IC-8-A & P2-IC-8-B: Mandatory	na
Basic Intel Collaboration	Indicator URL	P2-IC-9-A & P2-IC-9-B: Mandatory	na
Basic Intel Collaboration	Indicator URL or FQDN	P2-IC-10-A & P2-IC-10-B: Mandatory	na
Basic Intel Collaboration	Indicator File hash with SHA256 or MD5 values	P2-IC-11-A & P2-IC-11-B: Mandatory	na

3.3 Threat Intelligence Platform (TIP)

For the purpose of this document a TIP is defined as a 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.

Any software instance being qualified as a TIP must confirm test results for the following tests.

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

Test Case	Test	Verification	Results
Indicator Sharing	2.2.3.1 Indicator IPv4 Address	Mandatory	<fill in>

Indicator Sharing	2.2.3.2 Indicator IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	2.2.3.3 Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	2.2.3.4 Indicator with IPv6 Address	Optional	<if supported, fill in>
Indicator Sharing	2.2.3.5 Indicator with IPv6 Address CIDR	Optional	<if supported, fill in>
Indicator Sharing	2.2.3.6 Multiple Indicators within the same bundle	Mandatory	<fill in>
Indicator Sharing	2.2.3.7 Indicator FQDN	Mandatory	<fill in>
Indicator Sharing	2.2.3.8 Indicator URL	Mandatory	<fill in>
Indicator Sharing	2.2.3.9 Indicator URL or FQDN	Mandatory	<fill in>
Indicator Sharing	2.2.3.10 Indicator File hash with SHA256 or MD5 values	Mandatory	<fill in>
Sighting Sharing	2.3.3 Producer Test Case Data	Mandatory	<fill in>
Sighting Sharing	2.3.5.1 Sighting + Indicator with IPv4 Address	Mandatory	<fill in>
Sighting Sharing	2.3.5.2 Sighting + Indicator with IPv4 Address Matching CIDR	Mandatory	<fill in>
Sighting Sharing	2.3.5.3 Sighting + Indicator with IPv6 Address Matching CIDR	Optional	<if supported, fill in>
Sighting Sharing	2.3.5.4 Sighting + Indicator with NO observed data	Mandatory	<fill in>
Sighting Sharing	2.3.5.5 Sighting + Indicator with URL	Mandatory	<fill in>
Sighting Sharing	2.3.5.6 Sighting + Indicator with File Hash	Mandatory	<fill in>
Versioning	2.4.3.1 Creation of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	2.4.3.2 Creation of a Sighting with Identity and Date	Mandatory	<fill in>
Versioning	2.4.7.1 Modification of an Indicator with Identity and Date	Mandatory	<fill in>

Versioning	2.4.7.2 Modification of a Sighting with Identity and Date	Mandatory	<fill in>
Versioning	2.4.11.1 Deletion of an Indicator with Identity; Dates	Mandatory	<fill in>
Versioning	2.4.11.2 Deletion of a Sighting and Associated Observed Data	Mandatory	<fill in>
Data Markings	2.5.3.1 TLP Green + Indicator with IPv4 Address	Mandatory	<fill in>
Data Markings	2.5.3.2 TLP Amber + Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Data Markings	2.5.3.3 TLP White and TLP Red + Indicator with IPv6 Address	Optional	<fill in>
Data Markings	2.5.3.4 TLP Red + Sighting and Indicator	Optional	<fill in>
Custom Object Creation	2.6.3.1 Custom Object Creation	Optional	<if supported, fill in>
Custom Property Creation	2.6.3.2 Custom Property Creation	Optional	<if supported, fill in>
Custom Ingestion	2.6.4 Required Respondent Support	Mandatory	<fill in>
Create COA	2.7.3.1 Create COA	Optional	<if supported, fill in>
Create COA Relationship	2.7.3.2 Create COA with Relationship	Optional	<if supported, fill in>

Table 3.3.2 - Threat Intelligence Platform (TIP) Part 2 Test Verification List

(P == Producer; R == Respondent; M == Mandatory; O == Optional; UC# = Test Case#)

Test Case	Test	Producer	Respondent
Common Connection	Get Discovery Resource	P2-CC-1: Mandatory	P2-CC-1: Mandatory
Common Connection	Get API Root	P2-CC-2: Mandatory	P2-CC-2: Mandatory
Common	Missing Authorization Parameter	P2-CC-3:	P2-CC-3:

Connection		Mandatory	Mandatory
Common Connection	Incorrect Authorization Parameter Returns Unauthorized	P2-CC-4: Mandatory	P2-CC-4: Mandatory
Common Connection	Incorrect API Root Info Get Returns Not Found	P2-CC-5: Mandatory	P2-CC-5: Mandatory
Common Connection	Incorrect Collection Info Get Returns Not Found	P2-CC-6: Mandatory	P2-CC-6: Mandatory
Basic Feed Sharing	Verify Collection Information	P2-BF-1: Mandatory	P2-BF-1: Mandatory
Basic Feed Sharing	Indicator IPv4 Address	P2-BF-2-A & P2-BF-2-B: Mandatory	P2-BF-12-A & P2-BF-12-B & P2-BF-12-C: Mandatory
Basic Feed Sharing	Indicator IPv4 Address CIDR	P2-BF-3-A & P2-BF-3-B: Mandatory	P2-BF-13-A & P2-BF-13-B & P2-BF-13-C: Mandatory
Basic Feed Sharing	Two Indicators with IPv4 Address CIDR	P2-BF-4-A & P2-BF-4-B: Mandatory	P2-BF-14-A & P2-BF-14-B & P2-BF-14-C: Mandatory
Basic Feed Sharing	Indicator with IPv6 Address	P2-BF-5-A & P2-BF-5-B: Optional	P2-BF-15-A & P2-BF-15-B & P2-BF-15-C: Optional
Basic Feed Sharing	Indicator with IPv6 Address CIDR	P2-BF-6-A & P2-BF-6-B: Optional	P2-BF-16-A & P2-BF-16-B & P2-BF-16-C: Optional
Basic Feed Sharing	Multiple Indicators in same bundle	P2-BF-7-A & P2-BF-7-B: Mandatory	P2-BF-17-A & P2-BF-17-B & P2-BF-17-C: Mandatory
Basic Feed Sharing	Indicator FQDN	P2-BF-8-A & P2-BF-8-B: Mandatory	P2-BF-18-A & P2-BF-18-B & P2-BF-18-C: Mandatory

Basic Feed Sharing	Indicator URL	P2-BF-9-A & P2-BF-9-B: Mandatory	P2-BF-19-A & P2-BF-19-B & P2-BF-19-C: Mandatory
Basic Feed Sharing	Indicator URL or FQDN	P2-BF-10-A & P2-BF-10-B: Mandatory	P2-BF-20-A & P2-BF-20-B & P2-BF-20-C: Mandatory
Basic Feed Sharing	Indicator File hash with SHA256 or MD5 values	P2-BF-11-A & P2-BF-11-B: Mandatory	P2-BF-21-A & P2-BF-21-B & P2-BF-21-C: Mandatory
Basic Intel Collaboration	Verify Collection Information	P2-IC-1-A & P2-IC-2-B: Mandatory	P2-IC-1-A & P2-IC-2-B: Mandatory
Basic Intel Collaboration	Indicator IPv4 Address	P2-IC-2-A & P2-IC-2-B: Mandatory	P2-IC-12-A & P2-IC-12-B & P2-IC-22-A & P2-IC-22-B: M
Basic Intel Collaboration	Indicator IPv4 Address CIDR	P2-IC-3-A & P2-IC-3-B: Mandatory	P2-IC-13-A & P2-IC-13-B & P2-IC-23-A & P2-IC-23-B: M
Basic Intel Collaboration	Two Indicators with IPv4 Address CIDR	P2-IC-4-A & P2-IC-4-B: Mandatory	P2-IC-14-A & P2-IC-14-B & P2-IC-24-A & P2-IC-24-B: M
Basic Intel Collaboration	Indicator with IPv6 Address	P2-IC-5-A & P2-IC-5-B: Optional	P2-IC-15-A & P2-IC-15-B & P2-IC-25-A & P2-IC-25-B: O
Basic Intel Collaboration	Indicator with IPv6 Address CIDR	P2-IC-6-A & P2-IC-6-B: Optional	P2-IC-16-A & P2-IC-16-B & P2-IC-26-A & P2-IC-26-B: O
Basic Intel Collaboration	Multiple Indicators within the same bundle	P2-IC-7-A & P2-IC-7-B: Mandatory	P2-IC-17-A & P2-IC-17-B & P2-IC-27-A & P2-IC-27-B: M

Basic Intel Collaboration	Indicator FQDN	P2-IC-8-A & P2-IC-8-B: Mandatory	P2-IC-18-A & P2-IC-18-B & P2-IC-28-A & P2-IC-28-B: M
Basic Intel Collaboration	Indicator URL	P2-IC-9-A & P2-IC-9-B: Mandatory	P2-IC-19-A & P2-IC-19-B & P2-IC-29-A & P2-IC-29-B: M
Basic Intel Collaboration	Indicator URL or FQDN	P2-IC-10-A & P2-IC-10-B: Mandatory	P2-IC-20-A & P2-IC-20-B & P2-IC-30-A & P2-IC-30-B: M
Basic Intel Collaboration	Indicator File hash with SHA256 or MD5 values	P2-IC-11-A & P2-IC-11-B: Mandatory	P2-IC-21-A & P2-IC-21-B & P2-IC-31-A & P2-IC-31-B: M

3.4 Security Incident and Event Management (SIEM)

For the purpose of this document a SIEM is defined as a software instance that acts as a producer and/or Respondent of STIX 2.0 content. The primary Respondent role of a SIEM is to report indicators and high-level information. The primary producer role of a SIEM is with respect to incidents, observations, and sightings.

Any software instance being qualified as a SIEM must confirm test results for the following tests.

Table 3.4.1 - Security Incident and Event Management (SIEM) Part 1 Test Verification List

Test Case	Test	Verification	Results
Indicator Sharing	2.2.3.1 Indicator IPv4 Address	Mandatory	<fill in>
Indicator Sharing	2.2.3.2 Indicator IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	2.2.3.3 Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	2.2.3.4 Indicator with IPv6 Address	Optional	<if supported, fill in>
Indicator Sharing	2.2.3.5 Indicator with IPv6 Address CIDR	Optional	<if supported, fill in>

Indicator Sharing	2.2.3.6 Multiple Indicators within the same bundle	Mandatory	<fill in>
Indicator Sharing	2.2.3.7 Indicator FQDN	Mandatory	<fill in>
Indicator Sharing	2.2.3.8 Indicator URL	Mandatory	<fill in>
Indicator Sharing	2.2.3.9 Indicator URL or FQDN	Mandatory	<fill in>
Indicator Sharing	2.2.3.10 Indicator File hash with SHA256 or MD5 values	Mandatory	<fill in>
Sighting Sharing	2.3.3 Producer Test Case Data	Optional	<fill in>
Sighting Sharing	2.3.5.1 Sighting + Indicator with IPv4 Address	Mandatory	<fill in>
Sighting Sharing	2.3.5.2 Sighting + Indicator with IPv4 Address Matching CIDR	Mandatory	<fill in>
Sighting Sharing	2.3.5.3 Sighting + Indicator with IPv6 Address Matching CIDR	Optional	<if supported, fill in>
Sighting Sharing	2.3.5.4 Sighting + Indicator with NO observed data	Mandatory	<fill in>
Sighting Sharing	2.3.5.5 Sighting + Indicator with URL	Mandatory	<fill in>
Sighting Sharing	2.3.5.6 Sighting + Indicator with File Hash	Mandatory	<fill in>
Versioning	2.4.3.1 Creation of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	2.4.3.2 Creation of a Sighting with Identity and Date	Mandatory	<fill in>
Versioning	2.4.7.1 Modification of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	2.4.7.2 Modification of a Sighting with Identity and Date	Mandatory	<fill in>
Versioning	2.4.11.1 Deletion of an Indicator with Identity; Dates	Mandatory	<fill in>

Versioning	2.4.11.2 Deletion of a Sighting and Associated Observed Data	Mandatory	<fill in>
Data Markings	2.5.3.1 TLP Green + Indicator with IPv4 Address	Mandatory	<fill in>
Data Markings	2.5.3.2 TLP Amber + Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Data Markings	2.5.3.3 TLP White and TLP Red + Indicator with IPv6 Address	Optional	<fill in>
Data Markings	2.5.3.4 TLP Red + Sighting and Indicator	Optional	<fill in>
Custom Object Creation	2.6.3.1 Custom Object Creation	Optional	<if supported, fill in>
Custom Property Creation	2.6.3.2 Custom Property Creation	Optional	<if supported, fill in>
Custom Ingestion	2.6.4 Required Respondent Support	Mandatory	<fill in>
Create COA	2.7.3.1 Create COA	Optional	<if supported, fill in>
Create COA Relationship	2.7.3.2 Create COA with Relationship	Optional	<if supported, fill in>

Table 3.4.2 - Security Incident and Event Management (SIEM) Part 2 Test Verification List

(P == Producer; R == Respondent; M == Mandatory; O == Optional; UC# = Test Case#)

Test Case	Test	Producer	Respondent
Common Connection	Get Discovery Resource	P2-CC-1: Mandatory	P2-CC-1: Mandatory
Common Connection	Get API Root	P2-CC-2: Mandatory	P2-CC-2: Mandatory
Common Connection	Missing Authorization Parameter	P2-CC-3: Mandatory	P2-CC-3: Mandatory
Common Connection	Incorrect Authorization Parameter Returns Unauthorized	P2-CC-4: Mandatory	P2-CC-4: Mandatory
Common Connection	Incorrect API Root Info Get Returns Not Found	P2-CC-5: Mandatory	P2-CC-5: Mandatory

Common Connection	Incorrect Collection Info Get Returns Not Found	P2-CC-6: Mandatory	P2-CC-6: Mandatory
Basic Feed Sharing	Verify Collection Information	P2-BF-1: Mandatory	P2-BF-1: Mandatory
Basic Feed Sharing	Indicator IPv4 Address	P2-BF-2-A & P2-BF-2-B: Mandatory	P2-BF-12-A & P2-BF-12-B & P2-BF-12-C: Mandatory
Basic Feed Sharing	Indicator IPv4 Address CIDR	P2-BF-3-A & P2-BF-3-B: Mandatory	P2-BF-13-A & P2-BF-13-B & P2-BF-13-C: Mandatory
Basic Feed Sharing	Two Indicators with IPv4 Address CIDR	P2-BF-4-A & P2-BF-4-B: Mandatory	P2-BF-14-A & P2-BF-14-B & P2-BF-14-C: Mandatory
Basic Feed Sharing	Indicator with IPv6 Address	P2-BF-5-A & P2-BF-5-B: Optional	P2-BF-15-A & P2-BF-15-B & P2-BF-15-C: Optional
Basic Feed Sharing	Indicator with IPv6 Address CIDR	P2-BF-6-A & P2-BF-6-B: Optional	P2-BF-16-A & P2-BF-16-B & P2-BF-16-C: Optional
Basic Feed Sharing	Multiple Indicators in same bundle	P2-BF-7-A & P2-BF-7-B: Mandatory	P2-BF-17-A & P2-BF-17-B & P2-BF-17-C: Mandatory
Basic Feed Sharing	Indicator FQDN	P2-BF-8-A & P2-BF-8-B: Mandatory	P2-BF-18-A & P2-BF-18-B & P2-BF-18-C: Mandatory
Basic Feed Sharing	Indicator URL	P2-BF-9-A & P2-BF-9-B: Mandatory	P2-BF-19-A & P2-BF-19-B & P2-BF-19-C: Mandatory
Basic Feed Sharing	Indicator URL or FQDN	P2-BF-10-A & P2-BF-10-B: Mandatory	P2-BF-20-A & P2-BF-20-B & P2-BF-20-C:

			Mandatory
Basic Feed Sharing	Indicator File hash with SHA256 or MD5 values	P2-BF-11-A & P2-BF-11-B: Mandatory	P2-BF-21-A & P2-BF-21-B & P2-BF-21-C: Mandatory
Basic Intel Collaboration	Verify Collection Information	P2-IC-1-A & P2-IC-2-B: Mandatory	P2-IC-1-A & P2-IC-2-B: Mandatory
Basic Intel Collaboration	Indicator IPv4 Address	P2-IC-2-A & P2-IC-2-B: Mandatory	P2-IC-12-A & P2-IC-12-B & P2-IC-22-A & P2-IC-22-B: M
Basic Intel Collaboration	Indicator IPv4 Address CIDR	P2-IC-3-A & P2-IC-3-B: Mandatory	P2-IC-13-A & P2-IC-13-B & P2-IC-23-A & P2-IC-23-B: M
Basic Intel Collaboration	Two Indicators with IPv4 Address CIDR	P2-IC-4-A & P2-IC-4-B: Mandatory	P2-IC-14-A & P2-IC-14-B & P2-IC-24-A & P2-IC-24-B: M
Basic Intel Collaboration	Indicator with IPv6 Address	P2-IC-5-A & P2-IC-5-B: Optional	P2-IC-15-A & P2-IC-15-B & P2-IC-25-A & P2-IC-25-B: O
Basic Intel Collaboration	Indicator with IPv6 Address CIDR	P2-IC-6-A & P2-IC-6-B: Optional	P2-IC-16-A & P2-IC-16-B & P2-IC-26-A & P2-IC-26-B: O
Basic Intel Collaboration	Multiple Indicators within the same bundle	P2-IC-7-A & P2-IC-7-B: Mandatory	P2-IC-17-A & P2-IC-17-B & P2-IC-27-A & P2-IC-27-B: M
Basic Intel Collaboration	Indicator FQDN	P2-IC-8-A & P2-IC-8-B: Mandatory	P2-IC-18-A & P2-IC-18-B & P2-IC-28-A & P2-IC-28-B: M

Basic Intel Collaboration	Indicator URL	P2-IC-9-A & P2-IC-9-B: Mandatory	P2-IC-19-A & P2-IC-19-B & P2-IC-29-A & P2-IC-29-B: M
Basic Intel Collaboration	Indicator URL or FQDN	P2-IC-10-A & P2-IC-10-B: Mandatory	P2-IC-20-A & P2-IC-20-B & P2-IC-30-A & P2-IC-30-B: M
Basic Intel Collaboration	Indicator File hash with SHA256 or MD5 values	P2-IC-11-A & P2-IC-11-B: Mandatory	P2-IC-21-A & P2-IC-21-B & P2-IC-31-A & P2-IC-31-B: M

3.5 Threat Mitigation System (TMS)

For the purpose of this document, a TMS is a software instance that mitigates threats in a network. For some of the test test cases, it may act as both a Producer and Respondent. The Respondent TMS primarily consumes and acts on Indicators. The Producer TMS primarily reports sightings.

Any software instance being qualified as a TMS must confirm test results for the following test cases.

Table 3.5.1 - Threat Mitigation System (TMS) Part 1 Test Verification List

Test Case	Test	Verification	Results
Indicator Sharing	2.2.3.1 Indicator IPv4 Address	Mandatory	<fill in>
Indicator Sharing	2.2.3.2 Indicator IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	2.2.3.3 Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	2.2.3.4 Indicator with IPv6 Address	Optional	<if supported, fill in>
Indicator Sharing	2.2.3.5 Indicator with IPv6 Address CIDR	Optional	<if supported, fill in>
Indicator Sharing	2.2.3.6 Multiple Indicators within the same bundle	Mandatory	<fill in>
Indicator Sharing	2.2.3.7 Indicator FQDN	Mandatory	<fill in>
Indicator Sharing	2.2.3.8 Indicator URL	Mandatory	<fill in>
Indicator Sharing	2.2.3.9 Indicator URL or FQDN	Mandatory	<fill in>

Indicator Sharing	2.2.3.10 Indicator File hash with SHA256 or MD5 values	Mandatory	<fill in>
Sighting Sharing	2.3.3 Producer Test Case Data	Mandatory	<fill in>
Sighting Sharing	2.3.5.1 Sighting + Indicator with IPv4 Address	Mandatory	<fill in>
Sighting Sharing	2.3.5.2 Sighting + Indicator with IPv4 Address Matching CIDR	Mandatory	<fill in>
Sighting Sharing	2.3.5.3 Sighting + Indicator with IPv6 Address Matching CIDR	Optional	<if supported, fill in>
Sighting Sharing	2.3.5.4 Sighting + Indicator with NO observed data	Mandatory	<fill in>
Sighting Sharing	2.3.5.5 Sighting + Indicator with URL	Mandatory	<fill in>
Sighting Sharing	2.3.5.6 Sighting + Indicator with File Hash	Mandatory	<fill in>
Versioning	2.4.3.1 Creation of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	2.4.3.2 Creation of a Sighting with Identity and Date	Mandatory	<fill in>
Versioning	2.4.7.1 Modification of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	2.4.7.2 Modification of a Sighting with Identity and Date	Mandatory	<fill in>
Versioning	2.4.11.1 Deletion of an Indicator with Identity; Dates	Mandatory	<fill in>
Versioning	2.4.11.2 Deletion of a Sighting and Associated Observed Data	Mandatory	<fill in>
Data Markings	2.5.3.1 TLP Green + Indicator with IPv4 Address	Mandatory	<fill in>
Data Markings	2.5.3.2 TLP Amber + Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>

Data Markings	2.5.3.3 TLP White and TLP Red + Indicator with IPv6 Address	Optional	<fill in>
Data Markings	2.5.3.4 TLP Red + Sighting and Indicator	Optional	<fill in>
Custom Object Creation	2.6.3.1 Custom Object Creation	Optional	<if supported, fill in>
Custom Property Creation	2.6.3.2 Custom Property Creation	Optional	<if supported, fill in>
Custom Ingestion	2.6.4 Required Respondent Support	Mandatory	<fill in>
Create COA	2.7.3.1 Create COA	Optional	<if supported, fill in>
Create COA Relationship	2.7.3.2 Create COA with Relationship	Optional	<if supported, fill in>

Table 3.5.2 - Threat Mitigation System (TMS) Part 2 Test Verification List

(P == Producer; R == Respondent; M == Mandatory; O == Optional; UC# = Test Case#)

Test Case	Test	Producer	Respondent
Common Connection	Get Discovery Resource	na	P2-CC-1: Mandatory
Common Connection	Get API Root	na	P2-CC-2: Mandatory
Common Connection	Missing Authorization Parameter	na	P2-CC-3: Mandatory
Common Connection	Incorrect Authorization Parameter Returns Unauthorized	na	P2-CC-4: Mandatory
Common Connection	Incorrect API Root Info Get Returns Not Found	na	P2-CC-5: Mandatory
Common Connection	Incorrect Collection Info Get Returns Not Found	na	P2-CC-6: Mandatory
Basic Feed Sharing	Verify Collection Information	na	P2-BF-1: Mandatory
Basic Feed Sharing	Indicator IPv4 Address	na	P2-BF-12-A & P2-BF-12-B &

			P2-BF-12-C: Mandatory
Basic Feed Sharing	Indicator IPv4 Address CIDR	na	P2-BF-13-A & P2-BF-13-B & P2-BF-13-C: Mandatory
Basic Feed Sharing	Two Indicators with IPv4 Address CIDR	na	P2-BF-14-A & P2-BF-14-B & P2-BF-14-C: Mandatory
Basic Feed Sharing	Indicator with IPv6 Address	na	P2-BF-15-A & P2-BF-15-B & P2-BF-15-C: Optional
Basic Feed Sharing	Indicator with IPv6 Address CIDR	na	P2-BF-16-A & P2-BF-16-B & P2-BF-16-C: Optional
Basic Feed Sharing	Multiple Indicators in same bundle	na	P2-BF-17-A & P2-BF-17-B & P2-BF-17-C: Mandatory
Basic Feed Sharing	Indicator FQDN	na	P2-BF-18-A & P2-BF-18-B & P2-BF-18-C: Mandatory
Basic Feed Sharing	Indicator URL	na	P2-BF-19-A & P2-BF-19-B & P2-BF-19-C: Mandatory
Basic Feed Sharing	Indicator URL or FQDN	na	P2-BF-20-A & P2-BF-20-B & P2-BF-20-C: Mandatory
Basic Feed Sharing	Indicator File hash with SHA256 or MD5 values	na	P2-BF-21-A & P2-BF-21-B & P2-BF-21-C: Mandatory
Basic Intel	Verify Collection Information	na	na

Collaboration			
Basic Intel Collaboration	Indicator IPv4 Address	na	na
Basic Intel Collaboration	Indicator IPv4 Address CIDR	na	na
Basic Intel Collaboration	Two Indicators with IPv4 Address CIDR	na	na
Basic Intel Collaboration	Indicator with IPv6 Address	na	na
Basic Intel Collaboration	Indicator with IPv6 Address CIDR	na	na
Basic Intel Collaboration	Multiple Indicators within the same bundle	na	na
Basic Intel Collaboration	Indicator FQDN	na	na
Basic Intel Collaboration	Indicator URL	na	na
Basic Intel Collaboration	Indicator URL or FQDN	na	na
Basic Intel Collaboration	Indicator File hash with SHA256 or MD5 values	na	na

3.6 Threat Detection System (TDS)

For the purpose of this document a TDS detects threats in a network and may or may not mitigate them. It may act as both a Producer and Respondent depending on the type of test case. The Respondent is primarily concerned with indicators. The Producer role is primarily concerned with sightings.

Any software instance being qualified as a TMS must confirm test results for the following test cases.

Table 3.6.1 - Threat Detection System (TMS) Part 1 Test Verification List

Test Case	Test	Verification	Results

Indicator Sharing	2.2.3.1 Indicator IPv4 Address	Mandatory	<fill in>
Indicator Sharing	2.2.3.2 Indicator IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	2.2.3.3 Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	2.2.3.4 Indicator with IPv6 Address	Optional	<if supported, fill in>
Indicator Sharing	2.2.3.5 Indicator with IPv6 Address CIDR	Optional	<if supported, fill in>
Indicator Sharing	2.2.3.6 Multiple Indicators within the same bundle	Mandatory	<fill in>
Indicator Sharing	2.2.3.7 Indicator FQDN	Mandatory	<fill in>
Indicator Sharing	2.2.3.8 Indicator URL	Mandatory	<fill in>
Indicator Sharing	2.2.3.9 Indicator URL or FQDN	Mandatory	<fill in>
Indicator Sharing	2.2.3.10 Indicator File hash with SHA256 or MD5 values	Mandatory	<fill in>
Sighting Sharing	2.3.3 Producer Test Case Data	Mandatory	<fill in>
Sighting Sharing	2.3.5.1 Sighting + Indicator with IPv4 Address	Mandatory	<fill in>
Sighting Sharing	2.3.5.2 Sighting + Indicator with IPv4 Address Matching CIDR	Mandatory	<fill in>
Sighting Sharing	2.3.5.3 Sighting + Indicator with IPv6 Address Matching CIDR	Optional	<if supported, fill in>
Sighting Sharing	2.3.5.4 Sighting + Indicator with NO observed data	Mandatory	<fill in>
Sighting Sharing	2.3.5.5 Sighting + Indicator with URL	Mandatory	<fill in>
Sighting Sharing	2.3.5.6 Sighting + Indicator with File Hash	Mandatory	<fill in>
Versioning	2.4.3.1 Creation of an Indicator with Identity and Date	Mandatory	<fill in>

Versioning	2.4.3.2 Creation of a Sighting with Identity and Date	Mandatory	<fill in>
Versioning	2.4.7.1 Modification of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	2.4.7.2 Modification of a Sighting with Identity and Date	Mandatory	<fill in>
Versioning	2.4.11.1 Deletion of an Indicator with Identity; Dates	Mandatory	<fill in>
Versioning	2.4.11.2 Deletion of a Sighting and Associated Observed Data	Mandatory	<fill in>
Data Markings	2.5.3.1 TLP Green + Indicator with IPv4 Address	Mandatory	<fill in>
Data Markings	2.5.3.2 TLP Amber + Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Data Markings	2.5.3.3 TLP White and TLP Red + Indicator with IPv6 Address	Optional	<fill in>
Data Markings	2.5.3.4 TLP Red + Sighting and Indicator	Optional	<fill in>
Custom Object Creation	2.6.3.1 Custom Object Creation	Optional	<if supported, fill in>
Custom Property Creation	2.6.3.2 Custom Property Creation	Optional	<if supported, fill in>
Custom Ingestion	2.6.4 Required Respondent Support	Mandatory	<fill in>
Create COA	2.7.3.1 Create COA	Optional	<if supported, fill in>
Create COA Relationship	2.7.3.2 Create COA with Relationship	Optional	<if supported, fill in>

Table 3.6.2 - Threat Detection System (TDS) Part 2 Test Verification List

(P == Producer; R == Respondent; M == Mandatory; O == Optional; UC# = Test Case#)

Test Case	Test	Producer	Respondent
Common Connection	Get Discovery Resource	na	P2-CC-1: Mandatory

Common Connection	Get API Root	na	P2-CC-2: Mandatory
Common Connection	Missing Authorization Parameter	na	P2-CC-3: Mandatory
Common Connection	Incorrect Authorization Parameter Returns Unauthorized	na	P2-CC-4: Mandatory
Common Connection	Incorrect API Root Info Get Returns Not Found	na	P2-CC-5: Mandatory
Common Connection	Incorrect Collection Info Get Returns Not Found	na	P2-CC-6: Mandatory
Basic Feed Sharing	Verify Collection Information	na	P2-BF-1: Mandatory
Basic Feed Sharing	Indicator IPv4 Address	na	P2-BF-12-A & P2-BF-12-B & P2-BF-12-C: Mandatory
Basic Feed Sharing	Indicator IPv4 Address CIDR	na	P2-BF-13-A & P2-BF-13-B & P2-BF-13-C: Mandatory
Basic Feed Sharing	Two Indicators with IPv4 Address CIDR	na	P2-BF-14-A & P2-BF-14-B & P2-BF-14-C: Mandatory
Basic Feed Sharing	Indicator with IPv6 Address	na	P2-BF-15-A & P2-BF-15-B & P2-BF-15-C: Optional
Basic Feed Sharing	Indicator with IPv6 Address CIDR	na	P2-BF-16-A & P2-BF-16-B & P2-BF-16-C: Optional
Basic Feed Sharing	Multiple Indicators in same bundle	na	P2-BF-17-A & P2-BF-17-B & P2-BF-17-C: Mandatory
Basic Feed	Indicator FQDN	na	P2-BF-18-A &

Sharing			P2-BF-18-B & P2-BF-18-C: Mandatory
Basic Feed Sharing	Indicator URL	na	P2-BF-19-A & P2-BF-19-B & P2-BF-19-C: Mandatory
Basic Feed Sharing	Indicator URL or FQDN	na	P2-BF-20-A & P2-BF-20-B & P2-BF-20-C: Mandatory
Basic Feed Sharing	Indicator File hash with SHA256 or MD5 values	na	P2-BF-21-A & P2-BF-21-B & P2-BF-21-C: Mandatory
Basic Intel Collaboration	Verify Collection Information	na	na
Basic Intel Collaboration	Indicator IPv4 Address	na	na
Basic Intel Collaboration	Indicator IPv4 Address CIDR	na	na
Basic Intel Collaboration	Two Indicators with IPv4 Address CIDR	na	na
Basic Intel Collaboration	Indicator with IPv6 Address	na	na
Basic Intel Collaboration	Indicator with IPv6 Address CIDR	na	na
Basic Intel Collaboration	Multiple Indicators within the same bundle	na	na
Basic Intel Collaboration	Indicator FQDN	na	na
Basic Intel Collaboration	Indicator URL	na	na

Basic Intel Collaboration	Indicator URL or FQDN	na	na
Basic Intel Collaboration	Indicator File hash with SHA256 or MD5 values	na	na

3.7 Threat intelligence Sink (TIS)

For the purpose of this document, a (TIS) is a software instance that consumes STIX 2.0 content in order to perform translations to domain specific formats. Those translations are consumable by enforcement and/or detection systems that do not natively support STIX 2.0. These TIS consumers may or may not have the capability of reporting sightings. A (TIS) that consumes STIX content will typically consume indicators.

Any software instance being qualified as a (TIS) must confirm test results for the following test cases.

Table 3.7.1 — Threat Intelligence Sink (TIS) Part 1 Test Verification List

Test Case	Test	Verification	Results
Indicator Sharing	2.2.3.1 Indicator IPv4 Address	Mandatory	<fill in>
Indicator Sharing	2.2.3.2 Indicator IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	2.2.3.3 Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	2.2.3.4 Indicator with IPv6 Address	Optional	<if supported, fill in>
Indicator Sharing	2.2.3.5 Indicator with IPv6 Address CIDR	Optional	<if supported, fill in>
Indicator Sharing	2.2.3.6 Multiple Indicators within the same bundle	Mandatory	<fill in>
Indicator Sharing	2.2.3.7 Indicator FQDN	Mandatory	<fill in>
Indicator Sharing	2.2.3.8 Indicator URL	Mandatory	<fill in>
Indicator Sharing	2.2.3.9 Indicator URL or FQDN	Mandatory	<fill in>

Indicator Sharing	2.2.3.10 Indicator File hash with SHA256 or MD5 values	Mandatory	<fill in>
Sighting Sharing	2.3.3 Producer Test Case Data	Optional	<fill in>
Sighting Sharing	2.3.5.1 Sighting + Indicator with IPv4 Address	Optional	<fill in>
Sighting Sharing	2.3.5.2 Sighting + Indicator with IPv4 Address Matching CIDR	Optional	<fill in>
Sighting Sharing	2.3.5.3 Sighting + Indicator with IPv6 Address Matching CIDR	Optional	<if supported, fill in>
Sighting Sharing	2.3.5.4 Sighting + Indicator with NO observed data	Optional	<fill in>
Sighting Sharing	2.3.5.5 Sighting + Indicator with URL	Optional	<fill in>
Sighting Sharing	2.3.5.6 Sighting + Indicator with File Hash	Optional	<fill in>
Versioning	2.4.3.1 Creation of an Indicator with Identity and Date	Optional	<fill in>
Versioning	2.4.3.2 Creation of a Sighting with Identity and Date	Optional	<fill in>
Versioning	2.4.7.1 Modification of an Indicator with Identity and Date	Optional	<fill in>
Versioning	2.4.7.2 Modification of a Sighting with Identity and Date	Optional	<fill in>
Versioning	2.4.11.1 Deletion of an Indicator with Identity; Dates	Optional	<fill in>
Versioning	2.4.11.2 Deletion of a Sighting and Associated Observed Data	Optional	<fill in>
Data Markings	2.5.3.1 TLP Green + Indicator with IPv4 Address	Mandatory	<fill in>
Data Markings	2.5.3.2 TLP Amber + Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>

Data Markings	2.5.3.3 TLP White and TLP Red + Indicator with IPv6 Address	Optional	<fill in>
Data Markings	2.5.3.4 TLP Red + Sighting and Indicator	Optional	<fill in>
Custom Object Creation	2.6.3.1 Custom Object Creation	Optional	<if supported, fill in>
Custom Property Creation	2.6.3.2 Custom Property Creation	Optional	<if supported, fill in>
Custom Ingestion	2.6.4 Required Respondent Support	Mandatory	<fill in>
Create COA	2.7.3.1 Create COA	Optional	<if supported, fill in>
Create COA Relationship	2.7.3.2 Create COA with Relationship	Optional	<if supported, fill in>

Table 3.7.2 - Threat Intelligence Sink (TIS) Part 2 Test Verification List

(P == Producer; R == Respondent; M == Mandatory; O == Optional; UC# = Test Case#)

Test Case	Test	Producer	Respondent
Common Connection	Get Discovery Resource	na	P2-CC-1: Mandatory
Common Connection	Get API Root	na	P2-CC-2: Mandatory
Common Connection	Missing Authorization Parameter	na	P2-CC-3: Mandatory
Common Connection	Incorrect Authorization Parameter Returns Unauthorized	na	P2-CC-4: Mandatory
Common Connection	Incorrect API Root Info Get Returns Not Found	na	P2-CC-5: Mandatory
Common Connection	Incorrect Collection Info Get Returns Not Found	na	P2-CC-6: Mandatory
Basic Feed Sharing	Verify Collection Information	na	P2-BF-1: Mandatory
Basic Feed Sharing	Indicator IPv4 Address	na	P2-BF-12-A & P2-BF-12-B &

			P2-BF-12-C: Mandatory
Basic Feed Sharing	Indicator IPv4 Address CIDR	na	P2-BF-13-A & P2-BF-13-B & P2-BF-13-C: Mandatory
Basic Feed Sharing	Two Indicators with IPv4 Address CIDR	na	P2-BF-14-A & P2-BF-14-B & P2-BF-14-C: Mandatory
Basic Feed Sharing	Indicator with IPv6 Address	na	P2-BF-15-A & P2-BF-15-B & P2-BF-15-C: Optional
Basic Feed Sharing	Indicator with IPv6 Address CIDR	na	P2-BF-16-A & P2-BF-16-B & P2-BF-16-C: Optional
Basic Feed Sharing	Multiple Indicators in same bundle	na	P2-BF-17-A & P2-BF-17-B & P2-BF-17-C: Mandatory
Basic Feed Sharing	Indicator FQDN	na	P2-BF-18-A & P2-BF-18-B & P2-BF-18-C: Mandatory
Basic Feed Sharing	Indicator URL	na	P2-BF-19-A & P2-BF-19-B & P2-BF-19-C: Mandatory
Basic Feed Sharing	Indicator URL or FQDN	na	P2-BF-20-A & P2-BF-20-B & P2-BF-20-C: Mandatory
Basic Feed Sharing	Indicator File hash with SHA256 or MD5 values	na	P2-BF-21-A & P2-BF-21-B & P2-BF-21-C: Mandatory
Basic Intel	Verify Collection Information	na	na

Collaboration			
Basic Intel Collaboration	Indicator IPv4 Address	na	na
Basic Intel Collaboration	Indicator IPv4 Address CIDR	na	na
Basic Intel Collaboration	Two Indicators with IPv4 Address CIDR	na	na
Basic Intel Collaboration	Indicator with IPv6 Address	na	na
Basic Intel Collaboration	Indicator with IPv6 Address CIDR	na	na
Basic Intel Collaboration	Multiple Indicators within the same bundle	na	na
Basic Intel Collaboration	Indicator FQDN	na	na
Basic Intel Collaboration	Indicator URL	na	na
Basic Intel Collaboration	Indicator URL or FQDN	na	na
Basic Intel Collaboration	Indicator File hash with SHA256 or MD5 values	na	na

3.8 TAXII Feed (TXF)

For the purpose of this document, a TXF provides the ability for different systems to receive STIX 2.0 content from the TXF system. How the content is made available to the TXF is out of scope.

Any software instance being qualified as a TXF must confirm test results for the following test cases.

Table 3.8.1 — TAXII Feed (TXF) Part 2 Test Verification List

Test Case	Test	Producer	Respondent
Common Connection	Get Discovery Resource	na	P2-CC-1:Mandatory
Common Connection	Get API Root	na	P2-CC-2: Mandatory
Common Connection	Missing Authorization Parameter	na	P2-CC-3: Mandatory
Common Connection	Incorrect Authorization Parameter Returns Unauthorized	na	P2-CC-4: Mandatory
Common Connection	Incorrect API Root Info Get Returns Not Found	na	P2-CC-5: Mandatory
Common Connection	Incorrect Collection Info Get Returns Not Found	na	P2-CC-6: Mandatory
Basic Feed Sharing	Verify Collection Information	na	P2-BF-1: Mandatory
Basic Feed Sharing	Indicator IPv4 Address	na	P2-BF-12-A & P2-BF-12-B & P2-BF-12-C: Mandatory
Basic Feed Sharing	Indicator IPv4 Address CIDR	na	P2-BF-13-A & P2-BF-13-B & P2-BF-13-C: Mandatory
Basic Feed Sharing	Two Indicators with IPv4 Address CIDR	na	P2-BF-14-A & P2-BF-14-B & P2-BF-14-C: Mandatory
Basic Feed Sharing	Indicator with IPv6 Address	na	P2-BF-15-A & P2-BF-15-B & P2-BF-15-C: Optional
Basic Feed Sharing	Indicator with IPv6 Address CIDR	na	P2-BF-16-A & P2-BF-16-B & P2-BF-16-C: Optional

Basic Feed Sharing	Multiple Indicators in same bundle	na	P2-BF-17-A & P2-BF-17-B & P2-BF-17-C: Mandatory
Basic Feed Sharing	Indicator FQDN	na	P2-BF-18-A & P2-BF-18-B & P2-BF-18-C: Mandatory
Basic Feed Sharing	Indicator URL	na	P2-BF-19-A & P2-BF-19-B & P2-BF-19-C: Mandatory
Basic Feed Sharing	Indicator URL or FQDN	na	P2-BF-20-A & P2-BF-20-B & P2-BF-20-C: Mandatory
Basic Feed Sharing	Indicator File hash with SHA256 or MD5 values	na	P2-BF-21-A & P2-BF-21-B & P2-BF-21-C: Mandatory
Basic Intel Collaboration	Verify Collection Information	na	na
Basic Intel Collaboration	Indicator IPv4 Address	na	na
Basic Intel Collaboration	Indicator IPv4 Address CIDR	na	na
Basic Intel Collaboration	Two Indicators with IPv4 Address CIDR	na	na
Basic Intel Collaboration	Indicator with IPv6 Address	na	na
Basic Intel Collaboration	Indicator with IPv6 Address CIDR	na	na
Basic Intel Collaboration	Multiple Indicators within the same bundle	na	na
Basic Intel Collaboration	Indicator FQDN	na	na

Basic Intel Collaboration	Indicator URL	na	na
Basic Intel Collaboration	Indicator URL or FQDN	na	na
Basic Intel Collaboration	Indicator File hash with SHA256 or MD5 values	na	na

3.9 TAXII Server (TXS)

For the purpose of this document, a TXS provides the ability for different systems to share STIX 2.0 content. The TXS does not produce any STIX content.

Any software instance being qualified as a TXS must confirm test results for the following test cases.

Table 3.8.1 — TAXII Server (TXS) Part 2 Test Verification List

Test Case	Test	Producer	Respondent
Common Connection	Get Discovery Resource	P2-CC-1: Mandatory	P2-CC-1: Mandatory
Common Connection	Get API Root	P2-CC-2: Mandatory	P2-CC-2: Mandatory
Common Connection	Missing Authorization Parameter	P2-CC-3: Mandatory	P2-CC-3: Mandatory
Common Connection	Incorrect Authorization Parameter Returns Unauthorized	P2-CC-4: Mandatory	P2-CC-4: Mandatory
Common Connection	Incorrect API Root Info Get Returns Not Found	P2-CC-5: Mandatory	P2-CC-5: Mandatory
Common Connection	Incorrect Collection Info Get Returns Not Found	P2-CC-6: Mandatory	P2-CC-6: Mandatory
Basic Feed Sharing	Verify Collection Information	na	P2-BF-1: Mandatory

Basic Feed Sharing	Indicator IPv4 Address	na	P2-BF-12-A & P2-BF-12-B & P2-BF-12-C: Mandatory
Basic Feed Sharing	Indicator IPv4 Address CIDR	na	P2-BF-13-A & P2-BF-13-B & P2-BF-13-C: Mandatory
Basic Feed Sharing	Two Indicators with IPv4 Address CIDR	na	P2-BF-14-A & P2-BF-14-B & P2-BF-14-C: Mandatory
Basic Feed Sharing	Indicator with IPv6 Address	na	P2-BF-15-A & P2-BF-15-B & P2-BF-15-C: Optional
Basic Feed Sharing	Indicator with IPv6 Address CIDR	na	P2-BF-16-A & P2-BF-16-B & P2-BF-16-C: Optional
Basic Feed Sharing	Multiple Indicators in same bundle	na	P2-BF-17-A & P2-BF-17-B & P2-BF-17-C: Mandatory
Basic Feed Sharing	Indicator FQDN	na	P2-BF-18-A & P2-BF-18-B & P2-BF-18-C: Mandatory
Basic Feed Sharing	Indicator URL	na	P2-BF-19-A & P2-BF-19-B & P2-BF-19-C: Mandatory
Basic Feed Sharing	Indicator URL or FQDN	na	P2-BF-20-A & P2-BF-20-B & P2-BF-20-C: Mandatory
Basic Feed Sharing	Indicator File hash with SHA256 or MD5 values	na	P2-BF-21-A & P2-BF-21-B & P2-BF-21-C: Mandatory

Basic Intel Collaboration	Verify Collection Information	na	na
Basic Intel Collaboration	Indicator IPv4 Address	na	na
Basic Intel Collaboration	Indicator IPv4 Address CIDR	na	na
Basic Intel Collaboration	Two Indicators with IPv4 Address CIDR	na	na
Basic Intel Collaboration	Indicator with IPv6 Address	na	na
Basic Intel Collaboration	Indicator with IPv6 Address CIDR	na	na
Basic Intel Collaboration	Multiple Indicators within the same bundle	na	na
Basic Intel Collaboration	Indicator FQDN	na	na
Basic Intel Collaboration	Indicator URL	na	na
Basic Intel Collaboration	Indicator URL or FQDN	na	na
Basic Intel Collaboration	Indicator File hash with SHA256 or MD5 values	na	na

Appendix A. Acknowledgments

Interoperability Subcommittee Chairs:

Allan Thomson, LookingGlass,
Jason Keirstead, IBM

Additional Editors

Jane Ginn, Cyber Threat Intelligence Network, Inc.
Gus Creedon, Logistics Management Institute

Special Thanks:

Substantial contributions to this specification from the following individuals are gratefully acknowledged:

- Bret Jordan

Participants:

The following individuals were members of the OASIS CTI Technical Committee during the creation of this specification.

First Name	Last Name	Company
Kai	Li	360 Enterprise Security Group
Xinhua	Zheng	360 Enterprise Security Group
Robert	Coderre	Accenture
Kyle	Maxwell	Accenture
David	Crawford	Aetna
Marcos	Orallo	Airbus Group SAS
Roman	Fiedler	AIT Austrian Institute of Technology
Florian	Skopik	AIT Austrian Institute of Technology
Ryan	Clough	Anomali
Nicholas	Hayden	Anomali

Wei	Huang	Anomali
Angela	Nichols	Anomali
Hugh	Njemanze	Anomali
Katie	Pelusi	Anomali
Dean	Thompson	Australia and New Zealand Banking Group (ANZ Bank)
Radu	Marian	Bank of America
Sounil	Yu	Bank of America
Vicky	Laurens	Bank of Montreal
Alexandre	Dulaunoy	CIRCL
Andras	Iklody	CIRCL
Christian	Studer	CIRCL
RaphaÎl	Vinot	CIRCL
Syam	Appala	Cisco Systems
Ted	Bedwell	Cisco Systems
David	McGrew	Cisco Systems
Pavan	Reddy	Cisco Systems
Omar	Santos	Cisco Systems
Sam	Taghavi Zargar	Cisco Systems
Jyoti	Verma	Cisco Systems
Jart	Armin	Cyber Threat Intelligence Network, Inc. (CTIN)
Doug	DePeppe	Cyber Threat Intelligence Network, Inc. (CTIN)
Jane	Ginn	Cyber Threat Intelligence Network, Inc. (CTIN)

Ben	Ottoman	Cyber Threat Intelligence Network, Inc. (CTIN)
David	Powell	Cyber Threat Intelligence Network, Inc. (CTIN)
Andreas	Sfakianakis	Cyber Threat Intelligence Network, Inc. (CTIN)
Andrew	Byrne	Dell
Jeff	Odom	Dell
Sreejith	Padmajadevi	Dell
Ravi	Sharda	Dell
Will	Urbanski	Dell
Evette	Maynard-Noel	DHS Office of Cybersecurity and Communications (CS&C)
Sean	Sobieraj	DHS Office of Cybersecurity and Communications (CS&C)
Marlon	Taylor	DHS Office of Cybersecurity and Communications (CS&C)
Preston	Werntz	DHS Office of Cybersecurity and Communications (CS&C)
Wouter	Bolsterlee	EclecticIQ
Adam	Bradbury	EclecticIQ
Marko	Dragoljevic	EclecticIQ
Oliver	Gheorghe	EclecticIQ
Joep	Gommers	EclecticIQ
Christopher	O'Brien	EclecticIQ
Sergey	Polzunov	EclecticIQ
Rutger	Prins	EclecticIQ
Andrei	SÓrghi	EclecticIQ
Raymon	van der Velde	EclecticIQ

Tom	Vaughan	EclecticIQ
Ben	Sooter	Electric Power Research Institute (EPRI)
Chris	Ricard	Financial Services Information Sharing and Analysis Center (FS-ISAC)
Sean	Barnum	FireEye, Inc.
Phillip	Boles	FireEye, Inc.
Prasad	Gaikwad	FireEye, Inc.
Will	Green	FireEye, Inc.
Rajeev	Jha	FireEye, Inc.
Gary	Katz	FireEye, Inc.
Anuj	Kumar	FireEye, Inc.
James	Meck	FireEye, Inc.
Shyamal	Pandya	FireEye, Inc.
Paul	Patrick	FireEye, Inc.
Remko	Weterings	FireEye, Inc.
Tim	Jones	ForeScout
Ryusuke	Masuoka	Fujitsu Limited
Daisuke	Murabayashi	Fujitsu Limited
Derek	Northrope	Fujitsu Limited
Toshitaka	Satomi	Fujitsu Limited
Koji	Yamada	Fujitsu Limited
Kunihiko	Yoshimura	Fujitsu Limited
David	Lemire	G2

Iain	Brown	GDS
Adam	Cooper	GDS
James	Penman	GDS
Howard	Staple	GDS
Chris	Taylor	GDS
Laurie	Thomson	GDS
Alastair	Treharne	GDS
Julian	White	GDS
Robert	van Engelen	Genivia
Eric	Burger	Georgetown University
Allison	Miller	Google Inc.
Mark	Risher	Google Inc.
Yoshihide	Kawada	Hitachi, Ltd.
Jun	Nakanishi	Hitachi, Ltd.
Kazuo	Noguchi	Hitachi, Ltd.
Akihito	Sawada	Hitachi, Ltd.
Yutaka	Takami	Hitachi, Ltd.
Masato	Terada	Hitachi, Ltd.
Adrian	Bishop	Huntsman Security
Eldan	Ben-Haim	IBM
Allen	Hadden	IBM
Sandra	Hernandez	IBM

Jason	Keirstead	IBM
Chenta	Lee	IBM
John	Morris	IBM
Devesh	Parekh	IBM
Nick	Rossmann	IBM
Laura	Rusu	IBM
Ron	Williams	IBM
Paul	Martini	iboss, Inc.
Vasileios	Mavroeidis	IFI
Kamer	Vishi	IFI
Joerg	Eschweiler	Individual
Stefan	Hagen	Individual
Elysa	Jones	Individual
Terry	MacDonald	Individual
Tim	Casey	Intel Corporation
Julie	Modlin	Johns Hopkins University Applied Physics Laboratory
Mark	Moss	Johns Hopkins University Applied Physics Laboratory
Mark	Munoz	Johns Hopkins University Applied Physics Laboratory
Nathan	Reller	Johns Hopkins University Applied Physics Laboratory
Pamela	Smith	Johns Hopkins University Applied Physics Laboratory
Subodh	Kumar	JPMorgan Chase Bank, N.A.
David	Laurance	JPMorgan Chase Bank, N.A.

Russell	Culpepper	Kaiser Permanente
Beth	Pumo	Kaiser Permanente
Michael	Slavick	Kaiser Permanente
Gus	Creedon	Logistics Management Institute
Wesley	Brown	LookingGlass
Jamison	Day	LookingGlass
Dennis	Hostetler	LookingGlass
Himanshu	Kesar	LookingGlass
Matt	Pladna	LookingGlass
Vlad	Serban	LookingGlass
Allan	Thomson	LookingGlass
Ian	Truslove	LookingGlass
Chris	Wood	LookingGlass
Kent	Landfield	McAfee
Jonathan	Baker	Mitre Corporation
Desiree	Beck	Mitre Corporation
Michael	Chisholm	Mitre Corporation
Sam	Cornwell	Mitre Corporation
Sarah	Kelley	Mitre Corporation
Ivan	Kirillov	Mitre Corporation
Michael	Kouremetis	Mitre Corporation
Chris	Lenk	Mitre Corporation

Nicole	Parrish	Mitre Corporation
Richard	Piazza	Mitre Corporation
Larry	Rodrigues	Mitre Corporation
Jon	Salwen	Mitre Corporation
Charles	Schmidt	Mitre Corporation
Alex	Tweed	Mitre Corporation
Emmanuelle	Vargas-Gonzalez	Mitre Corporation
John	Wunder	Mitre Corporation
James	Cabral	MTG Management Consultants, LLC.
Scott	Algeier	National Council of ISACs (NCI)
Denise	Anderson	National Council of ISACs (NCI)
Josh	Poster	National Council of ISACs (NCI)
Mike	Boyle	National Security Agency
Jessica	Fitzgerald-McKay	National Security Agency
David	Kemp	National Security Agency
Shaun	McCullough	National Security Agency
Jason	Romano	National Security Agency
John	Anderson	NC4
Michael	Butt	NC4
Mark	Davidson	NC4
Daniel	Dye	NC4
Michael	Pepin	NC4

Natalie	Suarez	NC4
Benjamin	Yates	NC4
Sarah	Brown	NCI Agency
Oscar	Serrano	NCI Agency
Daichi	Hasumi	NEC Corporation
Takahiro	Kakumaru	NEC Corporation
Lauri	Korts-P‰rn	NEC Corporation
Trey	Darley	New Context Services, Inc.
John-Mark	Gurney	New Context Services, Inc.
Christian	Hunt	New Context Services, Inc.
Danny	Purcell	New Context Services, Inc.
Daniel	Riedel	New Context Services, Inc.
Andrew	Storms	New Context Services, Inc.
Drew	Varner	NineFX, Inc.
Stephen	Banghart	NIST
David	Darnell	North American Energy Standards Board
James	Crossland	Northrop Grumman
Robert	Van Dyk	Northrop Grumman
Cheolho	Lee	NSRI
Cory	Casanave	Object Management Group
Vishaal	Hariprasad	Palo Alto Networks
Brad	Bohen	Perch

Aharon	Chernin	Perch
Dave	Eilken	Perch
Zach	Kanzler	Perch
Michael	Lane	Perch
Michael	Riggs	Perch
Amanda	Stott	Perch
John	Tolbert	Queralt Inc.
Jay	Heidecker	Seekintoo
Joseph	Brand	Semper Fortis Solutions
Duncan	Sparrell	sFractal Consulting LLC
Thomas	Schreck	Siemens AG
Cedric	LeRoux	Splunk Inc.
Brian	Luger	Splunk Inc.
Philip	Royer	Splunk Inc.
Sourabh	Satish	Splunk Inc.
Bret	Jordan	Symantec Corp.
Robert	Keith	Symantec Corp.
Curtis	Kostrosky	Symantec Corp.
Chris	Larsen	Symantec Corp.
Michael	Mauch	Symantec Corp.
Aubrey	Merchant	Symantec Corp.
Efrain	Ortiz	Symantec Corp.

Mingliang	Pei	Symantec Corp.
Kenneth	Schneider	Symantec Corp.
Arnaud	Taddei	Symantec Corp.
Brian	Witten	Symantec Corp.
Greg	Reaume	TELUS
Alan	Steer	TELUS
Crystal	Hayes	The Boeing Company
Andrew	Gidwani	ThreatConnect, Inc.
Cole	Iliff	ThreatConnect, Inc.
Andrew	Pendergast	ThreatConnect, Inc.
Jason	Spies	ThreatConnect, Inc.
Ryan	Trost	ThreatQuotient, Inc.
Nir	Yosha	ThreatQuotient, Inc.
Kris	Anderson	Trend Micro
David	Girard	Trend Micro
Brandon	Niemczyk	Trend Micro
Eric	Shulze	Trend Micro
Patrick	Coughlin	TruSTAR Technology
Chris	Roblee	TruSTAR Technology
Mark	Angel	U.S. Bank
Brian	Fay	U.S. Bank
Joseph	Frazier	U.S. Bank

Mark	Heidrick	U.S. Bank
Richard	Shok	U.S. Bank
James	Bohling	US Department of Defense (DoD)
Gary	Katz	US Department of Defense (DoD)
Jeffrey	Mates	US Department of Defense (DoD)
Evette	Maynard-Noel	US Department of Homeland Security
Lee	Chieffalo	Viasat
Wilson	Figueroa	Viasat
Andrew	May	Viasat
Ales	Cernivec	XLAB
Anthony	Rutkowski	Yanna Technologies LLC

Appendix B. Revision History

Revision	Date	Editor	Changes Made
01	09/11/17	Allan Thomson, Jason Keirstead	First Version - Fixed collection ids - Added same org, different analysts for sharing collaboration - Added TIS persona - Defined test sections for common connection, basic feed sharing and collaboration
02	02/27/18	Allan Thomson Jason Keirstead	2nd Version - Added TXF Persona and updated tests accordingly
03	03/28/18	Allan Thomson	3rd Version - Updated uuids - Reference to new Part 1 v1.1 document - Updated test verification to include option for log file vs user interface checks
04	04/13/18	Allan Thomson	4th version - Fixed table for data sharing setup for TXF - Editorial fixes
FD	05/04/18	Allan Thomson	Final Draft (Rejected at Ballot) - Fix URLs / ending - Fix size of maximum result of TAXII - Add text to make it clear certain responses are best practices and not exact matches - Fix UUID references
05	09/04/18	Allan Thomson	5th Version - Fixed template based on Bret's review

			- Added test numbers - Restructured test definitions to clarify what is being tested and how
06	10/17/18	Allan Thomson	- Added reference section and fixed RFC mentions to those references - Updated all collection IDs across basic feed and collaboration tests - Updated to address editorial comments from Bret - Updated test matrix section for inconsistent references to tests for DFP - Added test summaries to both basic feed and basic intel collaboration sections - Updated contribution table based on latest roster - Updated the respondent definition to make it clear it both receives data and sends data back to the Producer
FD01	10/22/18	Allan Thomson	Final Draft for TC Ballot.