STIX/TAXII™ 2.0 Interoperability Test Document - Part 2

V1.0 Working Draft 4

13 April 2018

​Technical Committee:

[OASIS Cyber Threat Intelligence (CTI) TC](https://www.oasis-open.org/committees/cti/)

​Chair:

Richard Struse (rjs@mitre.org) Mitre Corporation

​Editors:

Allan Thomson (athomson@lookingglasscyber.com), [LookingGlass](https://www.lookingglasscyber.com/)

Jason Keirstead (jason.keirstead@ca.ibm.com), [IBM](http://www.ibm.com/)

Related work:

This document is related to:

* *STIX™ Version 2.0. Part 1: STIX Core Concepts. Edited by Bret Jordan, John Wunder, and Rich* Piazza. 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 Bret Jordan, John Wunder, and Rich* Piazza. 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 Bret Jordan, Mark Davidson, and John Wunder. Latest version: <http://docs.oasis-open.org/cti/taxii/v2.0/taxii-v2.0.html>.

Abstract:

This is Part 2 of the Interoperability test document to supplement the five-part Structured Threat Information Expression (STIX) and TAXII 2.0 specifications developed by the Cyber Threat Intelligence Technical Committee (CTI TC) of the Organization for the Advancement of Structured Information Systems (OASIS). The is the second in a series that will be developed concurrent with revisions to the STIX/TAXII specifications. This test document provides detailed requirements on how producers of products within the threat intelligence ecosystem may demonstrate conformity with STIX/TAXII 2.0 if they wish to self-certify that their software is verified as interoperable. 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 use cases: common connection, basic data sharing and basic threat intelligence collaboration. For each of these use cases the document details the Producer support, TAXII server support and the Respondent support to be used for the test cases.

Status:

This [Working Draft](https://www.oasis-open.org/policies-guidelines/tc-process#dWorkingDraft) (WD) has been produced by one or more TC Members; it has not yet been voted on by the TC or [approved](https://www.oasis-open.org/policies-guidelines/tc-process#committeeDraft) as a Committee Note Draft. The OASIS document [Approval Process](https://www.oasis-open.org/policies-guidelines/tc-process#standApprovProcess) begins officially with a TC vote to approve a WD as a Committee Note Draft. A TC may approve a Working Draft, revise it, and re-approve it any number of times as a Committee Note Draft.

URI patterns:

Initial publication URI:

<http://docs.oasis-open.org/cti/stix-taxii-2-interop/v1.0/cnd02/stix-taxii-2-interop-p2-v1-0-cnd01.docx>

Permanent “Latest version” URI:

<http://docs.oasis-open.org/cti/stix-taxii-2-interop/v1.0/stix-taxii-2-interop-p2-v1-0.docx>

(Managed by OASIS TC Administration; please don't modify.)

Copyright © OASIS Open 2018. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full [Policy](https://www.oasis-open.org/policies-guidelines/ipr) may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

**Table of Contents**

[1 ​Introduction 5](#_Toc511395412)

[1.1 Terminology 5](#_Toc511395413)

[1.2 Overview 5](#_Toc511395414)

[1.2.1 ​Part 2 Personas 5](#_Toc511395415)

[2 Use Case Details 7](#_Toc511395416)

[2.1 Common Use Case Requirements 8](#_Toc511395417)

[2.2 Common Connection 9](#_Toc511395418)

[2.2.1 Description 9](#_Toc511395419)

[2.2.2 Required TXS/TXF Configuration 9](#_Toc511395420)

[2.2.3 Required Persona Support 9](#_Toc511395421)

[2.2.4 Test Case Data 10](#_Toc511395422)

[2.2.4.1 Basic TXS/TXF Get 10](#_Toc511395423)

[2.2.4.2 Basic API-Root Get 10](#_Toc511395424)

[2.2.4.3 Missing Authorization Parameter Returns Unauthorized 11](#_Toc511395425)

[2.2.4.4 Incorrect Authorization Parameter Returns Unauthorized 11](#_Toc511395426)

[2.2.4.5 Incorrect API Root Info Get Returns Not Found 11](#_Toc511395427)

[2.2.4.6 Incorrect Collection Info Get Returns Not Found 12](#_Toc511395428)

[2.3 Basic Feed Sharing 13](#_Toc511395429)

[2.3.1 Description 13](#_Toc511395430)

[2.3.2 Required TXS or TXF Configuration 13](#_Toc511395431)

[2.3.3 Required Producer Persona Support 14](#_Toc511395432)

[2.3.4 Producer Test Case Data 16](#_Toc511395433)

[2.3.4.1 Verify Collection Information 16](#_Toc511395434)

[2.3.4.2 Indicator Publication 16](#_Toc511395435)

[2.3.5 ​Required Respondent Support 17](#_Toc511395436)

[2.3.6 ​Respondent Test Case Data 19](#_Toc511395437)

[2.3.6.1 Indicator Get 19](#_Toc511395438)

[2.4 Basic Intelligence Collaboration 21](#_Toc511395439)

[2.4.1 Description 21](#_Toc511395440)

[2.4.2 Required TXS Configuration 24](#_Toc511395441)

[2.4.3 Required Producer Persona Support 24](#_Toc511395442)

[2.4.4 Producer Test Case Data 25](#_Toc511395443)

[2.4.4.1 Verify Collection Information 25](#_Toc511395444)

[2.4.4.2 Indicator Publication 26](#_Toc511395445)

[2.4.5 ​Required Respondent Support 27](#_Toc511395446)

[2.4.6 ​Respondent Test Case Data 32](#_Toc511395447)

[2.4.6.1 Indicator Get & Update Modified Intelligence 32](#_Toc511395448)

[2.4.6.2 Indicator Get & Create Related Intelligence 33](#_Toc511395449)

[3 ​Persona Checklist 35](#_Toc511395450)

[3.1 Performing Verification Tests and Recording Results 35](#_Toc511395451)

[3.2 ​Data Feed Provider (DFP) 36](#_Toc511395452)

[3.3 ​Threat Intelligence Platform (TIP) 39](#_Toc511395453)

[3.4 Security Incident and Event Management (SIEM) 43](#_Toc511395454)

[3.5 Threat Mitigation System (TMS) 47](#_Toc511395455)

[3.6 Threat Detection System (TDS) 51](#_Toc511395456)

[3.7 Threat intelligence Sink (TIS) 55](#_Toc511395457)

[3.8 TAXII Feed (TXF) 60](#_Toc511395458)

[3.9 TAXII Server (TXS) 63](#_Toc511395459)

[4 ​Appendix A Acknowledgments 65](#_Toc511395460)

[5 Appendix B. Revision History 81](#_Toc511395461)

#

#

# 1 ​Introduction

This document defines additional test cases and personas for STIX/TAXII 2.0 Interoperability Use Cases and is supplementary to [Part 1 v1.1](https://docs.google.com/document/d/1TQrWR3RvLirV-HhgjfKNM4oJH_sOOlcvQaq18xmD10o/edit).

## 1.1 Terminology

Please refer to [Part 1 v1.1](https://docs.google.com/document/d/1TQrWR3RvLirV-HhgjfKNM4oJH_sOOlcvQaq18xmD10o/edit) Section 1.1 Terminology.

## 1.2 Overview

This document focuses on testing interoperability of software instances that support STIX and TAXII exchange. It leverages [Part 1 v1.1](https://docs.google.com/document/d/1TQrWR3RvLirV-HhgjfKNM4oJH_sOOlcvQaq18xmD10o/edit) test cases, and augments them by adding a TAXII Server to facilitate the exchange of STIX bundled content detailed in [Part 1 v1.1](https://docs.google.com/document/d/1TQrWR3RvLirV-HhgjfKNM4oJH_sOOlcvQaq18xmD10o/edit).

### 1.2.1 ​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.
* Threat Intelligence Platform (TIP)
	+ Software instance that acts as a producer and/or Respondent of STIX 2.0 content primarily used to aggregate, refine and share intelligence with other machines or security personnel operating other security infrastructure.
* Security Incident and Event Management system (SIEM)
	+ Software instance that acts as a producer and/or Respondent of STIX 2.0 content. A SIEM that produces STIX content will typically create incidents and indicators. A SIEM that consumes STIX content will typically consume sightings, indicators.
* 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.
* 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.
* 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.
* TAXII Feed (TXF)
	+ Software instance that publishes STIX data as a read-only TAXII Server where respondents may receive the STIX data from the TXF.
* TAXII Server (TXS)
	+ Software instance that acts as a TAXII Server enabling the sharing of STIX 2.0 content among producers and respondents.

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

For persona checklist and test requirements per persona please refer to [3 Persona Checklist](#_areh76or16u4).

#

#

# 2 Use Case Details

Part 2 use cases are broken down by persona into mandatory and optional sets of use cases. All use cases require the use of a TAXII Server (TXS) component used in concert with the producer and respondent persona components as shown below.

An organization’s software product under test may implement multiple personas. Therefore, it is conceivable that a single software product instance supports a TAXII Server, 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.



Figure 2: Basic Intelligence Data Flow

This document details the following use cases.

**Table 2.0 — List of TAXII Interoperability Test Categories**

|  |  |  |
| --- | --- | --- |
| Description | Producer Personas | Respondent Personas |
| [Common Connection](#2.2 Common Connection) and Error Handling | All | All |
| [Basic Feed Sharing](#2.3 Basic Feed Sharing) | DFP, TIP; SIEM, TXF | TMS, TDS, TIP, SIEM, TIS |
| [Basic Intel Collaboration](#2.4 Basic Intelligence Collaboration) | DFP, TIP, TMS, TDS; SIEM, TXF | TIP, SIEM |

## 2.1 Common Use Case Requirements

The HTTPS over IPv4 protocol must be used for all test cases in this document.

Future versions of this document may introduce testing HTTPS over IPv6 as the TAXII transport protocol.

There are no defined tests that exclude IPv6 support if an organization wishes to execute those tests with HTTPS over IPv6.

##

##

## 2.2 Common Connection

### 2.2.1 Description

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

To ensure baseline interoperability between a TAXII Client and TAXII Server, every test in this section must be completed. Advancing to [Basic Feed Sharing](#2.3 Basic Feed Sharing)and [Basic Intelligence Collaboration](#2.4 Basic Intelligence Collaboration) test cases should not be attempted until TAXII Client/Server interoperability is baselined.

### 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[[1]](#footnote-1)
2. Server configured to support client connections via HTTPS [[RFC7230](https://docs.google.com/document/d/1Jv9ICjUNZrOnwUXtenB1QcnBLO35RnjQcJLsa1mGSkI/edit#bookmark=id.hb9xzm4g5vgy)] and TLS 1.2 [[RFC5246](https://docs.google.com/document/d/1Jv9ICjUNZrOnwUXtenB1QcnBLO35RnjQcJLsa1mGSkI/edit#bookmark=id.hb5wa4a70wq)]
3. Server configured for HTTP Basic Authentication [[RFC 7617](https://docs.google.com/document/d/1Jv9ICjUNZrOnwUXtenB1QcnBLO35RnjQcJLsa1mGSkI/edit#bookmark=id.vde58tur741j)]
4. Server configured to authorize a client with the following credentials
	1. Username: test, Password: Passw0rd!
	2. HTTP Authentication Value (Base 64 encoded): “Authorization: Basic dGVzdDpQYXNzdzByZCE=”
5. Test Data #1: Server or Feed
	1. URL: 10.1.1.10:443
	2. Title: “TAXII [Server | Feed] Under Test”
	3. Description: “This is a TAXII [Server | Feed] under test”
	4. Contact: “Admin Contact 1-800-111-1111”
	5. Default: “[https://](https://taxii.undertest.com/api1)10.1.1.10[/api1](https://taxii.undertest.com/api1)/”
	6. Api\_roots: [ “[https://](https://taxii.undertest.com/api1)10.1.1.10[/api1](https://taxii.undertest.com/api1)/”]
6. Test Data #2: API-Root
	1. URL: 10.1.1.10/api1/
	2. Title: “Sharing Group 1”
	3. Description: “This sharing group shares intelligence”
	4. Versions: [ “taxii-2.0” ]
	5. MaxContentLength: 100000

### 2.2.3 Required Persona Support

The Producer must be able to connect to a TAXII Server (TXS) or TAXII Feed (TXF) and display the appropriate connection status.

Table 2.2.3 - Producer Support Behavior

|  |  |
| --- | --- |
| Personas | Behavior |
| All | 1. Producer allows a user to select or specify the URL Address of the TXS to connect to as: https://10.1.1.10:443
2. Producer connects to the TXS and gets the information associated with the TXS component and displays to the user the following information
	1. Get URL**:** https://10.1.1.10:443/taxii/
	2. All returned parameters are shown by the Producer that match Test-Data #1
3. Producer connects to the TXS API Root [https://](https://taxii.undertest.com/api1)10.1.1.10[/api1](https://taxii.undertest.com/api1)/ and gets the information associated with the TXS API Root and displays to the user the following information:
	1. Get URL: https://10.1.1.10:443/api1/
	2. All returned parameters are shown by the Producer that match the Test-Data #2
 |

### 2.2.4 Test Case Data

#### 2.2.4.1 Basic TXS/TXF Get

**2.2.4.2 Table 2.2.4.1 - Basic GET Request and Response**

|  |  |
| --- | --- |
| **To TXS/TXF** | **From TXS/TXF** |
| GET /taxii/ HTTP/1.1Host: 10.1.1.10Accept: application/taxii+json; version=2.0Authorization: Basic dGVzdDpQYXNzdzByZCE= | HTTP/1.1 200 OKContent-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://](https://taxii.undertest.com/api1)10.1.1.10[/api1](https://taxii.undertest.com/api1)/", "api\_roots": [ "[https:/](https://taxii.undertest.com/api1)/10.1.1.10[/api1](https://taxii.undertest.com/api1)/" ]} |

#### 2.2.4.2 Basic API-Root Get

Table 2.2.4.2 - Basic GET Request and Response

|  |  |
| --- | --- |
| **To TXS/TXF** | **From TXS/TXF** |
| GET /api1/ HTTP/1.1Host: 10.1.1.10Accept: application/taxii+json; version=2.0Authorization: Basic dGVzdDpQYXNzdzByZCE= | HTTP/1.1 200 OKContent-Type: application/taxii+json; version=2.0{ "title": "Sharing Group 1", "description": "This sharing group shares intelligence", "versions": [ "taxii-2.0"], "max\_content\_length": 1048576} |

#### 2.2.4.3 Missing Authorization Parameter Returns Unauthorized

**Table 2.2.4.4 - Basic GET Request and Response**

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

#### 2.2.4.4 Incorrect Authorization Parameter Returns Unauthorized

**Table 2.2.4.4 - Basic GET Request and Response**

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

#### 2.2.4.5 Incorrect API Root Info Get Returns Not Found

**Table 2.2.4.5 - Basic GET Request and Response**

|  |  |
| --- | --- |
| **To TXS/TXF** | **From TXS/TXF** |
| GET /api2/collections/170f24af-c685-411d-bd2a-f45248adb245/ HTTP/1.1Host: 10.1.1.10Accept: application/taxii+json; version=2.0Authorization: Basic dGVzdDpQYXNzdzByZCE= | HTTP/1.1 404 Not FoundContent-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 Incorrect Collection Info Get Returns Not Found

Table 2.2.4.6 - Basic GET Request and Response

|  |  |
| --- | --- |
| **To TXS/TXF** | **From TXS/TXF** |
| GET /api1/collections/d021ecc8-ab8e-41ab-815e-911c7e329f88/ HTTP/1.1Host: 10.1.1.10Accept: application/taxii+json; version=2.0Authorization: Basic dGVzdDpQYXNzdzByZCE= | HTTP/1.1 404 Not FoundContent-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

### 2.3.1 Description

Basic Feed Sharing provides for a Producer persona component to produce STIX content and share it via a TAXII Server with a Respondent persona component. The mechanism to publish the STIX content to the TXS is required via TAXII whereas the mechanism to publish to a TXF is out of scope.

### 2.3.2 Required TXS or TXF Configuration

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

Numerous tests in this section must refer to collection IDs during their execution. In these tests, the UUID "8c99d7d2-8a6c-4196-b216-c1692d0126f2" is used to reference the collection under test. When performing the test, this ID MUST be substituted with the UUID that exists in the TXS or TXF that meets the configuration requirements for the test being performed.

**TXS Setup A:** Use separate collections for adding data to the server and a separate collection for reading from the server.

1. Test Data #1: Write Collection
	1. ID: 8c99d7d2-8a6c-4196-b216-c1692d0126f2
	2. URL: [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)8c99d7d2-8a6c-4196-b216-c1692d0126f2[/objects](https://10.1.1.10/api1/collections/1000/objects)
	3. Title: “Write Collection 1”
	4. Description: “This is write collection 1”
	5. Can\_read: false
		1. For all client gets
	6. Can\_write: true
		1. For all client posts
	7. Media\_types: [ "application/stix+json; version=2.0" ]
2. Test Data #2: Read Collection
	1. ID: 91a7b528-80eb-42ed-a74d-bd526120
	2. URL: [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)91a7b528-80eb-42ed-a74d-bd526120[/objects](https://10.1.1.10/api1/collections/1000/objects)
	3. Title: “Read Collection 1”
	4. Description: “This is read collection 1”
	5. Can\_read: true
		1. For all client gets
	6. Can\_write: false
		1. For all client posts
	7. Media\_types: [ "application/stix+json; version=2.0" ]

**TXS Setup B:** Use the same collection for adding and reading data to/from the server.

1. Test Data #1: Read-Write Collection
	1. ID: 8c99d7d2-8a6c-4196-b216-c1692d0126d3
	2. URL: [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)8c99d7d2-8a6c-4196-b216-c1692d0126d3[/objects](https://10.1.1.10/api1/collections/1000/objects)
	3. Title: “Read-Write Collection 1”
	4. Description: “This is read-write collection 1”
	5. Can\_read: true
		1. For all client gets
	6. Can\_write: true
		1. For all client posts
	7. Media\_types: [ "application/stix+json; version=2.0" ]

**TXF Setup C:** Use a single collection for reading from the feed.

1. Test Data #1: Read Collection
	1. ID: 91a7b528-80eb-42ed-a74d-bd526120
	2. URL: [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)91a7b528-80eb-42ed-a74d-bd526120[/objects](https://10.1.1.10/api1/collections/1000/objects)
	3. Title: “Read Collection 1”
	4. Description: “This is read collection 1”
	5. Can\_read: true
		1. For all client gets
	6. Can\_write: false
		1. For all client posts
	7. Media\_types: [ "application/stix+json; version=2.0" ]

### 2.3.3 Required Producer Persona Support

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

**Table 2.2.3 — Producer Object Bundling Details**

|  |  |
| --- | --- |
| Personas | Behavior |
| DFP; TIP; SIEM | 1. Producer allows a user to select or specify the URL Address of the TXS to connect to as: <https://10.1.1.10:443> and performs the tests described in *Section 2.2: Common Connection* Tests

**Setup A Behavior** 1. Producer does a get on the Write collection [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)8c99d7d2-8a6c-4196-b216-c1692d0126f2
2. Verify at the Producer that the TXS responds with the following information:
	1. **HTTP Response Code** is 200 OK
	2. **id** is 8c99d7d2-8a6c-4196-b216-c1692d0126f2
	3. **title** is “Write Collection 1”
	4. **description** is “This is write collection 1”
	5. **can\_read** is false
	6. **can\_write** is true
	7. **media\_types** is "application/stix+json; version=2.0"
3. For each section described in *Part1: Indicator Sharing Producer Test Cases*the Producer will publish the content to the TXS at https://10.1.1.10/api1/collections/8c99d7d2-8a6c-4196-b216-c1692d0126f2/objects where the TXS component will not respond to the post until all objects within the bundle have been processed.
4. Verify the TXS accepts the content by verifying the following about the Producer:
	1. **HTTP Response code** is 202 Accepted
	2. **id** represents a unique identifier for each post
	3. **status** is complete
	4. **request\_timestamp** represents the time of the post
	5. **total\_count** represents the number of objects in the bundle test case
	6. **success\_count** is the same as total\_count
	7. **successes** is an array of the object identifiers in the submitted bundle and matches the identifiers posted for each indicator
	8. **failure\_count** is 0
	9. **pending\_count** is 0

**Setup B Behavior** 1. Producer does a get on the Read-Write collection [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)8c99d7d2-8a6c-4196-b216-c1692d0126d3
2. Verify at the Producer that the TXS responds with the following information:
	1. **HTTP Response Code** is 200 OK
	2. **id** is 8c99d7d2-8a6c-4196-b216-c1692d0126d3
	3. **title** is “Read-Write Collection 1”
	4. **description** is “This is read-write collection 1”
	5. **can\_read** is true
	6. **can\_write** is true
	7. **media\_types** is "application/stix+json; version=2.0"
3. For each section described in *Part1: Indicator Sharing Producer Test Cases*the Producer will publish the content to the TXS at [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)8c99d7d2-8a6c-4196-b216-c1692d0126d3/objects where the TXS component will not respond to the post until all objects within the bundle have been processed.
4. Verify the TXS accepts the content by verifying the following about the Producer:
	1. **HTTP Response code** is 202 Accepted
	2. **id** represents a unique identifier for each post
	3. **status** is complete
	4. **request\_timestamp** represents the time of the post
	5. **total\_count** represents the number of objects in the bundle test case
	6. **success\_count** is the same as total\_count
	7. **successes** is an array of the object identifiers in the submitted bundle and matches the identifiers posted for each indicator
	8. **failure\_count** is 0
	9. **pending\_count** is 0

**Setup C Behavior** * Setup C does not support writing to the TAXII server and therefore this test is n/a
 |

### 2.3.4 Producer Test Case Data

#### 2.3.4.1 Verify Collection Information

**This test case does not apply to a TXF persona.**

**Table 2.3.4.1 - Basic GET Request and Response**

***The UUID shown in this table is the write-only collection test. If the test is being performed for write-read collection, then replace the UUID with that collection id.***

|  |  |
| --- | --- |
| **To TXS** | **From TXS** |
| GET [/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)8c99d7d2-8a6c-4196-b216-c1692d0126f2/ HTTP/1.1Host: 10.1.1.10Accept: application/vnd.oasis.taxii+json; version=2.0Authorization: Basic dGVzdDpQYXNzdzByZCE= | HTTP/1.1 200 OKContent-Type: application/vnd.oasis.taxii+json; version=2.0{ "id": "8c99d7d2-8a6c-4196-b216-c1692d0126f2", "title": "Test Collection 1", "description": "This is Test Collection 1", "can\_read": true, "can\_write": true, "media\_types": [ "application/vnd.oasis.stix+json; version=2.0" ]} |

#### 2.3.4.2 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 bundle responses
	1. Match the content in the To TXS or From TXS cells in the table below, with the
	2. correct total count of objects.
2. These tests do not apply to the TXF persona.

**Table 2.3.4.2 - Basic GET Request and Response**

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

|  |  |
| --- | --- |
| **To TXS** | **From TXS** |
| POST /api1/collections/8c99d7d2-8a6c-4196-b216-c1692d0126f2/objects/ HTTP/1.1Host: 10.1.1.10Accept: application/vnd.oasis.taxii+json; version=2.0Authorization: Basic dGVzdDpQYXNzdzByZCE=Content-Type: application/vnd.oasis.stix+json; version=2.0{  "type": "content from test table below...",} | HTTP/1.1 202 AcceptedContent-Type: application/vnd.oasis.taxii+json; version=2.0{ "id": "2d086da7-4bdc-4f91-900e-d77486753710", "status": "complete", "request\_timestamp": "2016-11-02T12:34:34.12345Z", "total\_count": 4, "success\_count": 4, "successes": [ "List of objects defined in the Part1 bundle test cases" ], "failure\_count": 0, "pending\_count": 0} |

**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** | **Total Count\*** |
| ​2.3.4.3.1 Indicator IPv4 Address | 2 |
| ​2.3.4.3.2 Indicator IPv4 Address CIDR | 2 |
| 2.3.4.3.3 Two Indicators with IPv4 Address CIDR | 2 |
| 2.3.4.3.4 Indicator with IPv6 Address | 2 |
| 2.3.4.3.5 Indicator with IPv6 Address CIDR | 2 |
| 2.3.4.3.6 Multiple Indicators within the same bundle | 3 |
| ​2.3.4.3.7 Indicator FQDN | 2 |
| 2.3.4.3.8 ​Indicator URL | 2 |
| ​2.3.4.3.9 Indicator URL or FQDN | 2 |
| 2.3.4.3.10 Indicator File hash with SHA256 or MD5 values | 2 |

### 2.3.5 ​Required Respondent Support

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.

**Table 2.2.5 — Respondent Object Bundling Details**

|  |  |
| --- | --- |
| Personas | Behavior |
| TIP; SIEM; TMS; TDS; TIS | **Setup A & Setup C Behavior**1. Respondent 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> and performs the tests described in *Section 2.2: Common Connection* Tests
2. Respondent does a get on the collection [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)91a7b528-80eb-42ed-a74d-bd526120 and verifies the following information:
	1. **HTTP Response Code** is 200 OK
	2. **id** is 91a7b528-80eb-42ed-a74d-bd526120
	3. **title** is “Read Collection 1”
	4. **description** is “This is Read Collection 1”
	5. **can\_read** is true
	6. **can\_write** is false
	7. **media\_types** is "application/stix+json; version=2.0"
3. For each section described in *Part1: Indicator Sharing Producer Test Cases*the Respondent will get the content from the TXS or TXF at [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)91a7b528-80eb-42ed-a74d-bd526120 /objects and verify that each bundle returned matched the content for the respective publication test case.
	1. For each test case verify the appropriate behavior defined in Part 1 is met.

**Setup B Behavior**1. Respondent allows a user to select or specify the URL Address of the TXS to connect to as: <https://10.1.1.10:443> and performs the tests described in *Section 2.2: Common Connection* Tests
2. Respondent does a get on the collection [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)91a7b528-80eb-42ed-a74d-bd5a2118 and verifies the following information:
	1. **HTTP Response Code** is 200 OK
	2. **id** is 91a7b528-80eb-42ed-a74d-bd5a2118
	3. **title** is “Read-Write Collection 1”
	4. **description** is “This is Read-Write Collection 1”
	5. **can\_read** is true
	6. **can\_write** is true
	7. **media\_types** is "application/stix+json; version=2.0"
3. For each section described in *Part1: Indicator Sharing Producer Test Cases*the Respondent will get the content from the TXS at https://10.1.1.10/api1/collections/91a7b528-80eb-42ed-a74d-bd5a2118/objects and verify that each bundle returned matched the content for the respective publication test case.
	1. For each test case verify the appropriate behavior defined in Part 1 is met.
 |

### 2.3.6 ​Respondent Test Case Data

#### 2.3.6.1 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 responses
	1. match the content in the To TXS/TXF or From TXS/TXF cells in the table below, with the
	2. correct total count of objects.

**Table 2.3.6.1 - Basic GET Request and Response**

|  |  |
| --- | --- |
| **To TXS/TXF** | **From TXS/TXF** |
| GET /[api1/collections/](https://10.1.1.10/api1/collections/1000/objects)91a7b528-80eb-42ed-a74d-bd526120 HTTP/1.1Host: 10.1.1.10Accept: application/stix+json; version=2.0Authorization: Basic dGVzdDpQYXNzdzByZCE= | HTTP/1.1 200 OKContent-Type: application/stix+json; version=2.0{  "type": "bundle", ... "objects": [ { "type": "indicator", ... } ]} |

**Table 2.3.6.2 - Test Case Total Object Count Requirement**

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

|  |  |
| --- | --- |
| **Test Cases** | **Total Count\*** |
| ​2.3.6.1.1 Indicator IPv4 Address | 2 |
| ​2.3.6.1.2 Indicator IPv4 Address CIDR | 2 |
| 2.3.6.1.3 Two Indicators with IPv4 Address CIDR | 2 |
| 2.3.6.1.4 Indicator with IPv6 Address | 2 |
| 2.3.6.1.5 Indicator with IPv6 Address CIDR | 2 |
| 2.3.6.1.6 Multiple Indicators within the same bundle | 3 |
| ​2.3.6.1.7 Indicator FQDN | 2 |
| ​2.3.6.1.8 Indicator URL | 2 |
| ​2.3.6.1.9 Indicator URL or FQDN | 2 |
| 2.3.6.1.10 Indicator File hash with SHA256 or MD5 values | 2 |

##

##

## 2.4 Basic Intelligence Collaboration

### 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:

* **Use 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 and reshares back to the first analyst for their review and acknowledgement.
	+ See Figure 2.4.1.a
* **Use 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
* **Use Case #3: Analysts/Groups within the same** **organization** sharing and modifying **related** intelligence between two analysts using two systems where the analyst has their own **created\_by** identity. These analysts/groups would serve different missions within the same organization
	+ 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 Use Case #3 resembles Use 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**

###

###

### 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.

In addition, both Producer and Respondent in this test section 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.

Numerous tests in this section **MUST** refer to collection IDs during their execution. In these tests, the UUID "8c99d7d2-8a6c-4196-b216-c1692d0126f2" is used 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 Required Producer Persona Support

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.

**Table 2.4.3 — Producer Object Bundling Details**

|  |  |
| --- | --- |
| Personas | **Use Case #1, #2 & #3** Behavior[[2]](#footnote-2)  |
| TIP; SIEM | 1. Producer allows a user to select or specify the URL Address of the TXS to connect to as: <https://10.1.1.10:443> and performs the tests described in *Section 2.2: Common Connection* Tests

**Setup A Behavior - Write Collection**1. Producer does a GET on the Write collection [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)8c99d7d2-8a6c-4196-b216-c1692d0126f2
2. Verify at the Producer that the TXS responds with the following information:
	1. **HTTP Response Code** is 200 OK
	2. **id** is 8c99d7d2-8a6c-4196-b216-c1692d0126f2
	3. **title** is “Write Collection 1”
	4. **description** is “This is Write Collection 1”
	5. **can\_read** is false
	6. **can\_write** is true
	7. **media\_types** is "application/stix+json; version=2.0"
3. For each section described in *Part1: Indicator Sharing Producer Test Cases*the Producer will allow an analyst to create an Indicator in the user interface of Producer product and then publish the content to the TXS at https://10.1.1.10/api1/collections/8c99d7d2-8a6c-4196-b216-c1692d0126f2/objects where the TXS component will not respond to the post until all objects within the bundle have been processed.
4. Verify the TXS accepts the content by verifying the following on the Producer:
	1. **HTTP Response code** is 202 Accepted
	2. **id** represents a unique identifier for each post
	3. **status** is complete
	4. **request\_timestamp** represents the time of the post
	5. **total\_count** represents the number of objects in the bundle test case
	6. **success\_count** is the same as total\_count
	7. **successes** is an array of the object identifiers in the submitted bundle and matches the identifiers posted for each indicator
	8. **failure\_count** is 0
	9. **pending\_count** is 0
5. Verify that the Producer shows that the content shared to the TXS is visually shown to the user that the content was accepted successfully by the TXS.

**Setup B Behavior - Read-Write Collection**1. Producer does a GET on the Read-Write collection [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)91a7b528-80eb-42ed-a74d-bd5a2118
2. Verify at the Producer that the TXS responds with the following information:
	1. **HTTP Response Code** is 200 OK
	2. **id** is 91a7b528-80eb-42ed-a74d-bd5a2118
	3. **title** is “Read-Write Collection 1”
	4. **description** is “This is Read-Write Collection 1”
	5. **can\_read** is true
	6. **can\_write** is true
	7. **media\_types** is "application/stix+json; version=2.0"
3. For each section described in *Part1: Indicator Sharing Producer Test Cases* the Producer will allow an analyst to create an Indicator in the user interface of Producer product and then publish the content to the TXS at [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)91a7b528-80eb-42ed-a74d-bd5a2118/objects where the TXS component will not respond to the post until all objects within the bundle have been processed
4. Verify the TXS accepts the content by verifying the following on the Producer:
	1. **HTTP Response code** is 202 Accepted
	2. **id** represents a unique identifier for each post
	3. **status** is complete
	4. **request\_timestamp** represents the time of the post
	5. **total\_count** represents the number of objects in the bundle test case
	6. **success\_count** is the same as total\_count
	7. **successes** is an array of the object identifiers in the submitted bundle and matches the identifiers posted for each indicator
	8. **failure\_count** is 0
	9. **pending\_count** is 0
5. Verify that the Producer shows that the content shared to the TXS is visually shown to the user that the content was accepted successfully by the TXS.
 |

### 2.4.4 Producer Test Case Data

#### 2.4.4.1 Verify Collection Information

**Table 2.4.4.1 - Basic GET Request and Response**

|  |  |
| --- | --- |
| **To TXS** | **From TXS** |
| GET [/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)8c99d7d2-8a6c-4196-b216-c1692d0126f2/ HTTP/1.1Host: 10.1.1.10Accept: application/vnd.oasis.taxii+json; version=2.0Authorization: Basic dGVzdDpQYXNzdzByZCE= | HTTP/1.1 200 OKContent-Type: application/vnd.oasis.taxii+json; version=2.0{ "id": "8c99d7d2-8a6c-4196-b216-c1692d0126f2", "title": "Test Collection 1", "description": "This is Test Collection 1", "can\_read": true, "can\_write": true, "media\_types": [ "application/vnd.oasis.stix+json; version=2.0" ]} |

#### 2.4.4.2 Indicator Publication

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

1. The test organization must verify that the:
	1. responses match the posted content, **and** the
	2. user interface of the Producer product shows to the user that the content was posted successfully to the TXS.

**Table 2.4.4.2 - Basic GET Request and Response**

|  |  |
| --- | --- |
| **To TXS** | **From TXS** |
| POST /api1/collections/8c99d7d2-8a6c-4196-b216-c1692d0126f2/objects/ HTTP/1.1Host: 10.1.1.10Accept: application/vnd.oasis.taxii+json; version=2.0Authorization: Basic dGVzdDpQYXNzdzByZCE=Content-Type: application/vnd.oasis.stix+json; version=2.0{  "type": "content from test table below...",} | HTTP/1.1 202 AcceptedContent-Type: application/vnd.oasis.taxii+json; version=2.0{ "id": "2d086da7-4bdc-4f91-900e-d77486753710", "status": "complete", "request\_timestamp": "2016-11-02T12:34:34.12345Z", "total\_count": 4, "success\_count": 4, "successes": [ "List of objects defined in the Part1 bundle test cases" ], "failure\_count": 0, "pending\_count": 0} |

**Table 2.4.4.3 - Test Case Total Object Count Requirement**

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

|  |  |
| --- | --- |
| **Test Cases** | **Total Count Checks** |
| ​2.4.4.3.1 Indicator IPv4 Address | 2 |
| ​2.4.4.3.2 Indicator IPv4 Address CIDR | 2 |
| 2.4.4.3.3 Two Indicators with IPv4 Address CIDR | 2 |
| 2.4.4.3.4 Indicator with IPv6 Address | 2 |
| 2.4.4.3.5 Indicator with IPv6 Address CIDR | 2 |
| 2.4.4.3.6 Multiple Indicators within the same bundle | 3 |
| ​2.4.4.3.7 Indicator FQDN | 2 |
| ​2.4.4.3.8 Indicator URL | 2 |
| ​2.4.4.3.9 Indicator URL or FQDN | 2 |
| 2.4.4.3.10 Indicator File hash with SHA256 or MD5 values | 2 |

### 2.4.5 ​Required Respondent Support

The Respondent persona must be able to get all content according [Part1:Indicator Sharing](https://drive.google.com/open?id=1l54RhjxwuXrZUQ19zIHUiZ7_c6otbLbVVfluKJogU7s). The following behavior describes the general data flow for each test case.

**Table 2.4.5 — Respondent Object Bundling Details**

|  |  |
| --- | --- |
| Personas | **Use Case #1 Behavior (Same Organization, Different Analysts)** |
| TIP; SIEM;  | **Setup A Behavior - Read Collection**1. Respondent allows a user to select or specify the URL Address of the TXS to connect to as: <https://10.1.1.10:443> and performs the tests described in *Section 2.2: Common Connection* Tests
2. Respondent does a get on the collection [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)91a7b528-80eb-42ed-a74d-bd526120 and verifies the following information:
	1. **HTTP Response Code** is 200 OK
	2. **id** is 91a7b528-80eb-42ed-a74d-bd526120
	3. **title** is “Read Collection 1”
	4. **description** is “This is Read Collection 1”
	5. **can\_read** is true
	6. **can\_write** is false
	7. **media\_types** is "application/vnd.oasis.stix+json; version=2.0"
3. For each section described in *Part1: Indicator Sharing Producer Test Cases*the Respondent will get the content from the TXS at [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)91a7b528-80eb-42ed-a74d-bd526120 /objects and verify that each bundle returned matched the content for the respective publication test case.
4. The Respondent should also show in log files or via the user interface of the product that new intelligence has been received from the Producer and show in the log files or the user interface what intelligence including the following properties
	1. **Id** must be the uuid of the Indicator shared
	2. **created\_by\_ref** must point to the identity of the **Producer**;
	3. **created** and **modified** must match the timestamp to millisecond granularity of the original shared intelligence
	4. **name** contains the name of the Indicator
	5. **description** contains the description field of the Indicator
	6. **pattern** contains the pattern field of the Indicator
	7. **valid\_from** contains the date for the indicator valid\_from
5. The Respondent must then allow the Respondent analyst via the user interface to modify the **description** field value to “Changed Indicator Description” and allow them to publish that Indicator back to the Producer
6. *Repeat the verification steps of the original Indicator but instead performing the test with Respondent of the changed description as the Producer*

**Setup B Behavior - Read-Write Collection**1. Respondent allows a user to select or specify the URL Address of the TXS to connect to as: <https://10.1.1.10:443> and performs the tests described in *Section 2.2: Common Connection* Tests
2. Respondent does a get on the collection [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)91a7b528-80eb-42ed-a74d-bd5a2118 and verifies the following information:
	1. **HTTP Response Code** is 200 OK
	2. **id** is 91a7b528-80eb-42ed-a74d-bd5a2118
	3. **title** is “Read-Write Collection 1”
	4. **description** is “This is Read-Write Collection 1”
	5. **can\_read** is true
	6. **can\_write** is true
	7. **media\_types** is "application/vnd.oasis.stix+json; version=2.0"
3. For each section described in *Part1: Indicator Sharing Producer Test Cases*the Respondent will get the content from the TXS at https://10.1.1.10/api1/collections/91a7b528-80eb-42ed-a74d-bd5a2118/objects and verify that each bundle returned matched the content for the respective publication test case.
4. The Respondent should also show in log files or via the user interface of the product that new intelligence has been received from the Producer and show in the log files or the user interface what intelligence including the following properties
	1. **Id**
	2. **created\_by\_ref** must point to the identity of the **Producer**;
	3. **created** and **modified** must match the timestamp to millisecond granularity of the original shared intelligence
	4. **name** contains the name of the Indicator
	5. **description** contains the description field of the Indicator
	6. **pattern** contains the pattern field of the Indicator
	7. **valid\_from** contains the date for the indicator valid\_from
5. The Respondent must then allow the Respondent analyst via the user interface to modify the **description** field value to “Changed Indicator Description” and allow them to publish that Indicator back to the Producer
6. *Repeat the verification steps of the original Indicator but instead performing the test with Respondent of the changed description as the Producer*.
 |

|  |  |
| --- | --- |
| Personas | **Use Case #2 (Different Organization, Different Analysts) &** **Use Case #3 (Same Organization, Different Analysts)** |
| TIP; SIEM;  | **Setup A Behavior - Read Collection**1. Respondent allows a user to select or specify the URL Address of the TXS to connect to as: <https://10.1.1.10:443> and performs the tests described in *Section 2.2: Common Connection* Tests
2. Respondent does a get on the collection [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)91a7b528-80eb-42ed-a74d-bd526120 and verifies the following information:
	1. **HTTP Response Code** is 200 OK
	2. **id** is 91a7b528-80eb-42ed-a74d-bd526120
	3. **title** is “Read Collection 1”
	4. **description** is “This is Read Collection 1”
	5. **can\_read** is true
	6. **can\_write** is false
	7. **media\_types** is "application/stix+json; version=2.0
3. For each section described in [Part1: Indicator Sharing Producer Test Cases](https://drive.google.com/open?id=1l54RhjxwuXrZUQ19zIHUiZ7_c6otbLbVVfluKJogU7s) the Respondent will get the content from the TXS at [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)91a7b528-80eb-42ed-a74d-bd526120 and verify that each Bundle returned matched the content for the respective publication test case.
4. The Respondent should also show to the user of the product that new intelligence has been received from the Producer and show to the user what intelligence including the following properties
	1. **Id** must include the UUID of the Indicator shared
	2. **created\_by\_ref** must point to the identity of the **Producer**;
	3. **created** and **modified** must match the timestamp to millisecond granularity of the original shared intelligence
	4. **name** contains the name of the Indicator
	5. **description** contains the description field of the Indicator
	6. **pattern** contains the pattern field of the Indicator
	7. **valid\_from** contains the date for the indicator valid\_from
5. The Respondent must then 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:
	1. **Id** must include a new UUID of the Indicator being created
	2. **created\_by\_ref** must point to the identity of the **Respondent**;
	3. **created** and **modified** must match the timestamp to millisecond granularity of the original shared intelligence
	4. **name** contains the name of the new Indicator
	5. **description** contains the description field of the new Indicator
	6. **pattern** contains the pattern field of the new Indicator
	7. **valid\_from** contains the date for the indicator valid\_from
6. 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
7. *Repeat the verification steps of the original Indicator while include verification that the Producer of the original Indicator shows the new Indicator from the Respondent and its relationship to their original Indicator*

**Setup B Behavior - Read-Write Collection**1. Respondent allows a user to select or specify the URL Address of the TXS to connect to as: <https://10.1.1.10:443> and performs the tests described in *Section 2.2: Common Connection* Tests
2. Respondent does a get on the collection [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)91a7b528-80eb-42ed-a74d-bd5a2118 and verifies the following information:
	1. **HTTP Response Code** is 200 OK
	2. **id** is 91a7b528-80eb-42ed-a74d-bd5a2118
	3. **title** is “Read-Write Collection 1”
	4. **description** is “This is Read-Write Collection 1”
	5. **can\_read** is true
	6. **can\_write** is true
	7. **media\_types** is "application/vnd.oasis.stix+json; version=2.0"
3. For each section described in *Part1: Indicator Sharing Producer Test Cases*the Respondent will get the content from the TXS at [https://10.1.1.10/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)91a7b528-80eb-42ed-a74d-bd5a2118 and verify that each bundle returned matched the content for the respective publication test case.
4. The Respondent should also show to the user of the product that new intelligence has been received from the Producer and show to the user what intelligence including the following properties
	1. **Id**
	2. **created\_by\_ref** must point to the identity of the **Producer**;
	3. **created** and **modified** must match the timestamp to millisecond granularity of the original shared intelligence
	4. **name** contains the name of the Indicator
	5. **description** contains the description field of the Indicator
	6. **pattern** contains the pattern field of the Indicator
	7. **valid\_from** contains the date for the indicator valid\_from
5. The Respondent must then 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:
	1. **Id** must include a new UUID of the Indicator being created
	2. **created\_by\_ref** must point to the identity of the **Respondent**;
	3. **created** and **modified** must match the timestamp to millisecond granularity of the original shared intelligence
	4. **name** contains the name of the new Indicator
	5. **description** contains the description field of the new Indicator
	6. **pattern** contains the pattern field of the new Indicator
	7. **valid\_from** contains the date for the indicator valid\_from
6. 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
7. *Repeat the verification steps of the original Indicator while include verification that the Producer of the original Indicator shows the new Indicator from the Respondent and its relationship to their original Indicator*
 |

### 2.4.6 ​Respondent Test Case Data

#### 2.4.6.1 Indicator Get & Update Modified Intelligence

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

The test organization must verify that the:

1. responses match the posted content, **and**
2. user interface of the Respondent product shows to the user that the content was
	1. received from the TXS, and
	2. posted successfully to the TXS in response.

**Table 2.4.6.1 - Basic GET Request and Response**

|  |  |
| --- | --- |
| **To TXS** | **From TXS** |
| GET [/api1/collections/](https://10.1.1.10/api1/collections/1000/objects)91a7b528-80eb-42ed-a74d-bd5a2118/objects/ HTTP/1.1Host: 10.1.1.10Accept: application/vnd.oasis.stix+json; version=2.0Authorization: Basic dGVzdDpQYXNzdzByZCE= | HTTP/1.1 200 OKContent-Type: application/vnd.oasis.stix+json; version=2.0{  "type": "bundle", ... "objects": [ { "type": "indicator", ... } ]} |

**Table 2.4.6.2 - Test Case Total Object Count Requirement**

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

|  |  |
| --- | --- |
| **Test Cases** | **Total Count** |
| ​2.4.6.2.1 Indicator IPv4 Address | 2 |
| ​2.4.6.2.2 Indicator IPv4 Address CIDR | 2 |
| 2.4.6.2.3 Two Indicators with IPv4 Address CIDR | 2 |
| 2.4.6.2.4 Indicator with IPv6 Address | 2 |
| 2.4.6.2.5 Indicator with IPv6 Address CIDR | 2 |
| 2.4.6.2.6 Multiple Indicators within the same bundle | 3 |
| ​2.4.6.2.7 Indicator FQDN | 2 |
| 2.4.6.2.8 ​Indicator URL | 2 |
| ​2.4.6.2.9 Indicator URL or FQDN | 2 |
| 2.4.6.2.10 Indicator File hash with SHA256 or MD5 values | 2 |

#### 2.4.6.2 Indicator Get & Create Related Intelligence

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

The test organization should verify that the:

1. responses match the posted content **and** the
2. user interface of the Respondent product shows to the user that the content was
	1. received from the TXS and
	2. posted successfully to the TXS in response.

**Table 2.4.6.2 - Basic GET Request and Response**

|  |  |
| --- | --- |
| **To TXS** | **From TXS** |
| GET /api1/collections/91a7b528-80eb-42ed-a74d-bd5a2118/objects/ HTTP/1.1Host: 10.1.1.10Accept: application/stix+json; version=2.0Authorization: Basic dGVzdDpQYXNzdzByZCE= | HTTP/1.1 200 OKContent-Type: application/stix+json; version=2.0{  "type": "bundle", ... "objects": [ { "type": "indicator", ... } ]} |

**Table 2.4.6.3 - Test Case Total Object Count Requirement**

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

|  |  |
| --- | --- |
| **Test Cases** | **Total Count** |
| ​2.4.6.3.1 Indicator IPv4 Address | 2 |
| ​2.4.6.3.2 Indicator IPv4 Address CIDR | 2 |
| 2.4.6.3.3 Two Indicators with IPv4 Address CIDR | 3 |
| 2.4.6.3.4 Indicator with IPv6 Address | 2 |
| 2.4.6.3.5 Indicator with IPv6 Address CIDR | 2 |
| 2.4.6.3.6 Multiple Indicators within the same Bundle | 3 |
| ​2.4.6.3.7 Indicator FQDN | 2 |
| ​2.4.6.3.8 Indicator URL | 2 |
| ​2.4.6.3.9 Indicator URL or FQDN | 2 |
| 2.4.6.3.10 Indicator File hash with SHA256 or MD5 values | 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.**

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 use case data flows.
2. For each test, identify whether your software is a
	1. Producer, or
	2. Respondent, or
	3. TAXII Server (Part 2 use 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.
	1. 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 use case tests.
	2. 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.
		1. 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 Use 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**

|  |  |  |  |
| --- | --- | --- | --- |
| **Use 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 | n/a | n/a |
| Sighting Sharing | 2.3.5.2 Sighting + Indicator with IPv4 Address Matching CIDR | n/a | n/a |
| Sighting Sharing | 2.3.5.3 Sighting + Indicator with IPv6 Address Matching CIDR | n/a | n/a |
| Sighting Sharing | 2.3.5.4 Sighting + Indicator with NO observed data | n/a | n/a |
| Sighting Sharing | 2.3.5.5 Sighting + Indicator with URL  | n/a | n/a |
| Sighting Sharing | 2.3.5.6 Sighting + Indicator with File Hash  | n/a | n/a |
| 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**

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case** | **Test** | **Producer** | **Respondent** |
| Common Connection | 2.2.4.1 Basic TXS/TXF Get | Mandatory | na |
| Common Connection | 2.2.4.2 Basic API-Root Get | Mandatory | na |
| Common Connection | 2.2.4.3 Missing Authorization Parameter Returns Unauthorized | Mandatory | na |
| Common Connection | 2.2.4.4 Incorrect Authorization Parameter Returns Unauthorized | Mandatory | na |
| Common Connection | 2.2.4.5 Incorrect API Root Info Get Returns Not Found | Mandatory | na |
| Common Connection | 2.2.4.6 Incorrect Collection Info Get Returns Not Found | Mandatory | na |
| Basic Feed Sharing  | 2.3.4.1 Verify Collection Information | Mandatory | na |
| Basic Feed Sharing | ​2.3.4.3.1 Indicator IPv4 Address | Mandatory | na |
| Basic Feed Sharing  | ​2.3.4.3.2 Indicator IPv4 Address CIDR | Mandatory | na |
| Basic Feed Sharing | 2.3.4.3.3 Two Indicators with IPv4 Address CIDR | Mandatory | na |
| Basic Feed Sharing  | 2.3.4.3.4 Indicator with IPv6 Address | Optional | na |
| Basic Feed Sharing  | 2.3.4.3.5 Indicator with IPv6 Address CIDR | Optional | na |
| Basic Feed Sharing  | ​2.3.4.3.7 Indicator FQDN | Mandatory | na |
| Basic Feed Sharing | 2.3.4.3.8 ​Indicator URL | Mandatory | na |
| Basic Feed Sharing  | ​2.3.4.3.9 Indicator URL or FQDN | Mandatory | na |
| Basic Feed Sharing | 2.3.4.3.10 Indicator File hash with SHA256 or MD5 values | Mandatory | na |
| Basic Intel Collaboration | 2.4.4.1 Verify Collection Information | Mandatory | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.1 Indicator IPv4 Address | Publish - Mandatory | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.2 Indicator IPv4 Address CIDR | Publish - Mandatory | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.3 Two Indicators with IPv4 Address CIDR | Publish - Mandatory | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.4 Indicator with IPv6 Address | Publish - Optional | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.5 Indicator with IPv6 Address CIDR | Publish - Optional | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.6 Multiple Indicators within the same bundle | Publish - Mandatory | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.7 Indicator FQDN | Publish - Mandatory | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.8 Indicator URL | Publish - Mandatory | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.9 Indicator URL or FQDN | Publish - 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**

|  |  |  |  |
| --- | --- | --- | --- |
| **Use 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# = Use Case#)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case** | **Test** | **Producer** | **Respondent** |
| Common Connection | 2.2.4.1 Basic TXS/TXF Get | Mandatory | Mandatory |
| Common Connection | 2.2.4.2 Basic API-Root Get | Mandatory | Mandatory |
| Common Connection | 2.2.4.3 Missing Authorization Parameter Returns Unauthorized | Mandatory | Mandatory |
| Common Connection | 2.2.4.4 Incorrect Authorization Parameter Returns Unauthorized | Mandatory | Mandatory |
| Common Connection | 2.2.4.5 Incorrect API Root Info Get Returns Not Found | Mandatory | Mandatory |
| Common Connection | 2.2.4.6 Incorrect Collection Info Get Returns Not Found | Mandatory | Mandatory |
| Basic Feed Sharing | 2.3.4.1 Verify Collection Information | Mandatory | Mandatory |
| Basic Feed Sharing  | ​2.3.4.3.1 Indicator IPv4 Address | Mandatory | Mandatory |
| Basic Feed Sharing | ​2.3.4.3.2 Indicator IPv4 Address CIDR | Mandatory | Mandatory |
| Basic Feed Sharing  | 2.3.4.3.3 Two Indicators with IPv4 Address CIDR | Mandatory | Mandatory |
| Basic Feed Sharing | 2.3.4.3.4 Indicator with IPv6 Address | Mandatory | Mandatory |
| Basic Feed Sharing  | 2.3.4.3.5 Indicator with IPv6 Address CIDR | Optional | Optional |
| Basic Feed Sharing  | ​2.3.4.3.7 Indicator FQDN | Optional | Optional |
| Basic Feed Sharing  | 2.3.4.3.8 ​Indicator URL | Mandatory | Mandatory |
| Basic Feed Sharing | ​2.3.4.3.9 Indicator URL or FQDN | Mandatory | Mandatory |
| Basic Feed Sharing  | 2.3.4.3.10 Indicator File hash with SHA256 or MD5 values | Mandatory | Mandatory |
| Basic Intel Collaboration | 2.4.4.1 Verify Collection Information | Mandatory | Mandatory |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.1 Indicator IPv4 Address | Publish - Mandatory | Get & Update - MGet & Relate - M |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.2 Indicator IPv4 Address CIDR | Publish - Mandatory | Get & Update - MGet & Relate - M |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.3 Two Indicators with IPv4 Address CIDR | Publish - Mandatory | Get & Update - MGet & Relate - M |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.4 Indicator with IPv6 Address | Publish - Optional | Get & Update - OGet & Relate - O |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.5 Indicator with IPv6 Address CIDR | Publish - Optional | Get & Update - OGet & Relate - O |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.6 Multiple Indicators within the same bundle | Publish - Mandatory | Get & Update - MGet & Relate - M |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.7 Indicator FQDN | Publish - Mandatory | Get & Update - MGet & Relate - M |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.8 Indicator URL | Publish - Mandatory | Get & Update - MGet & Relate - M |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.9 Indicator URL or FQDN | Publish - Mandatory | Get & Update - MGet & Relate - 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**

|  |  |  |  |
| --- | --- | --- | --- |
| **Use 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# = Use Case#)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case** | **Test** | **Producer** | **Respondent** |
| Common Connection | 2.2.4.1 Basic TXS/TXF Get | Mandatory | Mandatory |
| Common Connection | 2.2.4.2 Basic API-Root Get | Mandatory | Mandatory |
| Common Connection | 2.2.4.3 Missing Authorization Parameter Returns Unauthorized | Mandatory | Mandatory |
| Common Connection | 2.2.4.4 Incorrect Authorization Parameter Returns Unauthorized | Mandatory | Mandatory |
| Common Connection | 2.2.4.5 Incorrect API Root Info Get Returns Not Found | Mandatory | Mandatory |
| Common Connection | 2.2.4.6 Incorrect Collection Info Get Returns Not Found | Mandatory | Mandatory |
| Basic Feed Sharing  | 2.3.4.1 Verify Collection Information | Mandatory | Mandatory |
| Basic Feed Sharing | ​2.3.4.3.1 Indicator IPv4 Address | Mandatory | M |
| Basic Feed Sharing  | ​2.3.4.3.2 Indicator IPv4 Address CIDR | Mandatory | Mandatory |
| Basic Feed Sharing | 2.3.4.3.3 Two Indicators with IPv4 Address CIDR | Mandatory | Mandatory |
| Basic Feed Sharing  | 2.3.4.3.4 Indicator with IPv6 Address | Optional | Optional |
| Basic Feed Sharing  | 2.3.4.3.5 Indicator with IPv6 Address CIDR | Optional | Optional |
| Basic Feed Sharing  | ​2.3.4.3.7 Indicator FQDN | Mandatory | Mandatory |
| Basic Feed Sharing | 2.3.4.3.8 ​Indicator URL | Mandatory | Mandatory |
| Basic Feed Sharing  | ​2.3.4.3.9 Indicator URL or FQDN | Mandatory | Mandatory |
| Basic Feed Sharing  | 2.3.4.3.10 Indicator File hash with SHA256 or MD5 values | Mandatory | Mandatory |
| Basic Intel Collaboration | 2.4.4.1 Verify Collection Information | Mandatory | Mandatory |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.1 Indicator IPv4 Address | Publish – Mandatory | Get & Update - MGet & Relate - M |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.2 Indicator IPv4 Address CIDR | Publish – Mandatory | Get & Update - MGet & Relate - M |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.3 Two Indicators with IPv4 Address CIDR | Publish - Mandatory | Get & Update - MGet & Relate - M |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.4 Indicator with IPv6 Address | Publish – Optional | Get & Update - OGet & Relate - O |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.5 Indicator with IPv6 Address CIDR | Publish - Optional | Get & Update - OGet & Relate - O |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.6 Multiple Indicators within the same bundle | Publish - Mandatory | Get & Update - MGet & Relate - M |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.7 Indicator FQDN | Publish - Mandatory | Get & Update - MGet & Relate - M |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.8 Indicator URL | Publish - Mandatory | Get & Update - MGet & Relate - M |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.9 Indicator URL or FQDN | Publish - Mandatory | Get & Update - MGet & Relate - 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 use 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 use cases.

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Use 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# = Use Case#)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case** | **Test** | **Producer** | **Respondent** |
| Common Connection | 2.2.4.1 Basic TXS/TXF Get | na | Mandatory |
| Common Connection | 2.2.4.2 Basic API-Root Get | na | Mandatory |
| Common Connection | 2.2.4.3 Missing Authorization Parameter Returns Unauthorized | na | Mandatory |
| Common Connection | 2.2.4.4 Incorrect Authorization Parameter Returns Unauthorized | na | Mandatory |
| Common Connection | 2.2.4.5 Incorrect API Root Info Get Returns Not Found | na | Mandatory |
| Common Connection | 2.2.4.6 Incorrect Collection Info Get Returns Not Found | na | Mandatory |
| Basic Feed Sharing  | 2.3.4.1 Verify Collection Information | na | Mandatory |
| Basic Feed Sharing | ​2.3.4.3.1 Indicator IPv4 Address | na | Mandatory |
| Basic Feed Sharing  | ​2.3.4.3.2 Indicator IPv4 Address CIDR | na | Mandatory |
| Basic Feed Sharing | 2.3.4.3.3 Two Indicators with IPv4 Address CIDR | na | Mandatory |
| Basic Feed Sharing  | 2.3.4.3.4 Indicator with IPv6 Address | na | Optional |
| Basic Feed Sharing  | 2.3.4.3.5 Indicator with IPv6 Address CIDR | na | Optional |
| Basic Feed Sharing  | ​2.3.4.3.7 Indicator FQDN | na | Mandatory |
| Basic Feed Sharing | 2.3.4.3.8 ​Indicator URL | na | Mandatory |
| Basic Feed Sharing  | ​2.3.4.3.9 Indicator URL or FQDN | na | Mandatory |
| Basic Feed Sharing  | 2.3.4.3.10 Indicator File hash with SHA256 or MD5 values | na | Mandatory |
| Basic Intel Collaboration | 2.4.4.1 Verify Collection Information | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.1 Indicator IPv4 Address | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.2 Indicator IPv4 Address CIDR | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.3 Two Indicators with IPv4 Address CIDR | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.4 Indicator with IPv6 Address | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.5 Indicator with IPv6 Address CIDR | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.6 Multiple Indicators within the same bundle | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.7 Indicator FQDN | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.8 Indicator URL | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.9 Indicator URL or FQDN | 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 use 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 use cases.

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Use 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# = Use Case#)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case** | **Test** | **Producer** | **Respondent** |
| Common Connection | 2.2.4.1 Basic TXS/TXF Get | na | Mandatory |
| Common Connection | 2.2.4.2 Basic API-Root Get | na | Mandatory |
| Common Connection | 2.2.4.3 Missing Authorization Parameter Returns Unauthorized | na | Mandatory |
| Common Connection | 2.2.4.4 Incorrect Authorization Parameter Returns Unauthorized | na | Mandatory |
| Common Connection | 2.2.4.5 Incorrect API Root Info Get Returns Not Found | na | Mandatory |
| Common Connection | 2.2.4.6 Incorrect Collection Info Get Returns Not Found | na | Mandatory |
| Basic Feed Sharing  | 2.3.4.1 Verify Collection Information | na | Mandatory |
| Basic Feed Sharing | ​2.3.4.3.1 Indicator IPv4 Address | na | Mandatory |
| Basic Feed Sharing  | ​2.3.4.3.2 Indicator IPv4 Address CIDR | na | Mandatory |
| Basic Feed Sharing | 2.3.4.3.3 Two Indicators with IPv4 Address CIDR | na | Mandatory |
| Basic Feed Sharing  | 2.3.4.3.4 Indicator with IPv6 Address | na | Optional |
| Basic Feed Sharing  | 2.3.4.3.5 Indicator with IPv6 Address CIDR | na | Optional |
| Basic Feed Sharing  | ​2.3.4.3.7 Indicator FQDN | na | Mandatory |
| Basic Feed Sharing | 2.3.4.3.8 ​Indicator URL | na | Mandatory |
| Basic Feed Sharing  | ​2.3.4.3.9 Indicator URL or FQDN | na | Mandatory |
| Basic Feed Sharing  | 2.3.4.3.10 Indicator File hash with SHA256 or MD5 values | na | Mandatory |
| Basic Intel Collaboration | 2.4.4.1 Verify Collection Information | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.1 Indicator IPv4 Address | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.2 Indicator IPv4 Address CIDR | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.3 Two Indicators with IPv4 Address CIDR | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.4 Indicator with IPv6 Address | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.5 Indicator with IPv6 Address CIDR | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.6 Multiple Indicators within the same bundle | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.7 Indicator FQDN | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.8 Indicator URL | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.9 Indicator URL or FQDN | 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 use cases.

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Use 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# = Use Case#)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case** | **Test** | **Producer** | **Respondent** |
| Common Connection | 2.2.4.1 Basic TXS/TXF Get | na | Mandatory |
| Common Connection | 2.2.4.2 Basic API-Root Get | na | Mandatory |
| Common Connection | 2.2.4.3 Missing Authorization Parameter Returns Unauthorized | na | Mandatory |
| Common Connection | 2.2.4.4 Incorrect Authorization Parameter Returns Unauthorized | na | Mandatory |
| Common Connection | 2.2.4.5 Incorrect API Root Info Get Returns Not Found | na | Mandatory |
| Common Connection | 2.2.4.6 Incorrect Collection Info Get Returns Not Found | na | Mandatory |
| Basic Feed Sharing  | 2.3.4.1 Verify Collection Information | na | Mandatory |
| Basic Feed Sharing | ​2.3.4.3.1 Indicator IPv4 Address | na | Mandatory |
| Basic Feed Sharing  | ​2.3.4.3.2 Indicator IPv4 Address CIDR | na | Mandatory |
| Basic Feed Sharing | 2.3.4.3.3 Two Indicators with IPv4 Address CIDR | na | Mandatory |
| Basic Feed Sharing  | 2.3.4.3.4 Indicator with IPv6 Address | na | Optional |
| Basic Feed Sharing  | 2.3.4.3.5 Indicator with IPv6 Address CIDR | na | Optional |
| Basic Feed Sharing  | ​2.3.4.3.7 Indicator FQDN | na | Mandatory |
| Basic Feed Sharing | 2.3.4.3.8 ​Indicator URL | na | Mandatory |
| Basic Feed Sharing  | ​2.3.4.3.9 Indicator URL or FQDN | na | Mandatory |
| Basic Feed Sharing  | 2.3.4.3.10 Indicator File hash with SHA256 or MD5 values | na | Mandatory |
| Basic Intel Collaboration | 2.4.4.1 Verify Collection Information | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.1 Indicator IPv4 Address | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.2 Indicator IPv4 Address CIDR | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.3 Two Indicators with IPv4 Address CIDR | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.4 Indicator with IPv6 Address | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.5 Indicator with IPv6 Address CIDR | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.6 Multiple Indicators within the same bundle | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.7 Indicator FQDN | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.8 Indicator URL | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.9 Indicator URL or FQDN | 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 use cases.

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case** | **Test** | **Producer** | **Respondent** |
| Common Connection | 2.2.4.1 Basic TXS/TXF Get | na | Mandatory |
| Common Connection | 2.2.4.2 Basic API-Root Get | na | Mandatory |
| Common Connection | 2.2.4.3 Missing Authorization Parameter Returns Unauthorized | na | Mandatory |
| Common Connection | 2.2.4.4 Incorrect Authorization Parameter Returns Unauthorized | na | Mandatory |
| Common Connection | 2.2.4.5 Incorrect API Root Info Get Returns Not Found | na | Mandatory |
| Common Connection | 2.2.4.6 Incorrect Collection Info Get Returns Not Found | na | Mandatory |
| Basic Feed Sharing  | 2.3.4.1 Verify Collection Information | na | Mandatory |
| Basic Feed Sharing | ​2.3.4.3.1 Indicator IPv4 Address | na | Mandatory |
| Basic Feed Sharing  | ​2.3.4.3.2 Indicator IPv4 Address CIDR | na | Mandatory |
| Basic Feed Sharing | 2.3.4.3.3 Two Indicators with IPv4 Address CIDR | na | Mandatory |
| Basic Feed Sharing  | 2.3.4.3.4 Indicator with IPv6 Address | na | Mandatory |
| Basic Feed Sharing  | 2.3.4.3.5 Indicator with IPv6 Address CIDR | na | Mandatory |
| Basic Feed Sharing  | ​2.3.4.3.7 Indicator FQDN | na | Mandatory |
| Basic Feed Sharing | 2.3.4.3.8 ​Indicator URL | na | Mandatory |
| Basic Feed Sharing  | ​2.3.4.3.9 Indicator URL or FQDN | na | Mandatory |
| Basic Feed Sharing  | 2.3.4.3.10 Indicator File hash with SHA256 or MD5 values | na | Mandatory |
| Basic Intel Collaboration | 2.4.4.1 Verify Collection Information | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.1 Indicator IPv4 Address | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.2 Indicator IPv4 Address CIDR | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.3 Two Indicators with IPv4 Address CIDR | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.4 Indicator with IPv6 Address | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.5 Indicator with IPv6 Address CIDR | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.6 Multiple Indicators within the same bundle | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.7 Indicator FQDN | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.8 Indicator URL | na | na |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.9 Indicator URL or FQDN | 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 use cases.

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case** | **Test** | **Producer** | **Respondent** |
| Common Connection | 2.2.4.1 Basic TXS/TXF Get | Mandatory | Mandatory |
| Common Connection | 2.2.4.2 Basic API-Root Get | Mandatory | Mandatory |
| Common Connection | 2.2.4.3 Missing Authorization Parameter Returns Unauthorized | Mandatory | Mandatory |
| Common Connection | 2.2.4.4 Incorrect Authorization Parameter Returns Unauthorized | Mandatory | Mandatory |
| Common Connection | 2.2.4.5 Incorrect API Root Info Get Returns Not Found | Mandatory | Mandatory |
| Common Connection | 2.2.4.6 Incorrect Collection Info Get Returns Not Found | Mandatory | Mandatory |
| Basic Feed Sharing  | 2.3.4.1 Verify Collection Information | Mandatory | Mandatory |
| Basic Feed Sharing | ​2.3.4.3.1 Indicator IPv4 Address | Mandatory | Mandatory |
| Basic Feed Sharing  | ​2.3.4.3.2 Indicator IPv4 Address CIDR | Mandatory | Mandatory |
| Basic Feed Sharing | 2.3.4.3.3 Two Indicators with IPv4 Address CIDR | Mandatory | Mandatory |
| Basic Feed Sharing  | 2.3.4.3.4 Indicator with IPv6 Address | Mandatory | Mandatory |
| Basic Feed Sharing  | 2.3.4.3.5 Indicator with IPv6 Address CIDR | Mandatory | Mandatory |
| Basic Feed Sharing  | ​2.3.4.3.7 Indicator FQDN | Mandatory | Mandatory |
| Basic Feed Sharing | 2.3.4.3.8 ​Indicator URL | Mandatory | Mandatory |
| Basic Feed Sharing  | ​2.3.4.3.9 Indicator URL or FQDN | Mandatory | Mandatory |
| Basic Feed Sharing  | 2.3.4.3.10 Indicator File hash with SHA256 or MD5 values | Mandatory | Mandatory |
| Basic Intel Collaboration | 2.4.4.1 Verify Collection Information | Mandatory | Mandatory |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.1 Indicator IPv4 Address | Mandatory | Mandatory |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.2 Indicator IPv4 Address CIDR | Mandatory | Mandatory |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.3 Two Indicators with IPv4 Address CIDR | Mandatory | Mandatory |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.4 Indicator with IPv6 Address | Mandatory | Mandatory |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.5 Indicator with IPv6 Address CIDR | Mandatory | Mandatory |
| Basic Intel Collaboration (UC1, UC2, UC3) | 2.4.4.3.6 Multiple Indicators within the same bundle | Mandatory | Mandatory |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.7 Indicator FQDN | Mandatory | Mandatory |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.8 Indicator URL | Mandatory | Mandatory |
| Basic Intel Collaboration (UC1, UC2, UC3) | ​2.4.4.3.9 Indicator URL or FQDN | Mandatory | Mandatory |

#

# 4 ​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:

**Participants:**

The following individuals were members of the OASIS CTI Technical Committee during the creation of this specification and their contributions are gratefully acknowledged:

|  |  |  |
| --- | --- | --- |
| First Name | Last Name | Company |
| 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 |
| Wei | Huang | Anomali |
| Angela | Nichols | Anomali |
| Hugh | Njemanze | Anomali |
| Katie | Pelusi | Anomali |
| Nicholas | Hayden | Anomali |
| Dean | Thompson | Australia and New Zealand Banking Group (ANZ Bank) |
| Alexander | Foley | Bank of America |
| 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 |
| Sarah | Kelley | CIS |
| Syam | Appala | Cisco Systems |
| Ted | Bedwell | Cisco Systems |
| David | McGrew | Cisco Systems |
| Mark-David | McLaughlin | 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) |
| Ben | Ottoman | Cyber Threat Intelligence Network, Inc. (CTIN) |
| David | Powell | Cyber Threat Intelligence Network, Inc. (CTIN) |
| Andreas | Sfakianakis | Cyber Threat Intelligence Network, Inc. (CTIN) |
| Jane | Ginn | 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) |
| Phillip | Boles | FireEye, Inc. |
| Prasad | Gaikwad | FireEye, Inc. |
| Will | Green | FireEye, Inc. |
| Rajeev | Jha | FireEye, Inc. |
| Anuj | Kumar | FireEye, Inc. |
| James | Meck | FireEye, Inc. |
| Scott | Shreve | FireEye, Inc. |
| Jon | Warren | FireEye, Inc. |
| Remko | Weterings | FireEye, Inc. |
| Sean | Barnum | FireEye, Inc. |
| Shyamal | Pandya | FireEye, Inc. |
| Paul | Patrick | FireEye, Inc. |
| Tim | Jones | ForeScout |
| Gavin | Chow | Fortinet Inc. |
| Steve | Fossen | Fortinet Inc. |
| Kenichi | Terashita | Fortinet Inc. |
| Daisuke | Murabayashi | Fujitsu Limited |
| Derek | Northrope | Fujitsu Limited |
| Ryusuke | Masuoka | Fujitsu Limited |
| Toshitaka | Satomi | Fujitsu Limited |
| Koji | Yamada | Fujitsu Limited |
| Kunihiko | Yoshimura | Fujitsu Limited |
| David | Lemire | G2 |
| Jonathan | Algar | GDS |
| Adam | Cooper | GDS |
| Mike | McLellan | GDS |
| Tyrone | Nembhard | GDS |
| Chris | O'Brien | GDS |
| James | Penman | GDS |
| Howard | Staple | GDS |
| Chris | Taylor | GDS |
| Laurie | Thomson | GDS |
| Alastair | Treharne | GDS |
| Julian | White | GDS |
| Bethany | Yates | GDS |
| Iain | Brown | 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. |
| Akihito | Sawada | Hitachi, Ltd. |
| Yutaka | Takami | Hitachi, Ltd. |
| Kazuo | Noguchi | Hitachi, Ltd. |
| Masato | Terada | Hitachi, Ltd. |
| Adrian | Bishop | Huntsman Security |
| Eldan | Ben-Haim | IBM |
| Allen | Hadden | IBM |
| Sandra | Hernandez | IBM |
| Chenta | Lee | IBM |
| Devesh | Parekh | IBM |
| Laura | Rusu | IBM |
| Jason | Keirstead | IBM |
| John | Morris | IBM |
| Ron | Williams | IBM |
| Paul | Martini | iboss, Inc. |
| Vasileios | Mavroeidis | IFI |
| Jerome | Athias | Individual |
| Joerg | Eschweiler | Individual |
| Alex | Pinto | 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 |
| Michael | Slavick | Kaiser Permanente |
| Beth | Pumo | Kaiser Permanente |
| Gus | Creedon | Logistics Management Institute |
| Wesley | Brown | LookingGlass |
| Himanshu | Kesar | LookingGlass |
| Ian | Truslove | LookingGlass |
| Chris | Wood | LookingGlass |
| Jamison | Day | LookingGlass |
| Dennis | Hostetler | LookingGlass |
| Allan | Thomson | LookingGlass |
| Kent | Landfield | McAfee |
| Richard | Struse | Mitre Corporation |
| Desiree | Beck | Mitre Corporation |
| Michael | Chisholm | Mitre Corporation |
| Sam | Cornwell | Mitre Corporation |
| Michael | Kouremetis | Mitre Corporation |
| Nicole | Parrish | Mitre Corporation |
| Larry | Rodrigues | Mitre Corporation |
| Jon | Salwen | Mitre Corporation |
| Charles | Schmidt | Mitre Corporation |
| Alex | Tweed | Mitre Corporation |
| Emmanuelle | Vargas-Gonzalez | Mitre Corporation |
| Greg | Back | Mitre Corporation |
| Jonathan | Baker | Mitre Corporation |
| Ivan | Kirillov | Mitre Corporation |
| Chris | Lenk | Mitre Corporation |
| Richard | Piazza | 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 |
| Joe | Brule | National Security Agency |
| Jessica | Fitzgerald-McKay | National Security Agency |
| David | Kemp | National Security Agency |
| Shaun | McCullough | National Security Agency |
| Jason | Romano | National Security Agency |
| Michael | Pepin | NC4 |
| Benjamin | Yates | NC4 |
| John | Anderson | NC4 |
| Michael | Butt | NC4 |
| Mark | Davidson | NC4 |
| Daniel | Dye | NC4 |
| Natalie | Suarez | NC4 |
| Sarah | Brown | NCI Agency |
| Oscar | Serrano | NCI Agency |
| Daichi | Hasumi | NEC Corporation |
| Lauri | Korts-P‰rn | NEC Corporation |
| Takahiro | Kakumaru | NEC Corporation |
| Danny | Purcell | New Context Services, Inc. |
| Trey | Darley | New Context Services, Inc. |
| John-Mark | Gurney | New Context Services, Inc. |
| Christian | Hunt | 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 |
| Aharon | Chernin | Perch |
| Dave | Eilken | Perch |
| Sourabh | Satish | Phantom |
| Philip | Royer | Phantom |
| John | Tolbert | Queralt Inc. |
| Jay | Heidecker | Seekintoo |
| Joseph | Brand | Semper Fortis Solutions |
| Duncan | Sparrell | sFractal Consulting LLC |
| Thomas | Schreck | Siemens AG |
| Rob | Roel | Southern California Edison |
| Armen | Tashjian | Southern California Edison |
| Dave | Cridland | Surevine Ltd. |
| Chris | Larsen | Symantec Corp. |
| Efrain | Ortiz | Symantec Corp. |
| Mingliang | Pei | Symantec Corp. |
| Kenneth | Schneider | Symantec Corp. |
| Arnaud | Taddei | Symantec Corp. |
| Brian | Witten | Symantec Corp. |
| Bret | Jordan | Symantec Corp. |
| Robert | Keith | Symantec Corp. |
| Curtis | Kostrosky | Symantec Corp. |
| Michael | Mauch | Symantec Corp. |
| Aubrey | Merchant | Symantec Corp. |
| Juha | Haaga | Synopsys |
| 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. |
| 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 |
| Ehab | Al-Shaer | UNCC |
| Bill | Chu | UNCC |
| Eoghan | Casey | US Department of Defense (DoD) |
| 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 |
| Eric | Osterweil | VeriSign |
| Lee | Chieffalo | Viasat |
| Wilson | Figueroa | Viasat |
| Andrew | May | Viasat |
| Ales | Cernivec | XLAB |
| Anthony | Rutkowski | Yanna Technologies LLC |

#

#

# 5 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 ThomsonJason 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
 |

1. 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. [↑](#footnote-ref-1)
2. The test case behavior for Use Case #1, Use Case #2 and Use Case #3 are the same the Producers [↑](#footnote-ref-2)