STIX/TAXII™ 2.0 Interoperability Test Document - Part 1

V1.0 Final Draft 03

14 July 2017

Technical Committee:

OASIS Cyber Threat Intelligence (CTI) TC

Chair:

Richard Struse (rjs@mitre.org) Mitre Corporation

Editors:

Allan Thomson (athomson@lookingglasscyber.com), LookingGlass
Jason Keirstead (jason.keirstead@ca.ibm.com), IBM

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 1 of the Interoperability test document to supplement the five-part Structured Threat Information Expression (STIX) 2.0 specification developed by the Cyber Threat Intelligence Technical Committee (CTI TC) of the Organization for the Advancement of Structured Information Systems (OASIS). The is the first in a series that will be developed concurrent with revisions to the STIX specification. This test document provides detailed requirements on how producers of products within the threat intelligence ecosystem may demonstrate conformity with STIX 2.0 if they wish to self-certify that their software is verified as interoperable. There are five personas detailed in Part 1 of this specification. These are: Data Feed Provider (DFP), Threat Intelligence Platform (TIP), Threat Mitigation System (TMS), Threat Detection System (TDS) and Security Incident and Event Management (SIEM). This interoperability test document defines tests of the following use cases: indicator sharing, sighting sharing, versioning, data markings, custom objects and properties, and course of action sharing. For each of these use cases the document details the Producer support and the Respondent support to be used for the test cases.

Status:

This Working Draft (WD) has been produced by one or more TC Members; it has not yet been voted on by the TC or approved as a Committee Note Draft. The OASIS document Approval Process 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/cnd01/stix-taxii-2-interop-p1-v1-0-cnd01.docx

Permanent “Latest version” URI:
http://docs.oasis-open.org/cti/stix-taxii-2-interop/v1.0/stix-taxii-2-interop-p1-v1-0.docx

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

Table of Contents

1 Introduction

This document details Part 1 of the Structured Threat Information Expression (STIX) 2.0 Interoperability Test Documents. It lists a set of use cases that a persona must follow as they develop minimally viable STIX compliant tools and services. To claim STIX interoperability compliance certification, persona tools/services must adhere to expected behaviors and outcomes as detailed in the use cases.

As tests will be developed separately and as the requirements are identified by industry involvement, the test documents will be broken into a series of parts. This document is Part 1. Subsequent documents will be created and numbered Part 2, Part 3, ...etc. Each test document will describe what personas and test cases are covered in that specific document version.

The Organization for the Advancement of Structured Information Standards (OASIS) Cyber Threat Intelligence Technical Committee (CTI TC) recommends users of this test document become familiar with the STIX 2.0 Core Concepts, and STIX 2.0 Objects, and other supporting specifications (as given in the Related Work section above) prior to implementing the use cases in this document. An organization must submit the results for their specific tests 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. Further submittal instructions are found in Section 3 Persona Checklists.

NOTE: The STIX & TAXII specifications contain normative references to other specifications with which an implementation may need to comply in order to comply with these specifications. This document assumes that such requirements are also met.

1.1 Terminology

Security Infrastructure - Any software or hardware instance that provides a function in the support of securing networks
Security Personnel - Any human being that is performing a security function within an organization including threat analysis; security operations; network operations...etc.
Producer - A software instance that creates STIX 2.0 content to share with other systems.
Respondent - A software instance that reads STIX 2.0 content and performs some action on that received data.

1.2 Overview

The approach that is being taken within the CTI TC is to rely primarily on well-defined, common use cases to drive the demonstration of interoperability between products using STIX 2.0 and the Trusted Automated Exchange for Indicator Information (TAXII) version 2.0, also under development within the CTI TC. Section 2 of this document outlines these common use cases for companies seeking to develop and demonstrate interoperability.

These use cases will enable personas (defined herein) of the cyber threat intelligence information sharing community to build and test information sharing files that are compliant with STIX 2.0 best practices. Future revisions to STIX 2.0 will be incorporated into a new version of this document.

1.2.1 Statement on OPTIONAL Properties as defined in STIX 2.0

Throughout this document, there will be numerous occurrences of required support for STIX 2.0 properties which are defined as OPTIONAL in the STIX 2.0 specification. These occurrences can be found in required producer persona support, as well as test cases. In these situations, producers must produce data containing these OPTIONAL properties in order to demonstrate interoperability compliance as defined in this document. Correspondingly, a respondent must properly process these OPTIONAL properties to demonstrate interoperability.

1.2.2 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 courses of action and other threat mitigations such as a firewall or IPS, Endpoint Detection and Response (EDR) software, etc.
- Threat Detection System (`TDS`)
    - Software instance of any network product that monitors, detects and alerts such as Intrusion Detection Software (IDS), Endpoint Detection and Response (EDR) software, web proxy, etc.

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

For documenting self-certification for each persona tested, refer to the checklist and test requirements in Section 3 Persona Checklist of this document.

2 Use Case Details

Part 1 use cases are broken down into a common set of use cases for each persona and an optional set of use cases.

The following use cases are captured in this document.

Table 1 - List of STIX Interoperability Use Cases

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

The following sections provide details on these use cases.

2.1 Common Use Case Requirements

In all test cases throughout this specification two aspects are used throughout.

1. Identities Created
    a. All tests require the creation of an identity for the **created_by_ref** property across all tests.
    b. The Identity created should represent the organization that is responsible for the software instance under test.
    c. The following properties should be filled in:
        i. **type** with value ‘identity’
        ii. **name** with a value that represents the organization’s name
        iii. **identity_class** with value ‘organization’
        iv. **id** with a unique UUID
        v. Example:

```
“type": "identity",
"name": "ACME Corp, Inc.",
"identity_class": "organization",
"id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
```

2. Bundles
    a. STIX 2.0 specification allows object references that are not distributed within the same bundle. However, for simplicity and test purposes only, this specification chooses to define all tests using a single Bundle to distribute all of the content being created.
    b. Future tests may verify cross-Bundle object references.
    c. Unless otherwise specified by a test description, all objects created and referenced by that test case must be contained within the same Bundle produced by the persona under test.

2.2 Indicator Sharing

One of the most common use cases that has emerged within enterprises tracking threat intelligence globally and/or within Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) has been the sharing of STIX Indicator objects using a threat intelligence platform (TIP) that integrates one or multiple Data Feed Providers (DFPs). The term-of-art that has emerged over time for the Indicator object is as an “indicator of compromise” (IOC) which is referenced regularly throughout the industry. It is also used periodically in this document.

IOCs and other STIX data objects (SDOs), as defined in the STIX 2.0 Specification, may be shared via proprietary feeds, open source feeds and/or through a sharing community. The TIP is used to aggregate and process the data and then map it to the STIX 2.0 data model. Some TIPs also provide for data enrichment, analysis and indexing, visualization and bi-directional IOC sharing with other security products through well-crafted application programming interfaces (APIs). The Respondents of the SDOs include both the personas documented in this Committee Note for machine readable threat intelligence (MRTI) and human analysts including, but not limited to: threat intelligence analysts, fraud and risk analysts, malware analysts, and network and endpoint guardians, among others. This high-level view is useful for illustrating how a use case (in this case, sharing of Indicator objects) and a persona will work together within this Committee Note for the purpose of interoperability demonstration.

The following sections provide more detailed descriptions of how a STIX 2.0 Indicator object may be used for the purpose of demonstrating interoperability.

2.2.1 Description

A STIX 2.0 Indicator is an object primarily used to identify malicious content where the content is identified by STIX Cyber Observables content (STIX top level data objects that capture this kind of activity). There are several common characteristics of data that will be verified. The TIP producer persona, shown on Figure 2-1 operated by the “Analyst”, has identified one or more Indicators that indicate malicious content on the Internet. That content may be an entity of interest to consider for monitoring activity. Also shown is how a TIP processes a STIX Bundle, and it illustrates how the information is published as a Bundle to a TMS, which then issues a response.

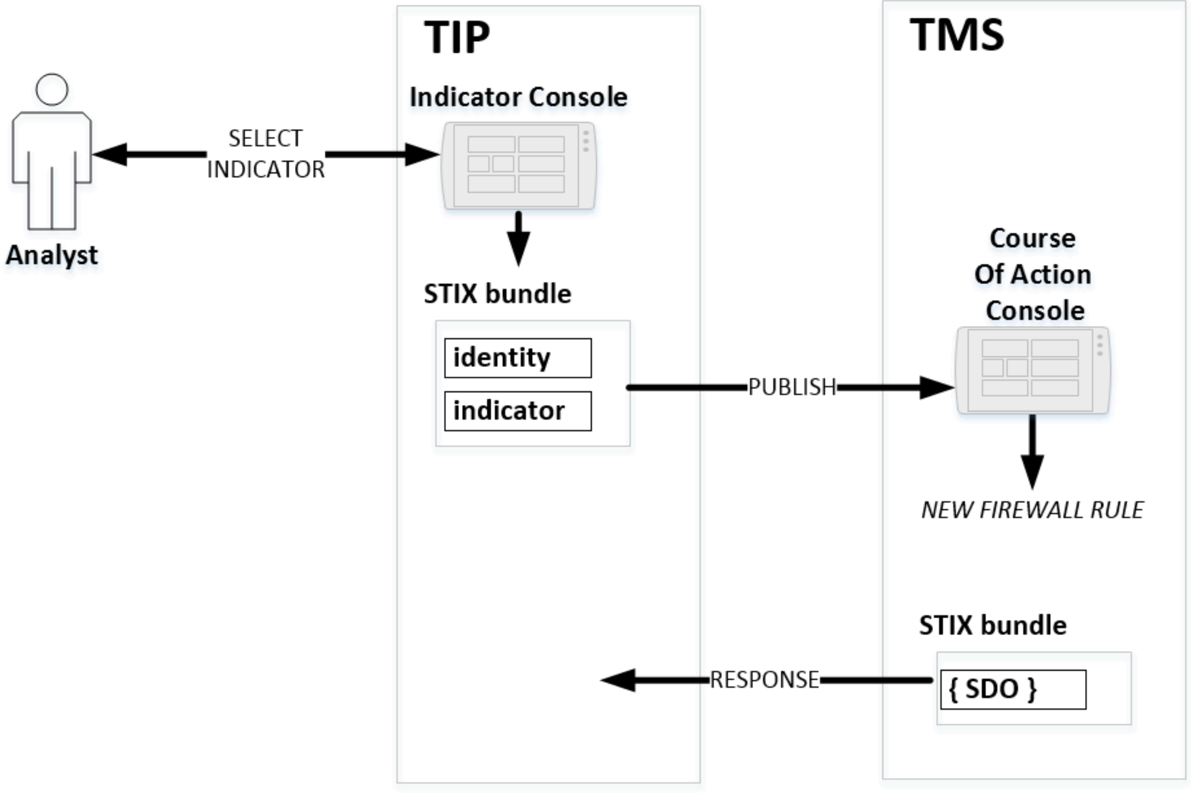

Figure 1 - An analyst shares an indicator

2.2.2 Required Producer Persona Support

The Producer persona must be able to create a STIX Bundle with one or more indicators such as IP Address v4; IP Address v6 for all Classless Inter-Domain Routing (CIDR) variations, and options.

Table 2 - Producer Object Bundling Details

Personas	Behavior
`DFP; TIP`	1. Producer allows a user to select or specify the IP Address associated with Actor A and identify that Actor A’s IP address as an Indicator of Compromise (IOC) to share to a Respondent persona. 2. The following data must be verified in the STIX bundle produced by the persona: a) A bundle object must conform to mandatory attributes within the bundle object including 'type'; 'id'; 'spec_version' and 'objects' where i) **id** has a globally unique identifier ii) **spec_version** is '2.0' iii) Within the **objects** array 1) at least one Identity for the organization of the Producer 2) at least one Indicator with the IP Address identified in the

	pattern parameter b) The Identity object must conform to mandatory attributes within the identity object spec including 'type'; 'name'; 'identity_class' and 'id' where i) **type** is 'identity' ii) **id** has a globally unique identifier iii) **identity_class** is specified by the organization of the Producer iv) **name** is the name that the Producer wishes to associate with the identity object c) The Indicator object must conform to mandatory attributes including 'type'; 'id'; 'created_by_ref'; 'created'; 'modified'; 'pattern'' where i) **created_by_ref** must point to the identity of the Producer; ii) **created** and **modified** must match the timestamp to millisecond granularity of when the user selected the Actor's IP address to be an IOC d) The pattern attribute captures the various required fields that must be supported by the Producer as defined in <ref 2.2.2.1>

2.2.3 Producer Test Case Data

The following subsections provide the test case data for the test.

2.2.3.1 Indicator IPv4 Address

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "labels": [
        "Malicious IP"
      ],
      "name": "Bad IP1",
      "description": "This indicator should be monitored for malicious activity",
      "pattern": "[ ipv4-addr:value: '198.51.100.1' ]",
      "valid_from": "2016-01-01T00:00:00Z"
    }
  ]
}
```

2.2.3.2 Indicator IPv4 Address CIDR

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "labels": [
        "Malicious CIDR"
      ],
      "name": "Bad IP CIDR",
      "description": "This indicator should be monitored for malicious activity",
      "pattern": "[ ipv4-addr:value: '198.51.100.12/24' ]",
      "valid_from": "2016-01-01T00:00:00Z"
    }
  ]
}
```

2.2.3.3 Two Indicators with IPv4 Address CIDR

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "labels": [
        "Malicious CIDRs"
      ],
      "name": "Bad IP Subnets",
      "description": "This indicator should be monitored for malicious activity from either
subnet",
      "pattern": "[ipv4-addr:value: '198.51.100.0/24' OR ipv4-addr:value: '196.45.200.0/24']",
      "valid_from": "2016-01-01T00:00:00Z"
    }
  ]
}
```

2.2.3.4 Indicator with IPv6 Address

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "labels": [
        "Malicious IPv6"
      ],
      "name": "Bad IPv6-1",
      "description": "This indicator should be monitored for malicious activity",
      "pattern": "[ ipv6-addr:value: '2001:0db8:85a3:0000:0000:8a2e:0370:7334' ]",
      "valid_from": "2016-01-01T00:00:00Z"
    }
  ]
}
```

2.2.3.5 Indicator with IPv6 Address CIDR

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "labels": [
        "Malicious IPv6 CIDR"
      ],
      "name": "Bad IPv6-CIDR",
      "description": "This indicator should be monitored for malicious activity",
      "pattern": "[ ipv6-addr:value: '2001:DB8::0/120' ]",
      "valid_from": "2016-01-01T00:00:00Z"
    }
  ]
}
```

2.2.3.6 Multiple Indicators within the same bundle

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd5f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "labels": [
        "Malicious CIDRs"
      ],
      "name": "Bad IP Subnets",
      "description": "This indicator should be monitored for malicious activity from either
subnet",
      "pattern": "[ipv4-addr:value: '198.51.100.0/24' OR ipv4-addr:value: '196.45.200.0/24']",
      "valid_from": "2016-01-01T00:00:00Z"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "labels": [
        "Malicious IP"
      ],
      "name": "Bad IP1",
      "description": "This indicator should be monitored for malicious activity",
      "pattern": "[ ipv4-addr:value: '198.51.100.12' ]",
      "valid_from": "2016-01-01T00:00:00Z"
    }
  ]
}
```

2.2.3.7 Indicator FQDN

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "labels": [
        "Malicious FQDN"
      ],
      "name": "Bad Domain",
      "description": "This indicator should be monitored for malicious activity",
      "pattern": "[ domain-name:value = 'www.5z8.info' ]",
      "valid_from": "2016-01-01T00:00:00Z"
    }
  ]
}
```

2.2.3.8 Indicator URL

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "labels": [
        "Malicious URL"
      ],
      "name": "Bad URL",
      "description": "This indicator should be monitored for malicious activity",
      "pattern": "[ url:value = 'https://www.5z8.info/foo' ]",
      "valid_from": "2016-01-01T00:00:00Z"
    }
  ]
}
```

2.2.3.9 Indicator URL or FQDN

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "labels": [
        "Malicious URL or Domain"
      ],
      "name": "Bad URL or Domain",
      "description": "This indicator should be monitored for malicious activity",
      "pattern": "[ url:value = 'https://www.5z8.info/foo' OR domain-name:value =
'www.5z8.info' ]",
      "valid_from": "2016-01-01T00:00:00Z"
    }
  ]
}
```

2.2.3.10 Indicator File hash with SHA256 or MD5 values

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "labels": [
        "Malicious File"
      ],
      "name": "Bad File1",
      "description": "This indicator should be monitored when distributed or communicated",
      "pattern": "[file:hashes.'SHA-256' =
'bf07a7fbb825fc0aae7bf4a1177b2b31fcf8a3feeaf7092761e18c859ee52a9c' OR file:hashes.'MD5' =
'cead3f77f6cda6ec00f57d76c9a6879f']",
      "valid_from": "2016-01-01T00:00:00Z"
    }
  ]
}
```

2.2.4 Required Respondent Support

The Respondent must be able to parse and display any indicator that has been shared with IP Address information.

Table 3 - Respondent Object Bundling Details

Persona	Behavior
`TIP`	1. TIP allows a user to receive a STIX bundle with an a. Identity and Indicator with the various required field pattern content b. Identity of the Producer c. Indicator with various required fields information contained in it 2. Once received the TIP is able to display to the user the source of the Indicator based on the identity's attribute **'name'** and the **identity_class** attribute 3. For each Indicator, the TIP is able to verify that the **created_by_ref** maps to an existing identity or one contained within the bundle received 4. For each Indicator object, the TIP is able to display that the indicator fields contained in the pattern represents an IOC.
`TMS; TDS`	1. Respondent allows the reception of a STIX bundle with a(n) a. Bundle with an identity, and Indicator with content b. Identity of the Producer c. Indicator with the content information contained in it 2. Once received the Respondent is able to verify the source of the Indicator based on the identity's attribute **'name'** and the **identity_class** attribute and determines that is an allowed source of intelligence to act upon 3. For each Indicator, the Respondent is able to verify that the created date represents an Indicator that has not been previously applied to its network monitoring function and may update its rules to match on that Indicator content 4. For each Indicator object, the Respondent is able to capture network information (packets or counts or flows) that the FileHash; IP; FQDN; URL contained in the pattern matched against. 5. Specifically, for the TMS persona, the TMS is able to block traffic based on the Indicator pattern matched within a packet sequence.
`SIEM`	1. SIEM allows the reception of a STIX Bundle with a(n) a. Bundle with an Identity and Indicator with the content

	b. Identity of the Producer c. Indicator with the content information contained in it 2. Once received the SIEM is able to verify the source of the indicator based on the Identity's attribute **'name'** and the **identity_class** attribute, and determines that it is an allowed source of intelligence to act upon 3. For each Indicator, the SIEM is able to verify that the created date represents an indicator that has not been previously applied to its event correlation and display functions, and updates its rules (if any) to match on that indicator content 4. For each Indicator object, the SIEM is able to display and/or alert upon other relevant security information it has from other event log sources (firewalls, sensors). The SIEM is able to show the overlap of previously logged indicators and incoming indicator information including FileHash, IP, FQDN, and URL. The SIEM may generate sightings based on the indicators.

2.2.5 Respondent Test Case Data

This use case is primarily testing the production of an Indicator and a Respondent's ability to parse and represent and act on the Indicator data correctly. No other data is sent from the Respondent back to the Producer.

2.3 Sighting Sharing

Another important scenario that will provide for crowdsourcing in the context of a sharing community is the use of a Sighting STIX Relationship Object (SRO). This is a unique form of a relationship object that provides for the confirmation of a "sighting" of an Indicator SDO (as evidenced by specific Cyber Observable objects) by a third-party; that is, by an Identity separate from the original Producer of an Indicator SDO. The full power of the use of trust communities within the ISAC and/or ISAO context cannot be realized without the use of this SRO. Therefore, it is an important use case to demonstrate for STIX interoperability.

2.3.1 Description

A STIX 2.0 Sighting object is an SRO primarily used to capture documentation that some entity in the network has been seen by an intelligence source. The Producer persona, shown on Figure 2.3 as an "Analyst", has selected one or more sightings observed by the supporting SIEM tool. Consequently, the SIEM publishes a STIX sighting bundle and publishes it for various receiving personas.

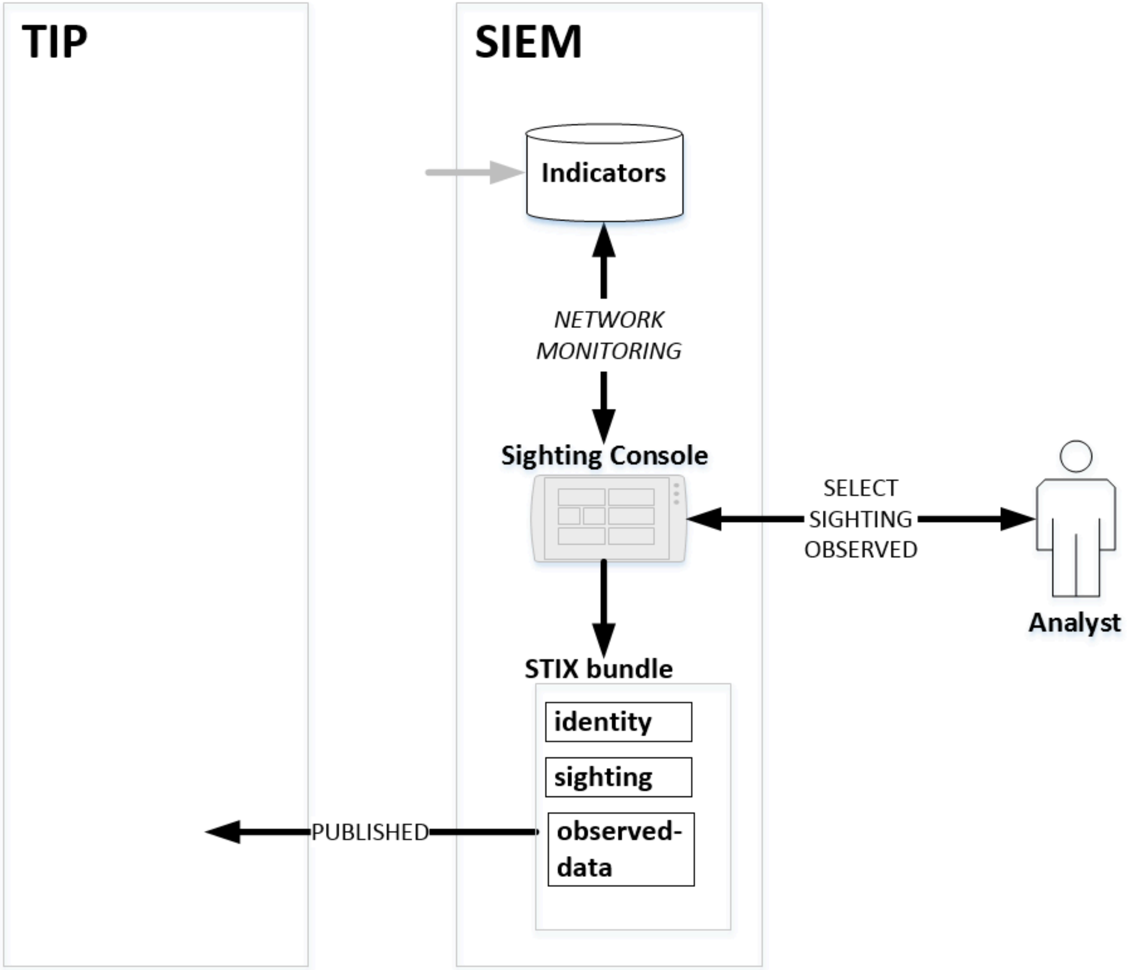

Figure 2 - An analyst reports a sighting

2.3.2 Required Producer Persona Support

The Producer persona must be able to create a STIX bundle with one or more Indicators as identified by the Indicator Sharing Producer Test Case Data. All personas defined in Required Producer Persona Support are also defined for Sighting Producer personas.

2.3.3 Producer Test Case Data

Same as Indicator Sharing Producer Test Case Data.

2.3.4 Required Respondent Persona Support

The Respondent must be able to parse and display any Indicator that has been shared as well as create a Sighting associated with the Indicator.

Table 4 - Producer Object Bundling Details

Persona	Behavior
`TIP; SIEM`	1. Respondent supports all Respondent required behavior for Indicator tests. 2. Respondent allows the user to create or select a Sighting object observed and associated with each Indicator pattern identified in the Producer's bundle. 3. Respondent in response allows user to send the Sighting information back to the Producer and supports creation of a bundle with a. its own identity unique and different from the Producer b. a reference to each Indicator shared from the Producer c. a Sighting object d. An Observed Data object 4. The sighting object must have a. **created_by_ref** must point to the identity of the Respondent; b. **created** and **modified** must match the timestamp to millisecond granularity of when the Sighting was created by the Respondent **c.** **first_seen** and **last_seen** must match when the observed data was first and last seen by the system reporting the observed data d. **count** must match the number of times that the Indicator was seen during the first and last seen values e. **sighting_of_ref** must match the Indicator sent by Producer 5. The Observed Data object must have a. **created_by_ref** must point to the identity of the Respondent; b. **created** and **modified** must match the timestamp to millisecond granularity of when the observed-data was created by the system producing the observed-data **c.** **first_observed** and **last_observed** must match when the

	observed data was first and last seen by the system reporting the Observed Data d. **number_observed** must match the number of times that the Indicator was seen during the start and stop values e. **objects** must match an Indicator pattern defined by the Producer.
`TMS`	In addition to the verification steps shown in the above row for `TIP; SIEM`, the `TMS` SHALL provide evidence that it blocked the traffic identified by the patterns in the Indicator.
`TDS`	In addition to the verification steps shown in the above row for `TIP; SIEM` the `TDS` SHALL show or provide statistics on how many packets or sessions matched the Indicator content.

2.3.5 Respondent Test Case Data

The following subsections provide the test case data for the test.

2.3.5.1 Sighting + Indicator with IPv4 Address

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp Sighting, Inc.",
      "identity_class": "organization",
      "id": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "sighting",
      "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c75",
      "created_by_ref": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:08:31.000Z",
      "modified": "2016-04-06T20:08:31.000Z",
      "first_seen": "2015-12-21T19:00:00Z",
      "last_seen": "2015-12-21T19:00:00Z",
      "count": 50,
      "sighting_of_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "observed_data_refs": [
        "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf"
      ],
      "where_sighted_refs": [
        "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff"
      ]
    },
    {
      "type": "observed-data",
      "id": "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf",
      "created_by_ref": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T19:58:16.000Z",
      "modified": "2016-04-06T19:58:16.000Z",
      "first_observed": "2015-12-21T19:00:00Z",
      "last_observed": "2016-04-06T19:58:16Z",
      "number_observed": 1,
      "objects": {
        "0": {
          "type": "ipv4-addr",
          "value": "198.51.100.1"
        }
      }
    }
  ]
}
```

2.3.5.2 Sighting + Indicator with IPv4 Address Matching CIDR

```
{
 "type": "bundle",
 "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
 "spec_version": "2.0",
 "objects": [
  {
   "type": "identity",
   "name": "ACME Corp Sighting, Inc.",
   "identity_class": "organization",
   "id": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff"
  },
  {
   "type": "sighting",
   "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c75",
   "created_by_ref": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff",
   "created": "2016-04-06T20:08:31.000Z",
   "modified": "2016-04-06T20:08:31.000Z",
   "first_seen": "2015-12-21T19:00:00Z",
   "last_seen": "2015-12-21T19:00:00Z",
   "count": 50,
   "sighting_of_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
   "observed_data_refs": [
    "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf"
   ],
   "where_sighted_refs": [
    "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff"
```

```
      ]
    },
    {
      "type": "observed-data",
      "id": "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf",
      "created_by_ref": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T19:58:16.000Z",
      "modified": "2016-04-06T19:58:16.000Z",
      "first_observed": "2015-12-21T19:00:00Z",
      "last_observed": "2016-04-06T19:58:16Z",
      "number_observed": 1,
      "objects": {
        "0": {
          "type": "ipv4-addr",
          "value": "198.51.100.12"
        }
      }
    }
  ]
}
```

2.3.5.3 Sighting + Indicator with IPv6 Address Matching CIDR

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp Sighting, Inc.",
      "identity_class": "organization",
      "id": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "sighting",
      "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c75",
      "created_by_ref": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:08:31.000Z",
      "modified": "2016-04-06T20:08:31.000Z",
      "first_seen": "2015-12-21T19:00:00Z",
      "last_seen": "2015-12-21T19:00:00Z",
      "count": 50,
      "sighting_of_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "observed_data_refs": [
        "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf"
      ],
      "where_sighted_refs": [
        "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff"
      ]
    },
    {
      "type": "observed-data",
      "id": "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf",
      "created_by_ref": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T19:58:16.000Z",
      "modified": "2016-04-06T19:58:16.000Z",
      "first_observed": "2015-12-21T19:00:00Z",
      "last_observed": "2016-04-06T19:58:16Z",
      "number_observed": 1,
      "objects": {
        "0": {
          "type": "ipv6-addr",
          "value": "2001:0db8:85a3:0000:0000:8a2e:0370:7334"
        }
      }
    }
  ]
}
```

2.3.5.4 Sighting + Indicator with NO observed data

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp Sighting, Inc.",
      "identity_class": "organization",
      "id": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "sighting",
      "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c75",
      "created_by_ref": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:08:31.000Z",
      "modified": "2016-04-06T20:08:31.000Z",
      "first_seen": "2015-12-21T19:00:00Z",
      "last_seen": "2015-12-21T19:00:00Z",
      "count": 50,
      "sighting_of_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "where_sighted_refs": [
        "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff"
      ]
    }
  ]
}
```

2.3.5.5 Sighting + Indicator with URL

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp Sighting, Inc.",
      "identity_class": "organization",
      "id": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "sighting",
      "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c75",
      "created_by_ref": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:08:31.000Z",
      "modified": "2016-04-06T20:08:31.000Z",
      "first_seen": "2015-12-21T19:00:00Z",
      "last_seen": "2015-12-21T19:00:00Z",
      "count": 50,
      "sighting_of_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "observed_data_refs": [
        "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf"
      ],
      "where_sighted_refs": [
        "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff"
      ]
    },
    {
      "type": "observed-data",
      "id": "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf",
      "created_by_ref": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T19:58:16.000Z",
      "modified": "2016-04-06T19:58:16.000Z",
      "first_observed": "2015-12-21T19:00:00Z",
      "last_observed": "2016-04-06T19:58:16Z",
      "number_observed": 1,
      "objects": {
        "0": {
          "type": "url",
          "Value": "http://www.matchthis.com/t1"
        }
      }
    }
  ]
}
```

2.3.5.6 Sighting + Indicator with File Hash

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp Sighting, Inc.",
      "identity_class": "organization",
      "id": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "sighting",
      "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c75",
      "created_by_ref": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:08:31.000Z",
      "modified": "2016-04-06T20:08:31.000Z",
      "first_seen": "2015-12-21T19:00:00Z",
      "last_seen": "2015-12-21T19:00:00Z",
      "count": 1,
      "sighting_of_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "observed_data_refs": [
        "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf"
      ],
      "where_sighted_refs": [
        "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff"
      ]
    },
    {
      "type": "observed-data",
      "id": "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf",
      "created_by_ref": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T19:58:16.000Z",
      "modified": "2016-04-06T19:58:16.000Z",
      "first_observed": "2015-12-21T19:00:00Z",
      "last_observed": "2016-04-06T19:58:16Z",
      "count": 1,
      "objects": {
        "0": {
          "type": "file",
          "hashes": {
            "MD5": "4472ea40dc71e5bb701574ea215a81a1"
          },
          "size": 25536,
          "name": "foo.dll"
        }
      }
    }
  ]
}
```

2.4 Versioning

As additional information is discovered about an SDO, the Producer of that object may version the original object using the versioning approach outlined in Part 1 of the STIX 2.0 Specification. Other recipients of the SDO will also be updated through their various personas as the original SDO is versioned. This feature of the STIX 2.0 Specification allows for SDOs to be updated as the context changes and the information becomes more complete, based on enrichments and further intelligence discovery.

2.4.1 Description

A STIX 2.0 Producer or Respondent must support versioning of objects to support interoperability within STIX.

2.4.2 Required Producer Persona Creation Support

The Producer persona must be able to create a STIX Bundle with one or more objects with the appropriate date representing when the object was created for sharing.

The Producer persona has identified an STIX object that they wish to share to Respondents.

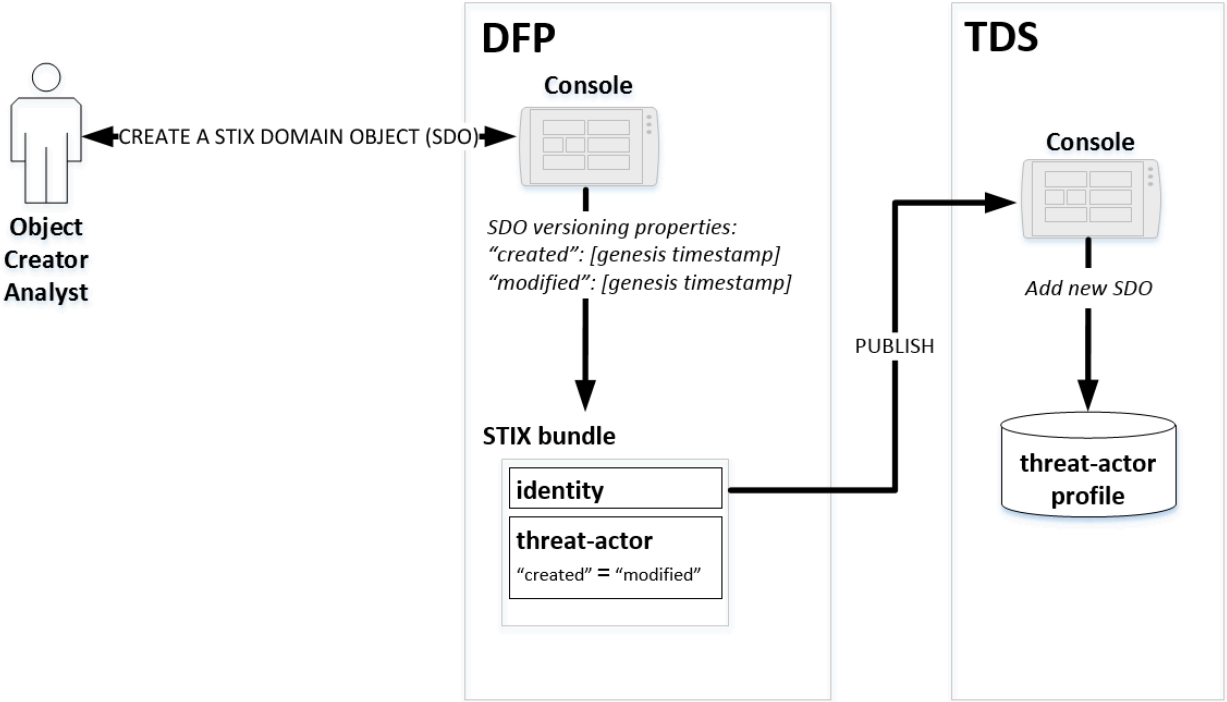

Figure 3 - An analyst creates a new STIX object

NOTE: Not all personas defined in this spec create Indicators.

Table 5 - Producer Object Bundling Details

Persona	Behavior
All **Indicator** producer personas	1. Producer allows a user to select or specify STIX content to create and send to a Respondent persona. 2. The following data must be verified in the STIX content produced by the persona: a. A bundle object must conform to mandatory attributes within the bundle object including **'type'**; **'id'**; **'spec_version'** and **'objects'** where i. **id** has a globally unique identifier ii. **spec_version** is '2.0' iii. Within the **objects** array, at least one; 1. Identity for the organization of the Producer 2. Indicator with the IP Address identified in the pattern parameter b. The identity object must conform to mandatory attributes within the identity object spec including 'type'; 'name'; 'identity_class' and 'id' where i. **type** is identity ii. **id** has a globally unique identifier iii. **identity_class** is specified by the organization of the Producer iv. **name** is the name that the Producer wishes to share associated with the Indicator c. The Indicator object must conform to mandatory attributes of Indicator including 'type'; 'id'; 'created_by_ref'; 'created'; 'modified'; 'pattern'' where i. **created_by_ref** must point to the Identity of the Producer; ii. **created** and **modified** must match the timestamp to millisecond granularity of when the user selected the IP address to be an IOC
All **Sighting** producer personas	1. Producer allows a user to select or specify the STIX content to create and send to a Respondent persona. 2. The following data must be verified in the STIX produced by the persona: a. A Bundle object must conform to mandatory attributes within the object including **'type'**; **'id'**; **'spec_version'** and **'objects'** where i. **id** has a globally unique identifier ii. **spec_version** is '2.0' iii. Within the **objects** array, at least one; 1) Identity for the organization of the Producer 2) Sighting with the observed data for the indicator identified in the pattern parameter b) The Identity object must conform to mandatory attributes within the object spec including 'type'; 'name'; 'identity_class' and 'id' where i) **type** is Identity ii) **id** has a globally unique identifier iii) **identity_class** is specified by the organization of the Producer iv) **name** is the name that the Producer wishes to share associated with the Sighting

	c) The Sighting object must conform to mandatory attributes of indicator including 'type'; 'id'; 'created_by_ref'; 'created'; 'modified'; 'pattern" where i) **created_by_ref** must point to the identity of the Producer; ii) **created** and **modified** must match the timestamp to millisecond granularity of when the Respondent created the Sighting

2.4.3 Producer Test Case Data

The following subsections provide the test case data for the test.

2.4.3.1 Creation of an Indicator with Identity and Date

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "labels": [
        "Malicious IP"
      ],
      "name": "Bad IP1",
      "description": "This indicator should be monitored for malicious activity",
      "pattern": "[ ipv4-addr:value: '198.51.100.1' ]",
      "valid_from": "2016-01-01T00:00:00Z"
    }
  ]
}
```

2.4.3.2 Creation of a Sighting with Identity and Date

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp Sighting, Inc.",
      "identity_class": "organization",
      "id": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "sighting",
      "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c75",
      "created_by_ref": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:08:31.000Z",
      "modified": "2016-04-06T20:08:31.000Z",
      "first_seen": "2015-12-21T19:00:00Z",
      "last_seen": "2015-12-21T19:00:00Z",
      "count": 50,
      "sighting_of_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "observed_data_refs": [
        "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf"
      ],
      "where_sighted_refs": [
        "identity--b67d30ff-02ac-498a-92f9-32f845f448ff"
      ]
    },
    {
      "type": "observed-data",
      "id": "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf",
      "created_by_ref": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T19:58:16.000Z",
      "modified": "2016-04-06T19:58:16.000Z",
      "start": "2015-12-21T19:00:00Z",
      "stop": "2016-04-06T19:58:16Z",
      "count": 1,
      "objects": {
        "0": {
          "type": "ipv4-addr",
          "value": "198.51.100.1"
        }
      }
    }
  ]
}
```

2.4.4 Required Respondent Creation Support

The Respondent must be able to parse and display the creation and modification date of the objects received.

Table 6 - Respondent Object Bundling Details

Persona	Behavior

All Indicator Respondent Persona	1. Respondent allows a user to receive a STIX Bundle with a(n) a. bundle with an identity and indicator with IP content b. identity of the producer c. indicator with IP address information contained in it 2. Once received the Respondent is able to display to the user the Producers of the indicator based on the identity's attribute **'name'** and the **identity_class** attribute 3. For each Indicator, the Respondent is able to verify that the **created_by_ref** maps to an existing identity received or one contained within the bundle received 4. For each Indicator, the Respondent may show the **creation** and **modified** dates for them.

2.4.5 Respondent Test Case Creation Data

This use case is primarily testing the production of an Indicator; its related version information and a Respondent's ability to parse and represent the data correctly. No other data is sent from the Respondent back to the Producer.

2.4.6 Required Producer Persona Modification Support

The Producer persona must be able to create a STIX Bundle with one or more objects with the appropriate date representing when the object was updated for sharing.

The Producer persona has identified an STIX object that they wish to update and re-share to Respondents.

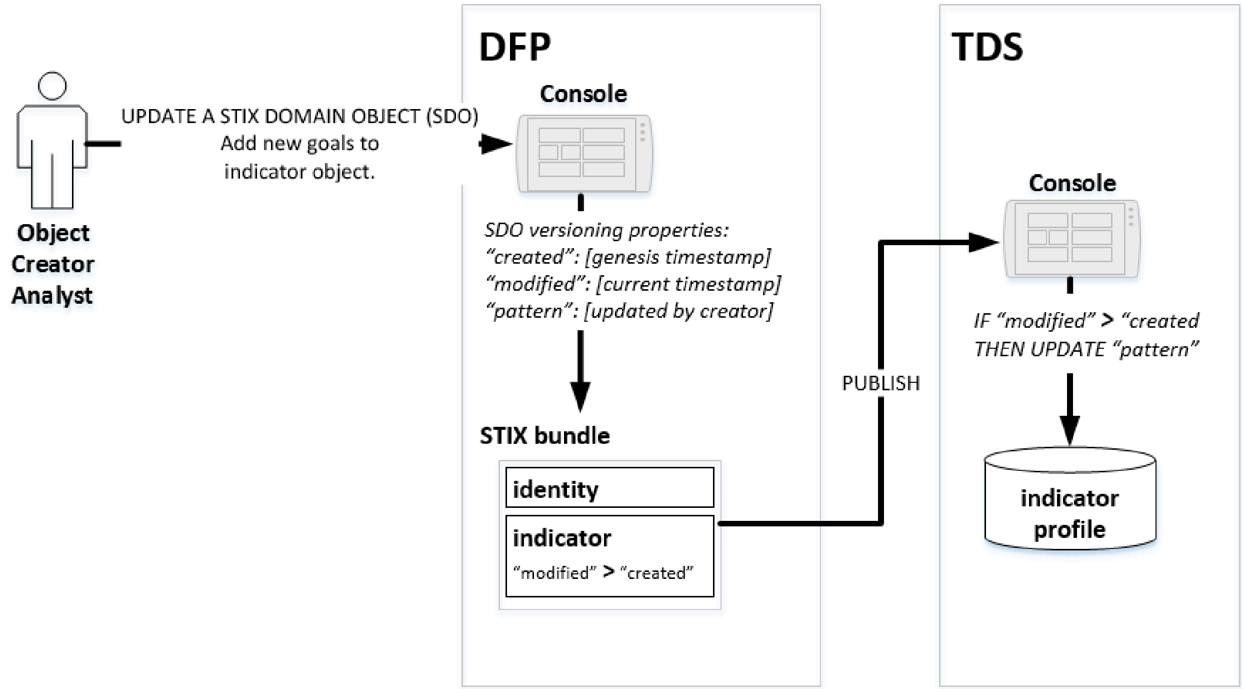
Object Creator Analyst
UPDATE A STIX DOMAIN OBJECT (SDO)
Add new goals to indicator object.
DFP
Console
SDO versioning properties:
“created”: [genesis timestamp]
“modified”: [current timestamp]
“pattern”: [updated by creator]
STIX bundle
identity
indicator
“modified” > “created”
PUBLISH
TDS
Console
IF “modified” > “created
THEN UPDATE “pattern”
indicator profile

Figure 4 - An analyst updates a STIX indicator object

Table 7 - Producer Object Bundling Details

Persona	Behavior
All Indicator Producer Personas	1. Producer allows a user to select a previously shared Indicator with IP Address associated with Actor A. 2. The following data must be verified in the STIX produced by the persona: a. A bundle object must conform to mandatory attributes within the bundle object including 'type'; 'id'; 'spec_version' and 'objects' where i. **id** has a globally unique identifier ii. **spec_version** is '2.0' iii. Within the **objects** array, at least one; 1. **identity** for the organization of the Producer 2. **indicator** with the IP Address identified in the pattern parameter b. The identity object must conform to mandatory attributes within the identity object spec including 'type'; 'name'; 'identity_class' and 'id' where i. **type** is identity ii. **id** has a globally unique identifier iii. **identity_class** is specified by the organization of the Producer iv. **name** is the name that the Producer wishes to share associated with the indicator c. The Indicator object must conform to mandatory attributes of indicator including 'type'; 'id'; 'created_by_ref'; 'created'; 'modified'; 'pattern'' where i. **created_by_ref** must point to the identity of the original Producer ii. **created** must match the original creation timestamp to millisecond granularity of when the user selected the IP address to be an IOC originally iii. **modified** must match the new modified timestamp to millisecond granularity of when the user selected the Indicator to be re-shared iv. **description** must be changed from the previously shared Indicator
All Sighting Producer Personas	1. Producer allows selection or specification of the STIX content to send to a Respondent persona. 2. The following data must be verified in the STIX produced by the persona: a. A bundle object must conform to mandatory attributes within the bundle object including **'type'**; **'id'**; **'spec_version'** and **'objects'** where i. **id** has a globally unique identifier **spec_version** is '2.0' ii. Within the **objects** array, at least one; 1. **identity** for the organization of the Producer

	2. **sighting** with the observed data for the Indicator identified in the pattern parameter b. The Identity object must conform to mandatory attributes within the Identity object spec including 'type'; 'name'; 'identity_class' and 'id' where i. **type** is identity ii. **id** has a globally unique identifier iii. **identity_class** is specified by the organization of the Producer iv. **name** is the name that the Producer wishes to share associated with the sighting c. The Sighting object must conform to mandatory attributes of sighting including 'type'; 'id'; 'created_by_ref'; 'created'; 'modified'; 'pattern" where i. **created_by_ref** must point to the identity of the Producer; ii. **created** must match the original creation timestamp to millisecond granularity of when the user selected the Observed Data object shared previously iii. **modified** must match the new modified timestamp to millisecond granularity of when the Sighting was updated with new Observed Data iv. **count** must be changed from the previously shared Sighting v. **last_observed** timestamp must be updated for the new sighting information

2.4.7 Producer Test Case Modification Data

The following subsections provide the test case data for the test.

2.4.7.1 Modification of an Indicator with Identity and Date

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:12:48.000Z",
      "labels": [
        "Malicious IP"
      ],
      "name": "Bad IP1",
      "description": "This is a changed indicator description",
      "pattern": "[ ipv4-addr:value: '198.51.100.1' ]",
      "valid_from": "2016-01-01T00:00:00Z"
    }
  ]
}
```

2.4.7.2 Modification of a Sighting with Identity and Date

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp Sighting, Inc.",
      "identity_class": "organization",
      "id": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "sighting",
      "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c75",
      "created_by_ref": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:08:31.000Z",
      "modified": "2016-04-06T20:08:31.000Z",
      "first_seen": "2015-12-21T19:00:00Z",
      "last_seen": "2015-12-21T19:00:00Z",
      "count": 50,
      "sighting_of_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "observed_data_refs": [
        "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf"
      ],
      "where_sighted_refs": [
        "identity--b67d30ff-02ac-498a-92f9-32f845f448ff"
      ]
    },
    {
      "type": "observed-data",
      "id": "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf",
      "created_by_ref": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T19:58:16.000Z",
      "modified": "2016-04-06T19:59:17.000Z",
      "first_observed": "2015-12-21T19:00:00Z",
      "last_observed": "2016-04-06T19:59:17Z",
      "number_observed": 1,
      "objects": {
        "0": {
          "type": "ipv4-addr",
          "value": "198.51.100.1"
        }
      }
    }
  ]
}
```

2.4.8 Required Respondent Modification Support

The Respondent must be able to parse and display the creation; modification dates as well as the changed field of the objects received.

Table 8 Producer Object Bundling Details

Persona	Behavior
All Indicator Respondent personas	1. Respondent allows a user to receive a STIX Bundle with an a. Identity and Indicator with pattern content b. Identity of the producer c. Indicator information contained in it 2. Once received the Respondent is able to display to the user the source of the indicator based on the identity's attribute 'name' and the **identity_class** attribute 3. For each Indicator, the Respondent is able to verify that the **created_by_ref** maps to an existing identity received or one contained within the bundle received 4. For each Indicator, the Respondent may show the **creation** and **modified** dates for them.
All Sighting Respondent personas	1. Respondent allows a user to receive a STIX bundle with a(n) a. Identity and Sighting with pattern content b. Identity of the Producer c. Sighting information contained in it 2. Once received the Respondent is able to display to the user the source of the Sighting based on the identity's attribute 'name' and the **identity_class** attribute 3. For each Sighting of Observed Data, the Respondent is able to verify that the **created_by_ref** maps to an existing Identity received or one contained within the Bundle received 4. For each Sighting, the Respondent may show the **creation** and **modified** dates for them.

2.4.9 Respondent Test Case Modification Data

This use case is primarily testing the production of an Indicator; its related version information and a Respondent's ability to parse and represent the data correctly. No other data is sent from the Respondent back to the Producer.

2.4.10 Required Producer Persona Revocation Support

The Producer persona must be able to create a STIX Bundle with one or more objects with the appropriate date representing when the object was revoked for sharing.

The producer persona has identified a STIX object that they wish to update as revoked and re-share to Respondents.

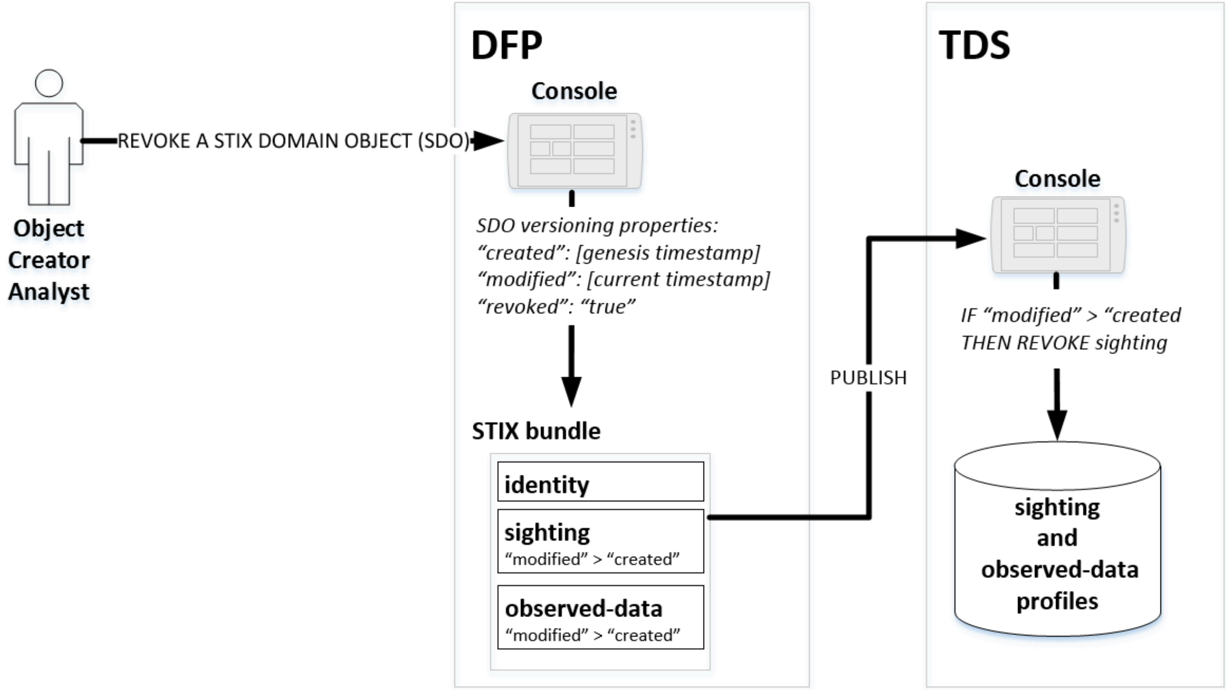

Figure 5 - An analyst revokes a STIX sighting object and its related observed data

Table 9 - Producer Object Bundling Details

Persona	Behavior
All Indicator Producer personas	1. Producer allows a user to select a previously shared Indicator that is no longer valid and wishes to delete that Indicator. 2. The following data must be verified in the STIX produced by the persona: a. A Bundle object must conform to mandatory attributes within the Bundle object including 'type'; 'id'; 'spec_version' and 'objects' where

	i. **id has** a globally unique identifier ii. **spec_version**is '2.0' iii. Within the **objects** array, at least one; 1. **Identity** for the organization of the Producer 2. **Indicator** with the IP Address identified in the pattern parameter b. The Identity object must conform to mandatory attributes within the Identity object spec including 'type'; 'name'; 'identity_class' and 'id' where i. **type is**Identity ii. **id has** a globally unique identifier iii. **identity_class** is specified by the organization of the Producer iv. **name is the** name that the Producer wishes to share associated with the Indicator c. The Indicator object must conform to mandatory attributes of Indicator including 'type'; 'id'; 'created_by_ref'; 'created'; 'modified'; 'pattern'' where i. **created_by_ref** must point to the identity of the original Producer; ii. **created** must match the original creation timestamp to millisecond granularity of when the user selected the IP address to be an IOC iii. **modified** must match the last modified timestamp to millisecond granularity of when the user selected the indicator to be revoked. iv. **revoked** must be set to true.
All Sighting Producer Personas	1. Producer allows a user to select a previously shared Sighting (and associated observed data) that is no longer valid and wishes to delete that sighting. 2. The following data must be verified in the STIX produced by the persona: a. A Bundle object must conform to mandatory attributes within the bundle object including 'type'; 'id'; 'spec_version' and 'objects' where i. **id** has a globally unique identifier ii. **spec_version**is '2.0' iii. Within the **objects** array, at least one 1. **identity** for the organization of the Producer 2. **sighting** and associated observed_data object b. The Identity object must conform to mandatory attributes within the object specification including 'type'; 'name'; 'identity_class' and 'id' where i. **type is**Identity ii. **id has** a globally unique identifier iii. **identity_class** is specified by the organization of the Producer iv. **name is the** name that the Producer wishes to share associated with the Sighting and Observed Data c. The Sighting object must conform to mandatory attributes of indicator including 'type'; 'id'; 'created_by_ref'; 'created'; 'modified'; revoked

	where i. **created_by_ref** MUS point to the Identity of the original Producer; ii. **created** must match the original creation timestamp to millisecond granularity of when the user selected the Sighting to be shared iii. **modified** must match the last modified timestamp to millisecond granularity of when the user selected the Sighting to be revoked. iv. **revoked** must be set to true. v. The previously shared optional Sighting attributes such as first_seen, last_seen, count ...etc may not be included in the object d. The observed_data object must conform to mandatory attributes of Indicator including 'type'; 'id'; 'created_by_ref'; 'created'; 'modified'; revoked where i. **created_by_ref** must point to the Identity of the original Producer; ii. **created** must match the original creation timestamp to millisecond granularity of when the user selected the observed_data to be shared iii. **modified** must match the last modified timestamp to millisecond granularity of when the user selected the observed_data to be revoked. iv. **revoked** must be set to true. v. The previously shared optional Observed Data attributes such as objects may not be included in the object

2.4.11 Producer Test Case Revocation Data

The following subsections provide the test case data for the test.

2.4.11.1 Deletion of an Indicator with Identity; Dates

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:12:50.000Z",
      "revoked": "true",
      "labels": [
        "Malicious IP"
      ],
      "name": "Bad IP1",
      "description": "This indicator should be monitored for malicious activity",
      "pattern": "[ ipv4-addr:value: '198.51.100.1' ]",
      "valid_from": "2016-01-01T00:00:00Z"
    }
  ]
}
```

2.4.11.2 Deletion of a Sighting and Associated Observed Data

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp Sighting, Inc.",
      "identity_class": "organization",
      "id": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "sighting",
      "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c75",
      "created_by_ref": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:08:31.000Z",
      "modified": "2016-04-06T20:10:31.000Z",
      "revoked": "true",
      "sighting_of_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    },
    {
      "type": "observed-data",
      "id": "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf",
      "created_by_ref": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T19:58:16.000Z",
      "modified": "2016-04-06T20:10:31.000Z",
      "revoked": "true",
      "start": "2015-12-21T19:00:00Z",
      "stop": "2016-04-06T19:59:17Z",
      "count": 2,
    }
    ]
}
```

2.4.12 Required Respondent Revocation Support

The Respondent must be able to parse and display the creation; modification dates and revoked field of the objects received.

Table 10 - Respondent Object Bundling Details

Persona	Behavior
All Indicator Respondent Personas	1. Respondent allows a user to receive a STIX **Bundle** with an a. **Identity** and Indicator with indicator content b. **Identity** of the Producer c. **Indicator** with pattern information contained in it 2. Once received the Respondent is able to display to the user the source of the Indicator based on the identity's attribute 'name' and the **identity_class** attribute 3. For each Indicator, the Respondent is able to verify that the **created_by_ref** maps to an existing **Identity** received or one contained within the **Bundle** received 4. For each **Indicator,** the Respondent may show the creation and modified dates for them.
All Sighting Respondent Personas	1. **Respondent** allows a user to receive a STIX bundle with a(n) a. **Identity** and sighting & observed_data content b. **Identity** of the Producer c. **Sighting** with associated **observed_data** object 2. Once received the **Respondent** is able to display to the user the source of the sighting based on the **Identity's** attribute **'name'** and the **identity_class** attribute 3. For each **sighting** & **observed_data** the Respondent is able to verify that the **created_by_ref** maps to an existing **Identity** received or one contained within the **Bundle** received 4. For each **Sighting,** the Respondent may show the creation and modified dates for them and that the object has been revoked.

2.4.13 Respondent Test Case Revocation Data

This use case is primarily testing the production of an Indicator or Sighting, its related version information, and a Respondent's ability to parse and represent the data correctly. No other data is sent from the Respondent back to the producer.

2.5 Data Markings

2.5.1 Description

A STIX 2.0 Producer or Respondent must support markings applied to objects and the related operations around them. The Data Markings use cases focus on how markings should be represented. How consumers mitigate markings and their related Indicator(s) is not prescribed in this specification. Data Markings can be produced at an object level and at an attribute level. Data Markings at the attribute level are known as granular markings.

This section describes basic tests for assigning Data Markings to shared data using the traffic light protocol (TLP). "TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience." It is defined by a Forum of Incident Response and Security Teams (FIRST) Special Interest Group (SIG).

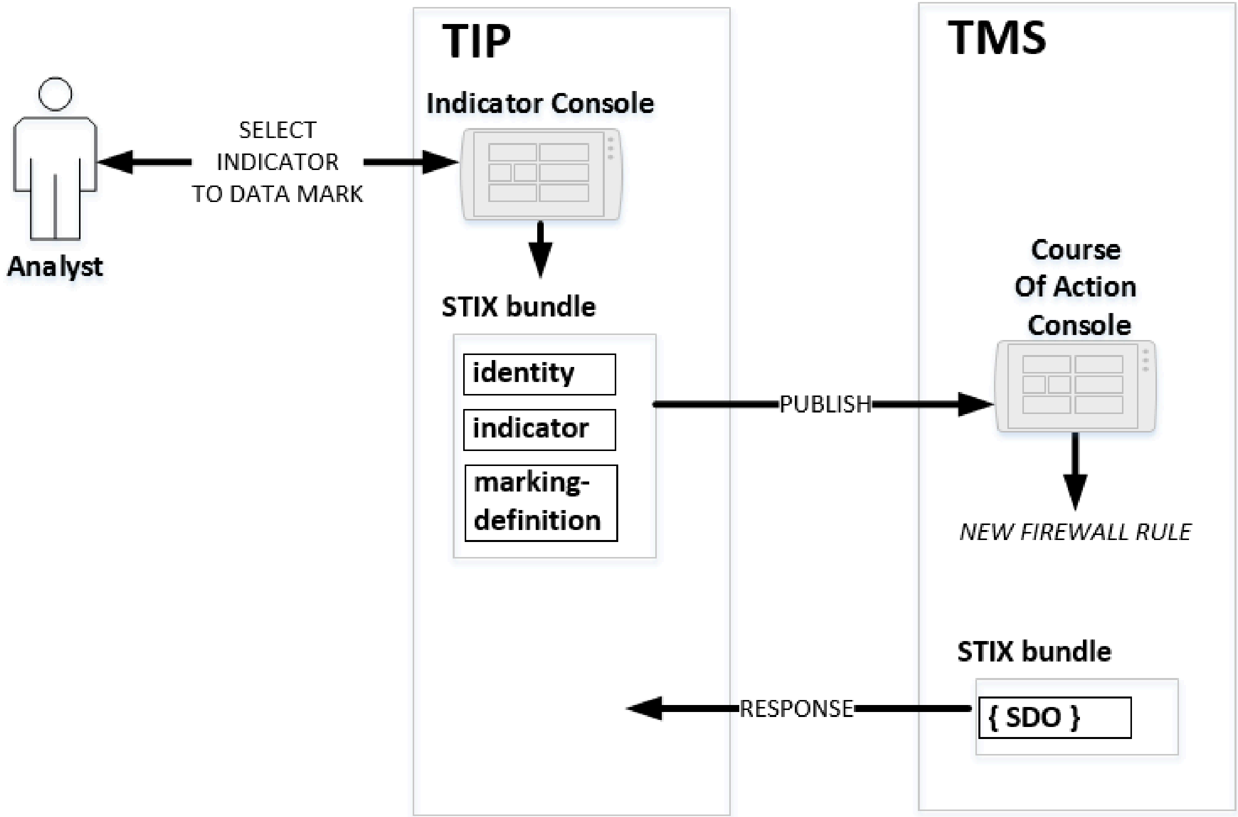

Figure 6 - An analyst marks an indicator with a TLP designation

2.5.2 Required Producer Persona Support

For these test cases, STIX TLP data markings must be accompanied by at least one Indicator. The producer persona must be able to create a STIX bundle with one or more Indicators as identified by the

Indicator Sharing Producer Test Case Data. All personas defined in Indicator Sharing Required Producer Persona Support are also defined for Data Markings producer personas.

Producers should allow users to create marking-definitions and apply object level markings to an SDO or SRO at all TLP levels.

Table 11 - Producer Object Bundling Details

Persona	Behavior
`DFP; TIP`	1. Producer allows a user or an administrator to apply object level markings to a variety of Indicators that are being shared. 2. Producer may provide TLP object level markings at any level. a. Producer verifies that objects to be marked do exist in the bundle. b. Producer must NOT mark Indicator objects with more than one TLP level markings. 3. The Producer creates the **marking-definition** object for the request: a. For different objects, the user can apply different TLP levels including: **tlp** “green”; **tlp** “amber”; **tlp** “red”; **tlp** “white”. b. The **marking-definition** must conform to its mandatory attributes including: i. **type** is **“marking-definition”** ii. **id** has a globally unique identifier iii. **created_by_ref** points to the organization identity creating both the **indicator** object and the associated marking iv. **created** and **modified** time at which the **marking-definition** was created v. **definition_type** open-vocab with a value of **“tlp”** vi. **definition** and the TLP level 4. The SDO **object_marking_refs** list of **marking-definition** is populated with markings created by Producer and the **id** that matches the intended TLP marking. 5. All **marking-definitions** are embedded in the Bundle.

2.5.3 Producer Test Case Data

The following subsections provide the test case data for the test.

2.5.3.1 TLP Green + Indicator with IPv4 Address

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "labels": [
        "Malicious IP"
      ],
      "name": "Bad IP1",
      "description": "This indicator should be monitored for malicious activity",
      "pattern": "[ ipv4-addr:value: '198.51.100.1' ]",
      "valid_from": "2016-01-01T00:00:00Z",
      "object_marking_refs": [
        "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da"
      ]
    },
    {
      "type": "marking-definition",
      "id": "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2017-01-20T00:00:00.000Z",
      "modified": "2017-01-20T00:00:00.000Z",
      "definition_type": "tlp",
      "definition": {
        "tlp": "green"
      }
    }
  ]
}
```

2.5.3.2 TLP Amber + Two Indicators with IPv4 Address CIDR

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "labels": [
        "Malicious CIDRs"
      ],
      "name": "Bad IP Subnets",
      "description": "This indicator should be monitored for malicious activity from either
subnet",
      "pattern": "[ipv4-addr:value: '198.51.100.0/24' OR ipv4-addr:value: '196.45.200.0/24']",
      "valid_from": "2016-01-01T00:00:00Z",
      "object_marking_refs": [
        "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"
      ]
    },
    {
      "type": "marking-definition",
      "id": "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2017-01-20T00:00:00.000Z",
      "modified": "2017-01-20T00:00:00.000Z",
      "definition_type": "tlp",
      "definition": {
        "tlp": "amber"
    }
  ]
}
```

2.5.3.3 TLP White and TLP Red + Indicator with IPv6 Address

```
{
 "type": "bundle",
 "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
 "spec_version": "2.0",
 "objects": [
  {
   "type": "identity",
   "name": "ACME Corp, Inc.",
   "identity_class": "organization",
   "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
   "object_marking_refs": [
    "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"
   ]
  },
  {
   "type": "indicator",
   "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
   "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
   "created": "2016-04-06T20:03:48.000Z",
   "modified": "2016-04-06T20:03:48.000Z",
   "labels": [
    "Malicious IPv6"
   ],
   "name": "Bad IPv6-1",
   "description": "This indicator should be monitored for malicious activity",
   "pattern": "[ ipv6-addr:value: '2001:0db8:85a3:0000:0000:8a2e:0370:7334' ]",
   "valid_from": "2016-01-01T00:00:00Z",
   "object_marking_refs": [
    "marking-definition--5e57c739-391a-4eb3-b6be-7d15ca92d5ed"
   ]
  },
  {
   "type": "marking-definition",
   "id": "marking-definition--5e57c739-391a-4eb3-b6be-7d15ca92d5ed",
   "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
   "created": "2017-01-20T00:00:00.000Z",
   "modified": "2017-01-20T00:00:00.000Z",
   "definition_type": "tlp",
   "definition": {
    "tlp": "red"
   }
  }
 ]
}
```

2.5.3.4 TLP Red + Sighting and Indicator

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp Sighting, Inc.",
      "identity_class": "organization",
      "id": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "labels": [
        "Malicious CIDR"
      ],
      "name": "Bad IP CIDR",
      "description": "This indicator should be monitored for malicious activity",
      "pattern": "[ ipv4-addr:value: '198.51.100.12/24' ]",
      "valid_from": "2016-01-01T00:00:00Z",
      "object_marking_refs": [
        "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da"
      ]
    },
    {
      "type": "sighting",
      "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c75",
      "created_by_ref": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:08:31.000Z",
      "modified": "2016-04-06T20:08:31.000Z",
      "first_seen": "2015-12-21T19:00:00Z",
      "last_seen": "2015-12-21T19:00:00Z",
      "count": 50,
      "sighting_of_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "observed_data_refs": [
        "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf"
      ],
      "where_sighted_refs": [
        "identity--b67d30ff-02ac-498a-92f9-32f845f448ff"
      ],
      "object_marking_refs": [
        "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da"
      ]
    },
    {
      "type": "observed-data",
      "id": "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf",
      "created_by_ref": "identity--29898928432-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T19:58:16.000Z",
      "modified": "2016-04-06T19:58:16.000Z",
      "start": "2015-12-21T19:00:00Z",
      "stop": "2016-04-06T19:58:16Z",
      "count": 1,
      "object_marking_refs": [
        "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da"
      ],
      "objects": {
        "0": {
          "type": "ipv4-addr",
          "value": "198.51.100.1"
        }
      }
    },
    {
      "type": "marking-definition",
      "id": "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2017-01-20T00:00:00.000Z",
      "modified": "2017-01-20T00:00:00.000Z",
      "definition_type": "tlp",
      "definition": {
        "tlp": "red"
      }
    }
  ]
}
```

2.5.4 Required Respondent Support

The Respondent must be able to parse and display any Indicator that has been shared with IP Address information and data markings, if present. All required Respondent support defined in 2.2.4 Required Respondent Support also applies to Data Markings.

Table 12 - Respondent Object Bundling Details

Persona	Behavior
`TIP; SIEM`	1. Respondent receives the STIX bundle with a. A Bundle the various required field pattern content as follows i. An **Identity** of the producer ii. An **Indicator** with various required fields iii. An **Indicator** with data markings applied iv. The **Indicator's** **object_marking_refs**, **must** be associated with a correct **marking definition** v. If the **Indicator** identifies a **marking-definition** object that does not exist, then the Respondent **should** reject the **Indicator** 2. Once received the Respondent can display to the user the source of the **Indicator** based on the **Identity's** attribute **'name'** and the **identity_class** attribute 3. For each **Indicator** and **marking-definition** object the Respondent is able to verify that the **created_by_ref** maps to an existing **Identity** received or one contained within the bundle received 4. For each set of objects, the Respondent must display or filter the objects based on the associated Data Markings applied to that object.

	This ensures that the user accessing the set of objects has appropriate marking authorization for TLP green, TLP amber, TLP red and TLP white depending on the test case performed.

2.6 Custom Objects and Properties

2.6.1 Description

If an organization produces or consumes custom STIX objects or properties the following tests verify that the capability is done correctly.

2.6.2 Required Producer Persona Support

The Producer persona must be able to create a STIX Bundle with one or more objects with the appropriate date representing when the object was created for sharing.

NOTE: Not all personas defined in this specification create **Indicators**.

Table 13 - Producer Object Bundling Details

Persona	Behavior
All Producer personas that generate custom objects	1. Producer allows a user to select or specify the STIX custom object content to send to a Respondent persona. 2. The following data must be verified in the STIX produced by the persona: a. A **Bundle** object must conform to mandatory attributes within the bundle object including **'type'**; **'id'**; **'spec_version'** and **'objects'** where i. **type is Bundle** ii. **id has** a globally unique identifier iii. **spec_version**is '2.0' iv. Within the **objects** array 1. at least one **Identity** for the organization of the Producer 2. at least one **custom object** where the custom object **type** name is prefixed with “**x-**” b. The **Identity** object must conform to mandatory attributes within the identity object spec including the following: i. **type is identity** ii. **id has** a globally unique identifier iii. **identity_class** is specified by the organization of the Producer iv. **name is the** name that the Producer wishes to share associated with the custom object c. The custom object must conform to mandatory attributes including 'type'; 'id'; 'created_by_ref'; 'created'; 'modified'; and one or more custom attributes where i. **created_by_ref** must point to the identity of the Producer; ii. **created** and **modified** must match the timestamp to millisecond granularity of when the user selected the custom object

All Producer personas that generate custom properties on SDOs	1. Producer allows a user to select or specify the STIX SDO object content to send to a Respondent persona including the custom property associated with the SDO. 2. The following data must be verified in the STIX produced by the persona: a. A Bundle object must conform to mandatory attributes within the bundle object including: i. **type is** Bundle ii. **id has** a globally unique identifier iii. **spec_versionis** '2.0' iv. Within the **objects** array 1. at least one **Identity** for the organization of the **Producer** 2. at least one **STIX SDO** with at least 1 custom property prefixed with “**x_**” b. The Identity object must conform to mandatory attributes within the identity object spec including: i. **type is** identity ii. **id has** a globally unique identifier iii. **identity_class** is specified by the organization of the Producer iv. **name is the** name that the Producer wishes to share associated with the SDO c. The custom object property must conform to mandatory attributes including **'type'**; **'id'**; **'created_by_ref'**; **'created'**; **'modified'**; and one or more **custom properties** where i. **created_by_ref** must point to the identity of the Producer; ii. **created** and **modified** must match the timestamp to millisecond granularity of when the user selected the custom object iii. **x-**{custom property name}

2.6.3 Producer Test Case Data

The following subsections provide the test case data for the test.

2.6.3.1 Custom Object Creation

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
       "type": "x-example-com-customobject",
       "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
       "id": "x-example-com-customobject--4527e5de-8572-446a-a57a-706f15467461",
       "created": "2017-08-01T00:00:00.000Z",
       "modified": "2017-08-01T00:00:00.000Z",
       "some_custom_stuff": 14,
       "other_custom_stuff": "hello"
    }
]
```

2.6.3.2 Custom Property Creation

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "name": "ACME Corp, Inc.",
      "identity_class": "organization",
      "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    },
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-06T20:03:48.000Z",
      "modified": "2016-04-06T20:03:48.000Z",
      "labels": [
        "Malicious IP"
      ],
      "name": "Bad IP1",
      "description": "This indicator should be monitored for malicious activity",
      "pattern": "[ ipv4-addr:value: '198.51.100.1' ]",
      "valid_from": "2016-01-01T00:00:00Z"
      "x_acme_custom_property": 10,
    }
]
```

2.6.4 Required Respondent Support

A Respondent receiving custom objects or properties must conform to the following tests.

Table 14 - Respondent Object Bundling Details

Persona	Behavior
All Respondent Personas	1. Respondent receives a STIX **Bundle** with a. A **Bundle** with an **Identity** and **custom object** or **custom properties** on standard STIX object 2. Once received the Respondent is able to display to the user the source of the Indicator based on the **Identity's** attribute **'name'** and the **identity_class** attribute 3. For each custom object, the Respondent must be able to determine that it is a custom object and not a SDO and can verify that the **created_by_ref** maps to an existing **Identity** received or one contained within the **bundle** received. 4. Respondent must be able to ingest all other SDOs in the **Bundle** 5. If the Respondent supports the custom object, then for each custom object, the Respondent may show the creation and modified dates for them.
All Respondent Personas	1. Respondent receives a STIX **Bundle** with a. an Identity and b. SDO with custom properties 2. Once received the Respondent is able to display to the user the source of the SDO based on the **identity's** attribute **'name'** and the **identity_class** attribute 3. For each SDO the Respondent must be able to determine that it is a SDO and able to ingest/parse all mandatory fields. 4. If the Respondent supports the custom property, then they may show or use the custom property included in the SDO. 5. If the Respondent does not support the custom property, then the Respondent may discard or show to the user that the SDO has been rejected. The Respondent's console should be able to continue servicing the user without crashing, and support remaining SDOs in the Bundle.

2.6.5 Respondent Test Case Data

This use case is primarily testing the production of custom objects, its related core property information, and a Respondent's ability to parse and ingest (not reject) all content that may be bundled with SDOs. No data is sent from the Respondent back to the Producer.

2.7 Course Of Action Sharing

2.7.1 Description

A Course of Action (COA) is a recommendation to respond to some form of threat. Typically, a COA would be created as a separate object that is then connected to other intelligence objects that, when detected, can be mitigated by the playbook sequencing called by the COA object.

However, the COA object in STIX 2.0 is a stub. It is included to support basic use cases (such as sharing prose courses of action) but, at this time, it does not support the ability to represent automated courses of action or contain properties to represent metadata about courses of action.

The COA SDO primarily focuses on a textual description of the mitigating action.

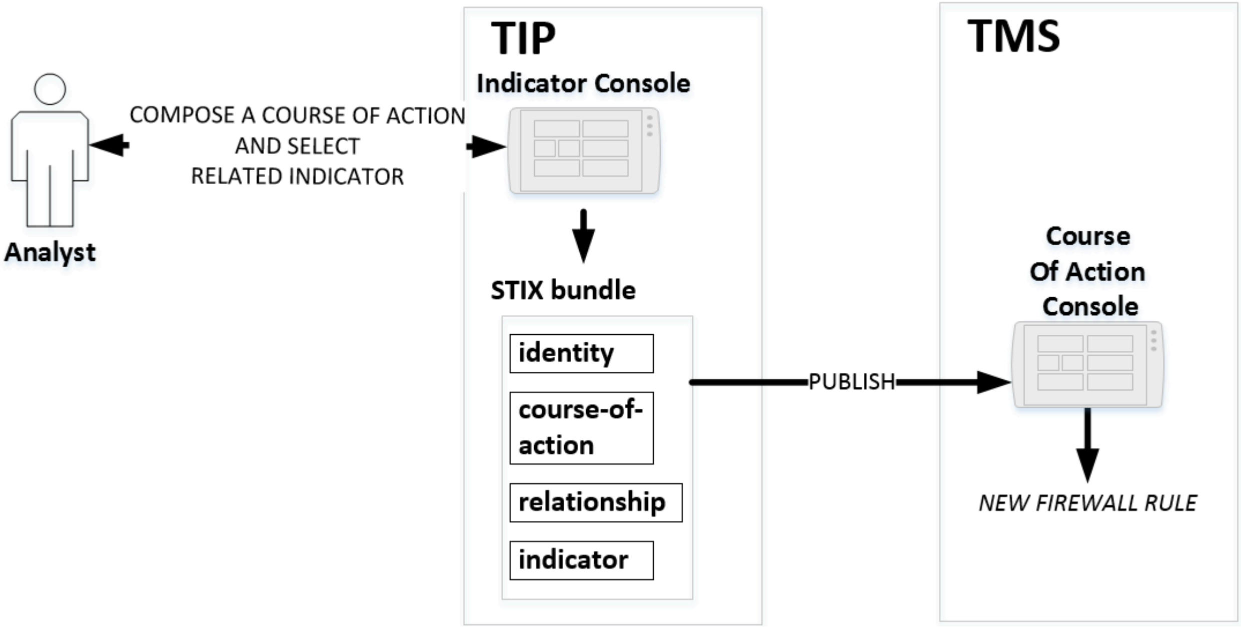

Figure 7 - Sharing Course Of Action

2.7.2. Required Producer Persona Support

The Producer must be able to populate the **'name'** and **'description'** with the textual information for the mitigating action to perform.

Table 15 - Producer Object Bundling Details

Personas	Behavior

All **Course of Action** producer personas	1. Producer allows a user to select or specify the STIX content to send to a Respondent persona. 2. The following data must be verified in the STIX produced by the persona: a) A **Bundle** object must conform to mandatory attributes within the **Bundle** object including: i) **id** has a globally unique identifier ii) **spec_version** is '2.0' iii) Within the **objects** array 1) at least one **identity** for the organization of the Producer 2) at least one **course of action** with the required fields populated b) The **Identity** object must conform to mandatory attributes within the **Identity** object spec including: i) **type** is **'identity'** ii) **id** has a globally unique identifier iii) **identity_class** is specified by the organization of the Producer iv) **name** is the name that the Producer wishes to share c) The **course-of-action** object must conform to its mandatory attributes including 'type', 'id', and the following where i) **created_by_ref** must point to the identity of the Producer; ii) **created** and **modified** must match the timestamp to millisecond granularity of when the user created the object iii) **name** that assigns a title to the **course-of-action** iv) **description** that provides more details and context about the **course-of-action**, potentially including its purpose and its key characteristics.

2.7.3 Producer Test Case Data

The following subsections provide the test case data for the test.

2.7.3.1 Create COA

```
{
 "type": "bundle",
 "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
 "spec_version": "2.0",
 "objects": [
   {
     "type": "identity",
     "name": "ACME Corp, Inc.",
     "identity_class": "organization",
     "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
   },
   {
     "type": "course-of-action",
     "id": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
     "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
     "created": "2016-04-06T20:03:48.000Z",
     "modified": "2016-04-06T20:03:48.000Z",
     "name": "Add TCP port 80 Filter Rule to the existing Block UDP 1434 Filter",
     "description": "This is how to add a filter rule to block inbound access to TCP port 80
to the existing UDP 1434 filter ..."
   }
 ]
}
```

2.7.3.2 Create COA with Relationship

```
{
 "type": "bundle",
 "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
 "spec_version": "2.0",
 "objects": [
   {
     "type": "identity",
     "name": "ACME Corp, Inc.",
     "identity_class": "organization",
     "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
   },
   {
     "type": "course-of-action",
     "id": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
     "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
     "created": "2016-04-06T20:03:48.000Z",
     "modified": "2016-04-06T20:03:48.000Z",
     "name": "Add TCP port 80 Filter Rule to the existing Block UDP 1434 Filter",
     "description": "This is how to add a filter rule to block inbound access to TCP port 80
to the existing UDP 1434 filter ..."
   },
   {
   "type": "relationship",
   "id": "relationship--44298a74-ba52-4f0c-87a3-1824e67d7fad",
   "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
   "created": "2016-04-06T20:06:37.000Z",
   "modified": "2016-04-06T20:06:37.000Z",
   "source_ref": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
   "target_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
   "relationship_type": "relates-to"
   },
   {
    "type": "indicator",
    "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-04-06T20:03:48.000Z",
    "modified": "2016-04-06T20:03:48.000Z",
    "labels": ["malicious-activity"],
    "name": "Poison Ivy Malware",
    "description": "This file is part of Poison Ivy",
    "pattern": "[ file.hashes.MD5 = '3773a88f65a5e780c8dff9cdc3a056f3' ]",
    "valid_from": "2016-01-01T00:00:00Z"
  }
 ]
}
```

2.7.4 Required Respondent Persona Support

The **Respondent** must be able to parse and display all COA Properties.

Table 16 - Respondent Object Bundling Details

Persona	Behavior
All **Course of Action** Respondent personas	1. Respondent allows a user to receive a STIX **Bundle** with a. A **Bundle** with an **Identity** and course-of-action with various content b. An **identity** of the Producer c. One or more **course-of-action** with required fields information contained in it 2. Once received, the Respondent is able to display to the user the source of the **course-of-action** based on the **Identity's** attribute 'name' and the **identity_class** attribute 3. For each **course-of-action,** the Respondent must be able to verify that the **created_by_ref** maps to an existing **Identity** received or one contained within the **Bundle** received 4. For each **course-of-action** object the Respondent is able to display the information from the course-of-action fields to the user.

3 Persona Checklist

The following checklists summarize all tests that a persona (Producer or Respondent) must conform to within that persona. 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 confirmed compliance to STIX 2.0 interoperability tests for their specific instance.

Instructions to organizations:

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

After review and verification of the demonstration submittal, the OASIS CTI TC Interoperability SC will post confirmation. Our listing will include the following:

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

No independent testing will be performed directly by the Interoperability SC; rather the verification process will confirm that the documentation is complete and accurate as claimed by the submitting party.

3.1 Data Feed Provider (DFP)

For the purpose of this document a DFP is 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 use cases.

Table 17 - Data Feed Provider (DFP) Test Verification List

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

	CIDR		
Indicator Sharing	Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	Indicator with IPv6 Address	Optional	<if supported, fill in>
Indicator Sharing	Indicator with IPv6 Address CIDR	Optional	<if supported, fill in>
Indicator Sharing	Indicator FQDN	Mandatory	<fill in>
Indicator Sharing	Indicator URL	Mandatory	<fill in>
Indicator Sharing	Indicator URL or FQDN	Mandatory	<fill in>
Indicator Sharing	Indicator File hash with SHA256 or MD5 values	Mandatory	<fill in>
Sighting Sharing	Producer Test Case Data	Mandatory	<fill in>
Versioning	Creation of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	Modification of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	Deletion of an Indicator with Identity; Dates	Mandatory	<fill in>
Versioning	Deletion of a Sighting and Associated Observed Data	Mandatory	<fill in>
Data Markings	TLP Green + Indicator with IPv4 Address	Mandatory	<fill in>
Data Markings	TLP Amber + Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Data Markings	TLP White and TLP Red + Indicator with IPv6 Address	Optional	<fill in>
Data Markings	TLP Red + Relationship between Indicator with IPv4 Address and Malware	Optional	<fill in>

Custom Object Creation	Custom Object Creation	Optional	<if supported, fill in>
Custom Property Creation	Custom Property Creation	Optional	<if supported, fill in>
Create COA	Create COA	Optional	<if supported, fill in>
Create COA Relationship	Create COA with Relationship	Optional	<if supported, fill in>

3.2 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 instance being qualified as a TIP must confirm test results for the following use cases.

Table 18 - Threat Intelligence Platform (TIP) Test Verification List

Use Case	Test	Verification	Results
Indicator Sharing	Indicator IPv4 Address	Mandatory	<fill in>
Indicator Sharing	Indicator IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	Indicator with IPv6 Address	Optional	<if supported, fill in>
Indicator Sharing	Indicator with IPv6 Address CIDR	Optional	<if supported, fill in>
Indicator Sharing	Indicator FQDN	Mandatory	<fill in>
Indicator Sharing	Indicator URL	Mandatory	<fill in>
Indicator Sharing	Indicator URL or FQDN	Mandatory	<fill in>
Indicator Sharing	Indicator File hash with SHA256 or MD5 values	Mandatory	<fill in>
Sighting Sharing	Producer Test Case Data	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with	Mandatory	<fill in>

	IPv4 Address		
Sighting Sharing	Sighting + Indicator with IPv4 Address Matching CIDR	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with IPv6 Address Matching CIDR	Optional	<if supported, fill in>
Sighting Sharing	Sighting + Indicator with NO observed data	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with URL	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with File Hash	Mandatory	<fill in>
Versioning	Creation of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	Modification of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	Deletion of an Indicator with Identity; Dates	Mandatory	<fill in>
Versioning	Deletion of a Sighting and Associated Observed Data	Mandatory	<fill in>
Data Markings	TLP Green + Indicator with IPv4 Address	Mandatory	<fill in>
Data Markings	TLP Amber + Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Data Markings	TLP White and TLP Red + Indicator with IPv6 Address	Optional	<fill in>
Data Markings	TLP Red + Relationship between Indicator with IPv4 Address and Malware	Optional	<fill in>
Custom Object Creation	Custom Object Creation	Optional	<if supported, fill in>
Custom Property	Custom Property	Optional	<if supported, fill in>

Creation	Creation		
Custom Ingestion	Required Respondent Support	Mandatory	<fill in>
Create COA	Create COA	Optional	<if supported, fill in>
Create COA Relationship	Create COA with Relationship	Optional	<if supported, fill in>

3.3 Security Incident and Event Management (SIEM)

For the purpose of this document a SIEM is a software instance that acts as a Producer and/or Respondent of STIX 2.0 content. The primary Respondent role of a SIEM is report Indicators and other high-level information. The Producer SIEM primarily reports Indicators.

Any instance being qualified as a SIEM must confirm test results for the following use cases.

Table 19 - Security Incident and Event Management (SIEM) Test Verification List

Use Case	Test	Verification	Results
Indicator Sharing	Indicator IPv4 Address	Mandatory	<fill in>
Indicator Sharing	Indicator IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	Indicator with IPv6 Address	Optional	<if supported, fill in>
Indicator Sharing	Indicator with IPv6 Address CIDR	Optional	<if supported, fill in>
Indicator Sharing	Indicator FQDN	Mandatory	<fill in>
Indicator Sharing	Indicator URL	Mandatory	<fill in>
Indicator Sharing	Indicator URL or FQDN	Mandatory	<fill in>
Indicator Sharing	Indicator File hash with SHA256 or MD5 values	Mandatory	<fill in>
Sighting Sharing	Producer Test Case Data	Optional	<fill in>
Sighting Sharing	Sighting + Indicator with	Mandatory	<fill in>

	IPv4 Address		
Sighting Sharing	Sighting + Indicator with IPv4 Address Matching CIDR	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with IPv6 Address Matching CIDR	Optional	<if supported, fill in>
Sighting Sharing	Sighting + Indicator with NO observed data	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with URL	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with File Hash	Mandatory	<fill in>
Versioning	Creation of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	Modification of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	Deletion of an Indicator with Identity; Dates	Mandatory	<fill in>
Versioning	Deletion of a Sighting and Associated Observed Data	Mandatory	<fill in>
Data Markings	TLP Green + Indicator with IPv4 Address	Mandatory	<fill in>
Data Markings	TLP Amber + Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Data Markings	TLP White and TLP Red + Indicator with IPv6 Address	Optional	<fill in>
Data Markings	TLP Red + Relationship between Indicator with IPv4 Address and Malware	Optional	<fill in>
Custom Object Creation	Custom Object Creation	Optional	<if supported, fill in>
Custom Property	Custom Property	Optional	<if supported, fill in>

Creation	Creation		
Custom Ingestion	Required Respondent Support	Mandatory	<fill in>
Create COA	Create COA	Optional	<if supported, fill in>
Create COA Relationship	Create COA with Relationship	Optional	<if supported, fill in>

3.4 Threat Mitigation System (TMS)

For the purpose of this document a TMS is a software instance that mitigates threats in a network. It may act as both a Producer and Respondent some use cases. The Respondent TMS primarily reports Indicators. The Producer TMS primarily reports Sightings.

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

Table 20 - Threat Mitigation System (TMS) Test Verification List

Use Case	Test	Verification	Results
Indicator Sharing	Indicator IPv4 Address	Mandatory	<fill in>
Indicator Sharing	Indicator IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	Indicator with IPv6 Address	Optional	<if supported, fill in>
Indicator Sharing	Indicator with IPv6 Address CIDR	Optional	<if supported, fill in>
Indicator Sharing	Indicator FQDN	Mandatory	<fill in>
Indicator Sharing	Indicator URL	Mandatory	<fill in>
Indicator Sharing	Indicator URL or FQDN	Mandatory	<fill in>
Indicator Sharing	Indicator File hash with SHA256 or MD5 values	Mandatory	<fill in>
Sighting Sharing	Producer Test Case Data	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with	Mandatory	<fill in>

	IPv4 Address		
Sighting Sharing	Sighting + Indicator with IPv4 Address Matching CIDR	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with IPv6 Address Matching CIDR	Optional	<if supported, fill in>
Sighting Sharing	Sighting + Indicator with NO observed data	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with URL	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with File Hash	Mandatory	<fill in>
Versioning	Creation of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	Modification of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	Deletion of an Indicator with Identity; Dates	Mandatory	<fill in>
Versioning	Deletion of a Sighting and Associated Observed Data	Mandatory	<fill in>
Data Markings	TLP Green + Indicator with IPv4 Address	Mandatory	<fill in>
Data Markings	TLP Amber + Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Data Markings	TLP White and TLP Red + Indicator with IPv6 Address	Optional	<fill in>
Data Markings	TLP Red + Relationship between Indicator with IPv4 Address and Malware	Optional	<fill in>
Custom Object Creation	Custom Object Creation	Optional	<if supported, fill in>
Custom Property	Custom Property	Optional	<if supported, fill in>

Creation	Creation		
Custom Ingestion	Required Respondent Support	Mandatory	<fill in>
Create COA	Create COA	Optional	<if supported, fill in>
Create COA Relationship	Create COA with Relationship	Optional	<if supported, fill in>

3.5 Threat Detection System (TDS)

For the purpose of this document a TDS detects threats in a network without necessarily mitigating the threat. 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 instance being qualified as a TDS must confirm test results for the following use cases.

Table 21 - Threat Detection System (TDS) Test Verification List

Use Case	Test	Verification	Results
Indicator Sharing	Indicator IPv4 Address	Mandatory	<fill in>
Indicator Sharing	Indicator IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	Indicator with IPv6 Address	Optional	<if supported, fill in>
Indicator Sharing	Indicator with IPv6 Address CIDR	Optional	<if supported, fill in>
Indicator Sharing	Indicator FQDN	Mandatory	<fill in>
Indicator Sharing	Indicator URL	Mandatory	<fill in>
Indicator Sharing	Indicator URL or FQDN	Mandatory	<fill in>
Indicator Sharing	Indicator File hash with SHA256 or MD5 values	Mandatory	<fill in>
Sighting Sharing	Producer Test Case Data	Mandatory	<fill in>

Sighting Sharing	Sighting + Indicator with IPv4 Address	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with IPv4 Address Matching CIDR	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with IPv6 Address Matching CIDR	Optional	<if supported, fill in>
Sighting Sharing	Sighting + Indicator with NO observed data	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with URL	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with File Hash	Mandatory	<fill in>
Versioning	Creation of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	Modification of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	Deletion of an Indicator with Identity; Dates	Mandatory	<fill in>
Versioning	Deletion of a Sighting and Associated Observed Data	Mandatory	<fill in>
Data Markings	TLP Green + Indicator with IPv4 Address	Mandatory	<fill in>
Data Markings	TLP Amber + Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Data Markings	TLP White and TLP Red + Indicator with IPv6 Address	Optional	<fill in>
Data Markings	TLP Red + Relationship between Indicator with IPv4 Address and Malware	Optional	<fill in>
Custom Object Creation	Custom Object Creation	Optional	<if supported, fill in>

Custom Property Creation	Custom Property Creation	Optional	<if supported, fill in>
Custom Ingestion	Required Respondent Support	Mandatory	<fill in>
Create COA	Create COA	Optional	<if supported, fill in>
Create COA Relationship	Create COA with Relationship	Optional	<if supported, fill in>

4 Appendix A Acknowledgments

Interoperability Subcommittee Chairs:

Allan Thomson, LookingGlass,
Jason Keirstead, IBM

Additional Editors

Jane Ginn, Cyber Threat Intelligence Network, Inc.

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:

Ray-yu	Chang	Accenture
Robert	Coderre	Accenture
Haripriya	Gajendran	Accenture
Kyle	Maxwell	Accenture
Ralph	Thomas	Accenture
David	Crawford	Aetna
Marcos	Orallo	Airbus Group SAS
Sébastien	Rummelhardt	Airbus Group SAS
Roman	Fiedler	AIT Austrian Institute of Technology
Giuseppe	Settanni	AIT Austrian Institute of Technology
Florian	Skopik	AIT Austrian Institute of Technology
Russell	Spitler	AlienVault
Ryan	Clough	Anomali
Nicholas	Hayden	Anomali

Wei	Huang	Anomali
Angela	Nichols	Anomali
Hugh	Njemanze	Anomali
Katie	Pelusi	Anomali
Dean	Thompson	Australia and New Zealand Banking Group (ANZ Bank)
Alexander	Foley	Bank of America
Tony	Pham	Bank of America
Sounil	Yu	Bank of America
Vicky	Laurens	Bank of Montreal
Alexandre	Dulaunoy	CIRCL
Andras	Iklody	CIRCL
Raphaël	Vinot	CIRCL
Sarah	Kelley	CIS
Syam	Appala	Cisco Systems
Ted	Bedwell	Cisco Systems
Craig	Brozefsky	Cisco Systems
David	McGrew	Cisco Systems
Mark-David	McLaughlin	Cisco Systems
Henry	Peltokangas	Cisco Systems
Pavan	Reddy	Cisco Systems
Omar	Santos	Cisco Systems
Sam	Taghavi Zargar	Cisco Systems
Jyoti	Verma	Cisco Systems
Doug	DePeppe	Cyber Threat Intelligence Network, Inc. (CTIN)
Jane	Ginn	Cyber Threat Intelligence Network, Inc. (CTIN)

Ben	Othman	Cyber Threat Intelligence Network, Inc. (CTIN)
David	Powell	Cyber Threat Intelligence Network, Inc. (CTIN)
Andrew	Byrne	Dell
Jeff	Odom	Dell
Sreejith	Padmajadevi	Dell
Ravi	Sharda	Dell
Will	Urbanski	Dell
Inette	Furey	DHS Office of Cybersecurity and Communications (CS&C)
Michael	Rosa	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)
Jens	Aabol	Difi-Agency for Public Management and eGovernment
Wouter	Bolsterlee	EclecticIQ
Marko	Dragoljevic	EclecticIQ
Oliver	Gheorghe	EclecticIQ
Joep	Gommers	EclecticIQ
Sergey	Polzunov	EclecticIQ
Rutger	Prins	EclecticIQ
Andrei	Sîrghi	EclecticIQ
Aukjan	van Belkum	EclecticIQ
Raymon	van der Velde	EclecticIQ
Ben	Sooter	Electric Power Research Institute (EPRI)
Carolina	Canales-Valenzuela	Ericsson
Chris	Ricard	Financial Services Information Sharing and Analysis Center (FS-ISAC)

Phillip	Boles	FireEye, Inc.
Prasad	Gaikwad	FireEye, Inc.
Rajeev	Jha	FireEye, Inc.
Anuj	Kumar	FireEye, Inc.
Shyamal	Pandya	FireEye, Inc.
Paul	Patrick	FireEye, Inc.
Scott	Shreve	FireEye, Inc.
Jon	Warren	FireEye, Inc.
Remko	Weterings	FireEye, Inc.
Charles	White	Fornetix
Simon	Bryden	Fortinet Inc.
Gavin	Chow	Fortinet Inc.
Steve	Fossen	Fortinet Inc.
Adam	Shewchuk	Fortinet Inc.
Kenichi	Terashita	Fortinet Inc.
Yasutaka	Ebihara	Fujitsu Limited
David	Markham	Fujitsu Limited
Ryusuke	Masuoka	Fujitsu Limited
Daisuke	Murabayashi	Fujitsu Limited
Derek	Northrope	Fujitsu Limited
Toshitaka	Satomi	Fujitsu Limited
Koji	Yamada	Fujitsu Limited
Kunihiko	Yoshimura	Fujitsu Limited
David	Lemire	G2
Jonathan	Algar	GDS

Iain	Brown	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
Peter	Yapp	GDS
Bethany	Yates	GDS
Robert	van Engelen	Genivia
Eric	Burger	Georgetown University
Allison	Miller	Google Inc.
Mark	Risher	Google Inc.
Naoki	Hayashi	Hitachi, Ltd.
Yoshihide	Kawada	Hitachi, Ltd.
Jun	Nakanishi	Hitachi, Ltd.
Kazuo	Noguchi	Hitachi, Ltd.
Akihito	Sawada	Hitachi, Ltd.
Yutaka	Takami	Hitachi, Ltd.
Masato	Terada	Hitachi, Ltd.
Xiaoyu	Ge	Huawei Technologies Co., Ltd.

Ho	Hock, William	Huawei Technologies Co., Ltd.
David	Webber	Huawei Technologies Co., Ltd.
Nick	Humphrey	Huntsman Security
Peter	Allor	IBM
Eldan	Ben-Haim	IBM
Allen	Hadden	IBM
Sandra	Hernandez	IBM
Jason	Keirstead	IBM
John	Morris	IBM
Laura	Rusu	IBM
frank	schaffa	IBM
garret	taylor	IBM
Ron	Williams	IBM
Paul	Martini	iboss, Inc.
Atsuhiro	Goto	IISEC
Ashwini	Jarral	IJIS Institute
Jerome	Athias	Individual
Peter	Brown	Individual
Michele	Drgon	Individual
Joerg	Eschweiler	Individual
Stefan	Hagen	Individual
Elysa	Jones	Individual
Sanjiv	Kalkar	Individual
Terry	MacDonald	Individual
Alex	Pinto	Individual

Mike	Schmidt	Individual
Tim	Casey	Intel Corporation
Andres	More	Intel Corporation
Steve	Orrin	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
David	Laurance	JPMorgan Chase Bank, N.A.
Russell	Culpepper	Kaiser Permanente
Beth	Pumo	Kaiser Permanente
Michael	Slavick	Kaiser Permanente
Gus	Creedon	Logistics Management Institute
Wesley	Brown	LookingGlass
Jamison	Day	LookingGlass
Allan	Thomson	LookingGlass
Ian	Truslove	LookingGlass
Chris	Wood	LookingGlass
Kent	Landfield	McAfee
Greg	Back	Mitre Corporation
Jonathan	Baker	Mitre Corporation
Sean	Barnum	Mitre Corporation
Desiree	Beck	Mitre Corporation
Jen	Burns	Mitre Corporation

Michael	Chisholm	Mitre Corporation
Nikki	Ellis	Mitre Corporation
Nicole	Gong	Mitre Corporation
Jasen	Jacobsen	Mitre Corporation
Ivan	Kirillov	Mitre Corporation
Michael	Kouremetis	Mitre Corporation
Chris	Lenk	Mitre Corporation
Bob	Natale	Mitre Corporation
Richard	Piazza	Mitre Corporation
Larry	Rodrigues	Mitre Corporation
Jon	Salwen	Mitre Corporation
Charles	Schmidt	Mitre Corporation
Matt	Scola	Mitre Corporation
Richard	Struse	Mitre Corporation
Alex	Tweed	Mitre Corporation
Emmanuelle	Vargas-Gonzalez	Mitre Corporation
Bryan	Worrell	Mitre Corporation
John	Wunder	Mitre Corporation
Jackson	Wynn	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
John	Anderson	NC4
Michael	Butt	NC4
Mark	Davidson	NC4
Daniel	Dye	NC4
Michael	Pepin	NC4
Natalie	Suarez	NC4
Benjamin	Yates	NC4
Daichi	Hasumi	NEC Corporation
Takahiro	Kakumaru	NEC Corporation
Lauri	Korts-Pärn	NEC Corporation
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.
Phil	Cutforth	New Zealand Government
Stephen	Banghart	NIST
David	Darnell	North American Energy Standards Board
Stephan	Relitz	Northrop Grumman
James Bryce	Clark	OASIS
Robin	Cover	OASIS

Chet	Ensign	OASIS
Dee	Schur	OASIS
Cory	Casanave	Object Management Group
Johnny	Gau	Oracle
Sunil	Ravipati	Oracle
Aharon	Chernin	Perch
Dave	Eilken	Perch
Sourabh	Satish	Phantom
John	Tolbert	Queralt Inc.
Ted	Julian	Resilient Systems, Inc..
Joseph	Brand	Semper Fortis Solutions
Duncan	Sparrell	sFractal Consulting LLC
Thomas	Schreck	Siemens AG
Rob	Roel	Southern California Edison
Dave	Cridland	Surevine Ltd.
Tom	Blauvelt	Symantec Corp.
Bret	Jordan	Symantec Corp.
Robert	Keith	Symantec Corp.
Curtis	Kostrosky	Symantec Corp.
Juha	Haaga	Synopsys
Masood	Nasir	TELUS
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.
Alejandro	Valdivia	ThreatConnect, Inc.
Ryan	Trost	ThreatQuotient, Inc.
Nir	Yosha	ThreatQuotient, Inc.
Patrick	Gannon	Thrivaca
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
Mona	Magathan	U.S. Bank
Yevgen	Sautin	U.S. Bank
Richard	Shok	U.S. Bank
James	Bohling	US Department of Defense (DoD)
Eoghan	Casey	US Department of Defense (DoD)
Jim	Fowler	US Department of Defense (DoD)
Gary	Katz	US Department of Defense (DoD)
Jeffrey	Mates	US Department of Defense (DoD)
Juan	Gonzalez	US Department of Homeland Security
Evette	Maynard-Noel	US Department of Homeland Security
Preston	Werntz	US Department of Homeland Security
Eric	Osterweil	VeriSign

Lee	Chieffalo	ViaSat
Wilson	Figueroa	ViaSat
Jerry	Goodwin	ViaSat
Andrew	May	ViaSat
Michael	Rogers	ViaSat
Franklin	Van Vorhees	ViaSat
Patrick	Maroney	Wapack Labs LLC
Ales	Cernivec	XLAB
Anthony	Rutkowski	Yanna Technologies LLC

5 Appendix B. Revision History

Revision	Date	Editor	Changes Made
01	2017-03-17	Allan Thomson, Jason Keirstead	Draft 1 for TC review
02	2017-04-19	Allan Thomson, Jason Keirstead	Draft 2 for TC Review. - Separation of future test cases into another document focusing this document on defined use cases only - Additional use cases for COA; Custom objects; Versioning; Sightings - Additional persona checklists for TMS; TDS - Various other editorial and content updates across entire document
03	2017-07-14	Allan Thomson, Jason Keirstead	Final Draft for TC Ballot - Changed title to reflect document template vs specification - Changed normative statements to lowercase - Lots of editorial updates - Removed malware references in various tests and replaced with objects being tested in Part1 - Added clarification on identity - Added clarification on bundles - Changed mandatory producer tests in SIEM to optional for sightings