STIX™ 2.0 Interoperability Use Cases

Working Draft 01 - draft1

17 March 2017

Technical Committee:

OASIS Cyber Threat Intelligence (CTI) TC

Chair:

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

Editors:

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

Related work:

This specification 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/csd01/part1-stix-core/stix-v2.0-csd01-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/csd01/part2-stix-objects/stix-v2.0-csd01-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/csd01/part3-cyber-observable-core/stix-v2.0-csd01-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/csd01/part4-cyber-observable-objects/stix-v2.0-csd01-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/csd01/part5-stix-patterning/stix-v2.0-csd01-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:

[TODO]

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 Draft (Committee Specification Draft or a Committee

Note Draft). The OASIS document Approval Process begins officially with a TC vote to approve a WD as a Committee Draft. A TC may approve a Working Draft, revise it, and re-approve it any number of times as a Committee Draft.

URI patterns:

Initial publication URI:
[TODO]
Permanent “Latest version” URI:
[TODO]
(Managed by OASIS TC Administration; please don't modify.)

Table of Contents

1 Introduction

This document defines the set of actors, behaviors and expected outcomes for the use cases that will be used to define Structured Threat Information Expression (STIX) 2.0 Interoperability Test Specifications. The Organization for the Advancement of Structured Information Standards (OASIS) Cyber Threat Intelligence Technical Committee (CTI TC) recommends users of this guide become familiar with the STIX 2.0 Core Concepts, STIX 2.0 Objects, and other supporting specifications prior to implementing the use cases in this document.

1.1 Terminology

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in [RFC2119].

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 Normative References

TODO - insert references to STIX and other related specs

1.3 Non-Normative References

TODO

1.4 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 will be incorporated into a new version of this document.

1.4.1 Target Milestones

- 15th March - 1st draft of all **MVP** tests for STIX TC broader review
- 15th April - 2nd draft
- 15th May - Final draft
- 30th May - TC Review

1.4.2 Personas

The following system personas are used throughout this document. A minimum viable product (MVP) persona will be defined for all test-cases/behaviors before the 1st revision of this document is considered 'complete'.

- **MVP**: Data Feed Provider (`DFP`)
  - Software instance that acts as a producer of STIX 2.0 content.
- **MVP**: 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.
- **MVP**: Security Incident and Event Management system (`SIEM`)
  - Software instance that acts as a producer and/or Respondent of STIX 2.0 content. The primary Respondent role of a SIEM is with respect to indicators and high-level information from a reporting perspective. The primary producer role of a SIEM is with respect to incidents, observations, and sightings.
- Threat Mitigation System (`TMS`)
  - Software instance that acts on course of actions and acts on mitigations such as a firewall or IPS, Endpoint Detection and Response (EDR) software, etc.
- Threat Detection System (`TDS`)
  - Software instance of any network product that monitors and/or detects such as Intrusion Detection Software (IDS), Endpoint Detection and Response (EDR) software, web proxy, etc.
- Digital Forensics (`DF`)
  - Software instance of any product that allows searching and/or forensic analysis of full artifacts and/or network packet captures (ie. Network Forensics, Endpoint Forensics, etc.)
- Incident Response Platform (`IRP`)
  - Software instance of any product used for management, orchestration, and response of IR (incident response) processes in an organization. Could also be a “ticketing” system.

1.4.3 Use Cases

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

Work Item Status

- **None**
  - No work has taken place yet on these use cases; looking for volunteers
- **In Progress**
  - Work by the named person(s) on this section
- **Draft Ready**
  - The use cases are considered ready for review

The following use cases are captured in this document.

Use Case Section #	Release Target	Description	Producer Personas	Respondent Personas	Status
1	V1 MVP	Indicator Sharing	DFP; TIP	TIP; TMS; TDS, SIEM	Draft Ready (Allan)
2	V1 MVP	Sightings Sharing	DFP; TIP	TIP; TMS; TDS; SIEM	Draft Ready (Allan)
3	V1 MVP	Versioning	All	All	Draft Ready (Allan)
4		Threat Actor Sharing	DFP; TIP	TIP; TMS; TDS, SIEM	None
5		Report Sharing	DFP; TIP, IRP	TIP, IRP	None
6		Malware Sharing	DFP; TIP	TIP; TMS; TDS, SIEM	None
7		Campaign Sharing	DFP; TIP	TIP, SIEM	None
8		Intrusion Set Sharing	DFP; TIP	TIP, SIEM	None
9		Vulnerability Sharing	SIEM, IRP	TIP, SIEM, IRP	None
10		Attack Pattern Sharing	DFP; TIP	TIP, TDS, TMS	None
11		Course of Action Sharing	DFP; TIP	TIP, TDS, TMS	In Progress (Marlon)
12		Tool Sharing	DFP; TIP	TIP, TDS	None
13	V1 MVP - Focused on TLP basic/test	Data Markings	All	All	Draft Ready (Emmanuelle)

14	V1 MVP Basic parsing	Custom Objects & Properties	All	All	Draft Ready (Allan)

2 Use Case Details

The initial use cases that may be used for demonstrating interoperability will include:

- Indicator Sharing
- Sighting Sharing
- Versioning
- Data Markings Sharing
- Custom Object & Property Handling

The following sections provide details on these use cases.

2.1 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). The reader will note that a TIP is defined within this document as one of the “personas” that will be used as a basis for the demonstration of interoperability. 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.

IOCs and other STIX data objects (SDOs) 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-direction IOC sharing with other security products through well-crafted application interfaces (APIs). The Respondents of the SDOs include threat intelligence analysts, fraud and risk analysts, malware analysts, network and endpoint guardians, among others. This high-level view is useful for illustrating how a use case (in this case, the Indicator object) and a persona will work together within this Specification Annex 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.

2.1.1 Description

A STIX 2.0 Indicator is an object primarily used to identify malicious content where the content is identified by STIX Cyber Observable content. There are several common characteristics of data that will be verified. The producer persona, shown on Figure 2-1 as an “Analyst”, has identified one or more indicators associated with Actor A, that is producing malicious content on the Internet or Actor A is an entity of interest to consider monitoring activity on. Also shown is how a TIP processes a STIX bundle and publishes the bundle to a TMS, which then issues a response.

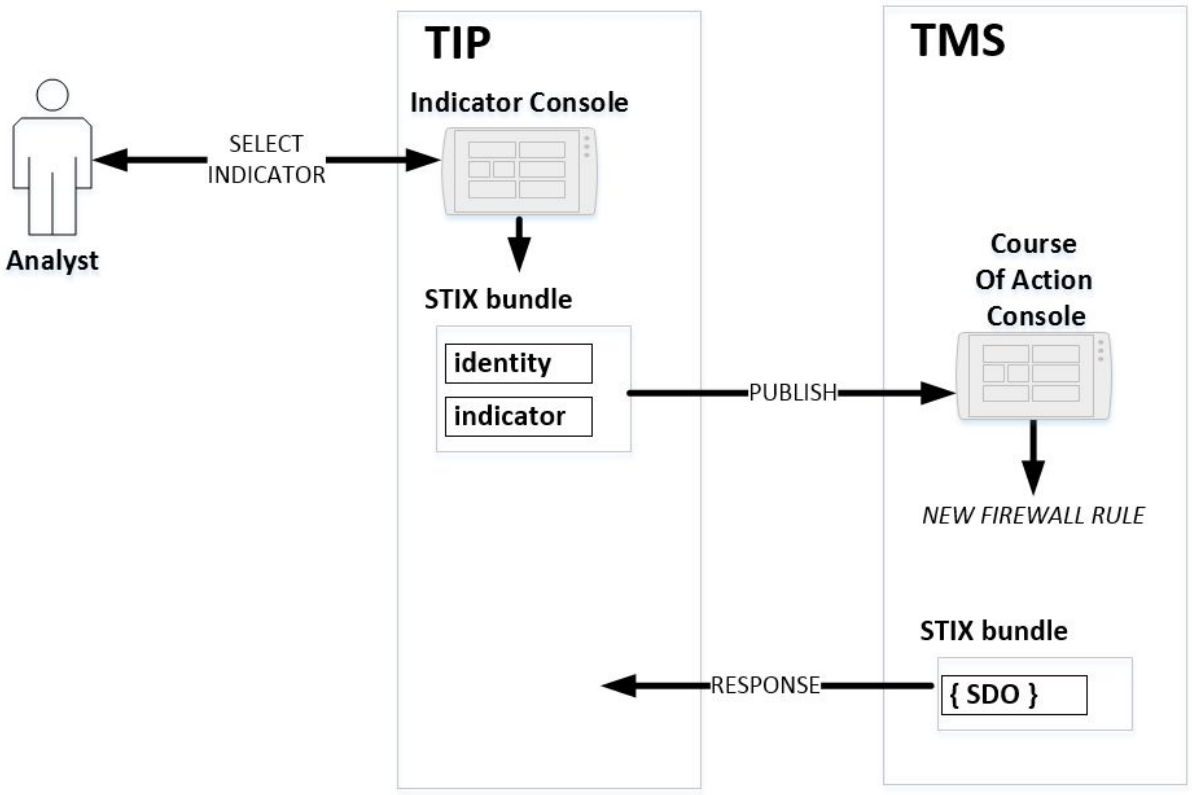


Figure 2.1 - An analyst shares an indicator

2.1.2 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.

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 as an Indicator of Compromise (IOC) to share 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 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 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 d) The pattern attribute captures the various required fields that MUST be supported by the **Producer** as defined in <ref 2.2.2.1>
	1.

2.1.2.1 Producer Test Case Data

2.1.2.1.1 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"
    }
  ]
}
```

2.1.2.1.2 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"
    }
  ]
}
```

2.1.2.1.3 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"
    }
  ]
}
```

2.1.2.1.4 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"
    }
  ]
}
```

2.1.2.1.5 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"
    }
  ]
}
```

2.1.2.1.6 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"
    }
  ]
}
```

2.1.2.1.7 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"
    }
  ]
}
```

2.1.2.1.8 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"
    }
  ]
}
```

2.1.2.1.9 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"
    }
  ]
}
```

2.1.2.1.10 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"
    }
  ]
}
```

2.1.2.2 Required Respondent Support

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

Persona	Behavior
`TIP`	1. TIP allows a user to receive a STIX bundle with a. A bundle with an identity and indicator with the various required field pattern content b. An identity of the producer c. An 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 received 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. A bundle with an identity and indicator with the indicator content b. An identity of the producer c. An indicator with the indicator 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 updates 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. A bundle with an identity and indicator with the indicator content b. An identity of the producer c. An indicator with the indicator content information contained in it 6. 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 is an allowed source of intelligence to act upon 7. 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 8. For each Indicator object the **SIEM** is able to display other relevant security information it has from other sources (firewalls, sensors) that are sending their event logs to the SIEM and show the overlap between the SIEM and the indicator information consumed including FileHash; IP; FQDN; URL contained in the pattern matched against.

2.1.2.3 Respondent Test Case Data

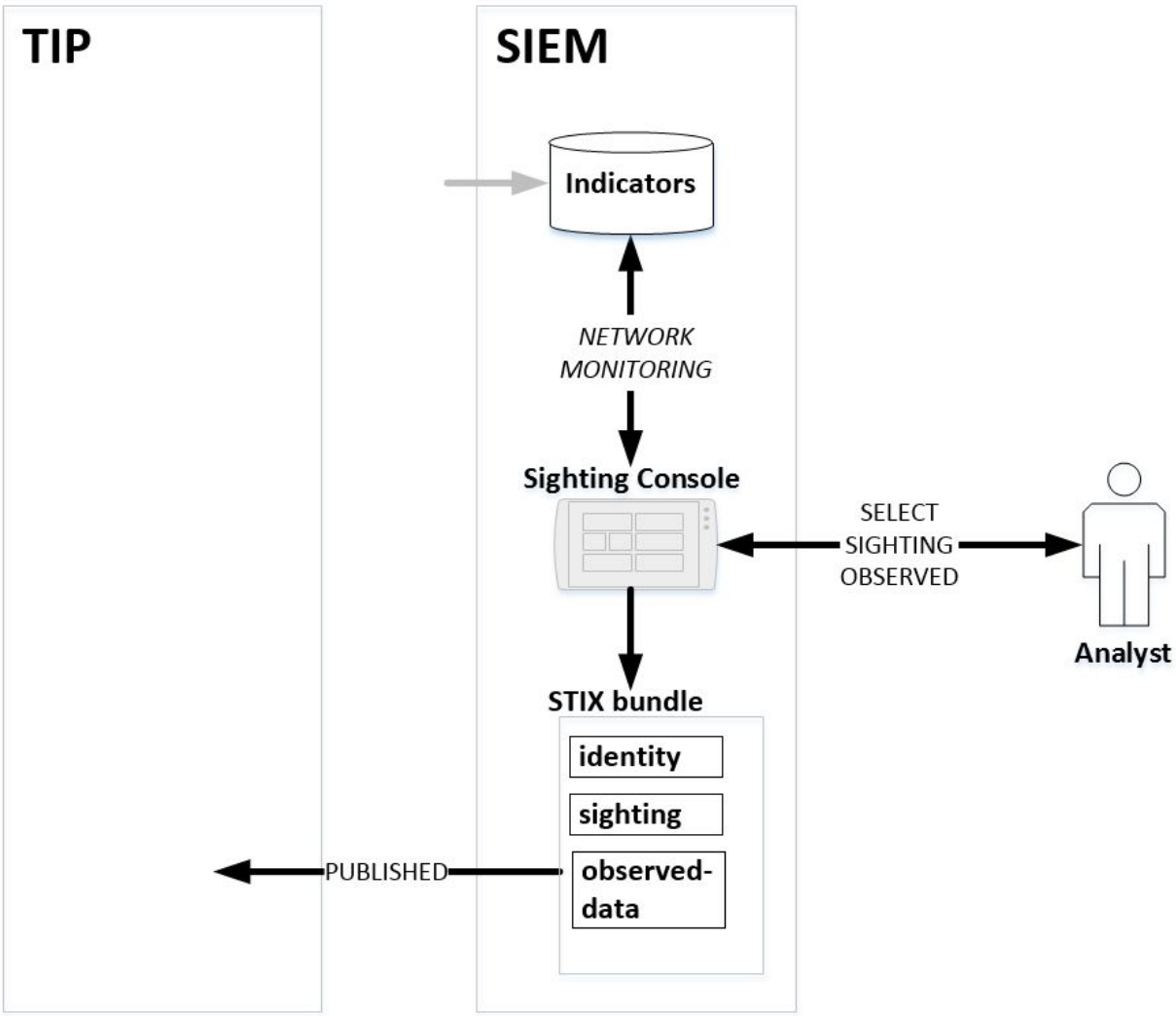
This use case is primarily testing the production of an indicator and a Respondent's ability to parse and represent and act on the indicator data correctly. No other data is sent from the Respondent back to the producer.

2.2 Sighting Sharing

Another important scenario that will provide for crowdsourcing in the context of a sharing community is the use of a Sighting SDO. 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 Observables) 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 STIX Relationship Object (SRO). Therefore, it is an important use case to demonstrate for STIX interoperability.

2.2.1 Description

A STIX 2.0 Sighting is an SRO primarily used to capture that some entity in the network has been seen by an intelligence source. The producer persona, shown on Figure 2-2 as an “Analyst”, has selected one or more sightings observed by the supporting Security Incident and Event Management (SIEM) tool. Consequently, the SIEM publishes a STIX sighting bundle and publishes it for various consumer personas.



.**Figure 2-2 - An analyst reports a sighting**

2.2.2 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 2.1.2.1 Producer Test Case Data. All personas defined in 2.1.2 Required Producer Persona Support are also defined for Sighting producer personas.

2.2.3 Producer Test Case Data

Same as Indicator Sharing 2.1.2.1 Producer Test Case Data..

2.2.4 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.

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 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 Producer A b. a reference to each indicator shared from Producer A 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 A 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.** **start** and **stop** 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 start and stop values e. **objects** must match an indicator value that matches the pattern defined by Producer A.
`TMS`	In addition to the verification steps shown in the above row for TIP & SIEM, the

	TMS will 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 will show or provide statistics on how many packets or sessions matched the indicator content.

2.2.5 Respondent Test Case Data

2.2.5.1 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--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"
        }
      }
    }
  ]
}
```

2.2.5.2 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--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": "198.51.100.12"
        }
      }
    }
  ]
}
```

2.2.5.3 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--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": "ipv6-addr",
          "value": "2001:0db8:85a3:0000:0000:8a2e:0370:7334"
        }
      }
    }
  ]
}
```

2.2.5.4 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--b67d30ff-02ac-498a-92f9-32f845f448ff"
      ]
    }
  ]
}
```

2.2.5.5 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--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": "url",
          "Value": "http://www.matchthis.com/t1"
        }
      }
    }
  ]
}
```

2.2.5.6 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--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": "file",
          "hashes": {
            "MD5": "4472ea40dc71e5bb701574ea215a81a1"
          },
          "size": 25536,
          "name": "foo.dll"
        }
      }
    }
  ]
}
```

2.3 Versioning

As additional information is discovered about a STIX SDO the Producer of that object may version the original object using the versioning approach outlined in Part 1 of the Specification. Other recipients of the STIX 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 richer based on enrichments and further intelligence discovery.

2.3.1 Description

A STIX 2.0 **Producer** or **Respondent** must support versioning of objects as a mandatory to implement (MTI) feature within STIX.

2.3.2 Creation

2.3.2.1 Description

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

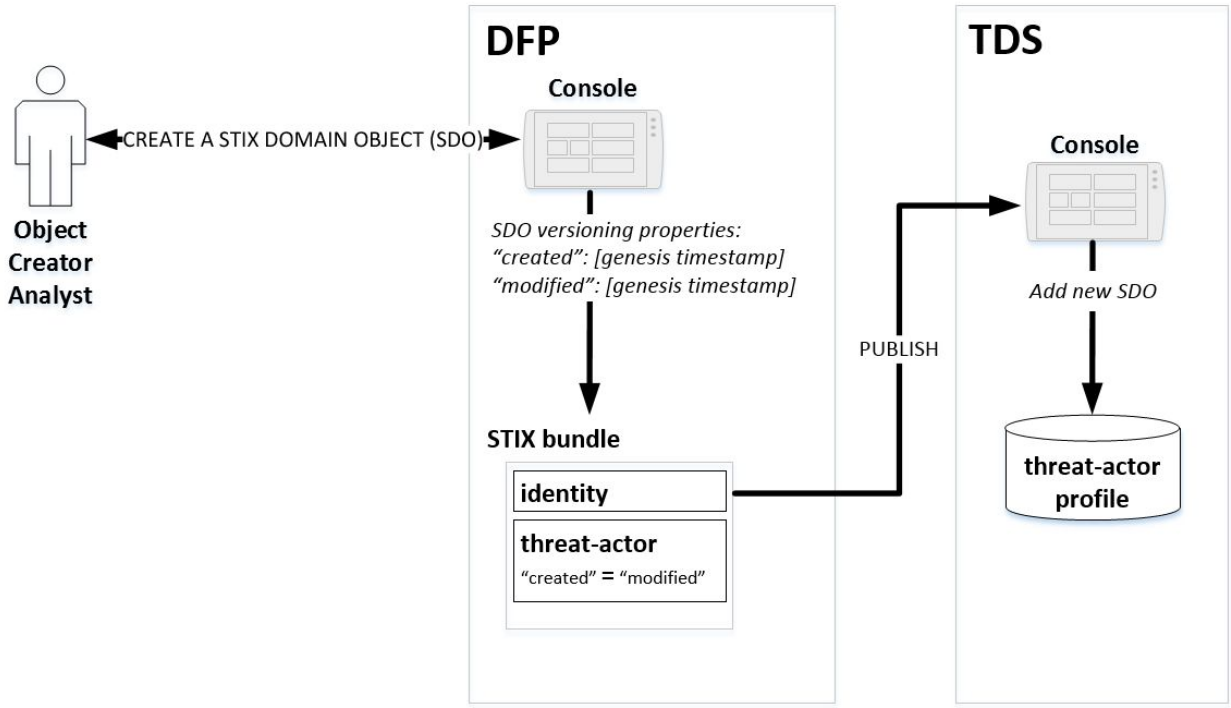


Figure 2.3.2 - An analyst creates a new STIX object

2.3.2.2 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 spec creator Indicators.

Persona	Behavior
All **Indicator** producer personas	1. **Producer** allows a user to select or specify the STIX content the persona supports creation for 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 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 e) 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 f) 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 the persona supports creation for to send to a Respondent persona. 3. The following data MUST be verified in the STIX produced by the persona: b) A bundle object must conform to mandatory attributes within the bundle object including **'type'**; **'id'**; **'spec_version'** and **'objects'** where iii) **Id** has a globally unique identifier iv) **Spec_version** is '2.0' v) Within the **objects** array 1) at least one **identity** for the organization of the **Producer** 2) at least one **sighting** with the observed data for the indicator identified in the pattern parameter g) 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 h) 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

2.3.2.3 Producer Test Case Data

2.3.2.3.1 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"
    }
  ]
}
```

2.3.2.4 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"
        }
      }
    }
  ]
}
```

2.3.2.5 Required Respondent Support

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

Persona	Behavior
All Indicator Respondent Persona	1. **Respondent** allows a user to receive a STIX bundle with a. A bundle with an identity and indicator with IP content b. An identity of the producer c. An indicator with IP address information contained in it 5. Once received the **Respondent** is able to display to the user the Producer's of the indicator based on the identity's attribute 'name' and the identity_class attribute 6. 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 7. For each indicator the **Respondent** may show the **creation** and **modified** dates for them.

2.3.2.6 Respondent Test Case 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.

2.3.3 Modification

2.3.3.1 Description

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

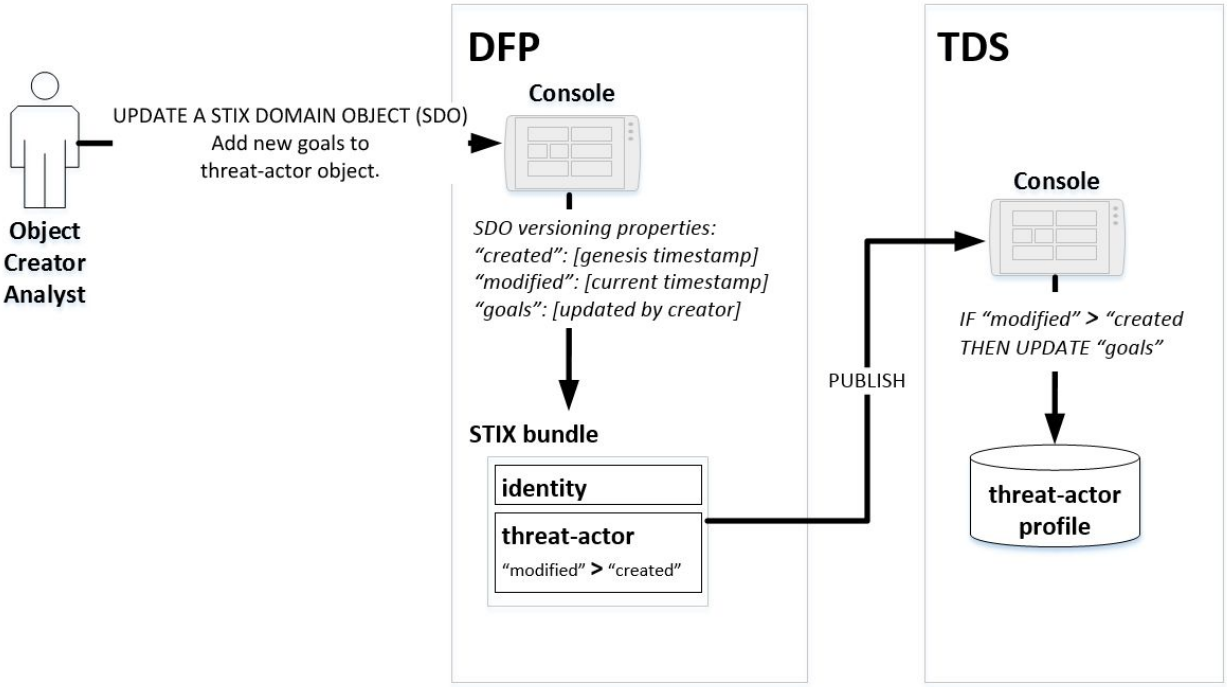


Figure 2.3.3 - An analyst updates a STIX threat-actor object

2.3.3.2 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 updated for sharing.

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 iii) **Id** has a globally unique identifier iv) **Spec_version** is '2.0' v) 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 i) 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 j) 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 the persona supports updates to send to a Respondent persona. 4. The following data MUST be verified in the STIX produced by the persona: c) A bundle object must conform to mandatory attributes within the bundle object including **'type'**; **'id'**; **'spec_version'** and **'objects'** where v) **Id** has a globally unique identifier vi) **Spec_version** is '2.0' vii) Within the **objects** array 1) at least one **identity** for the organization of the **Producer** 2) at least one **sighting** with the observed data for the indicator identified in the pattern parameter k) 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 l) 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 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) **Stop** timestamp must be updated for the new sighting information

2.3.3.3 Producer Test Case Data

2.3.3.3.1 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"
    }
  ]
}
```

2.3.3.3.2 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",
      "start": "2015-12-21T19:00:00Z",
      "stop": "2016-04-06T19:59:17Z",
      "count": 2,
      "objects": {
        "0": {
          "type": "ipv4-addr",
          "value": "198.51.100.1"
        }
      }
    }
  ]
}
```

2.3.3.4 Required Respondent Support

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

Persona	Behavior
All Indicator Respondent personas	1. Respondent allows a user to receive a STIX bundle with a. A bundle with an identity and indicator with pattern content b. An identity of the producer c. An indicator information contained in it 8. 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 9. 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 10. 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. A bundle with an identity and Sighting with pattern content b. An identity of the producer c. An Sighting information contained in it 11. 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 12. 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 13. For each Sighting the Respondent may show the **creation** and **modified** dates for them.

2.3.3.5 Respondent Test Case 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.

2.3.4 Revocation

2.3.4.1 Description

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

<Graphic Here>

2.3.4.2 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 revocation for sharing.

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: d) A bundle object must conform to mandatory attributes within the bundle object including 'type'; 'id'; 'spec_version' and 'objects' where vi) **Id** has a globally unique identifier

	vii) **Spec_version** is '2.0' viii) 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 m) 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 n) 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: e) A bundle object must conform to mandatory attributes within the bundle object including 'type'; 'id'; 'spec_version' and 'objects' where v) **Id** has a globally unique identifier vi) **Spec_version** is '2.0' vii) Within the **objects** array 1) at least one **identity** for the organization of the **Producer** 2) at least one **sighting** and associated observed_data object o) 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 and observed_data p) The sighting 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 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** q) The observed_data object must conform to mandatory attributes of indicator including 'type'; 'id'; 'created_by_ref'; 'created'; 'modified'; revoked where 1) **created_by_ref** must point to the identity of the original

	Producer; 2) **created** must match the original creation timestamp to millisecond granularity of when the user selected the observed_data to be shared 3) **modified** must match the last modified timestamp to millisecond granularity of when the user selected the observed_data to be revoked. 4) **revoked** must be set to true. 5) **The previously shared optional observed_data attributes such as objects may not be included in the object**

2.3.4.3 Producer Test Case Data

2.3.4.3.1 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"
    }
  ]
}
```

2.3.4.3.2 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,
    }
  ]
}
```

2.3.4.4 Required Respondent Support

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

Persona	Behavior
All Indicator Respondent Personas	1. **Respondent** allows a user to receive a STIX bundle with a. A bundle with an identity and indicator with indicator content b. An identity of the producer c. An indicator with pattern information contained in it 14. 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 15. 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 16. 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. A bundle with an identity and sighting & observed_data content b. An identity of the producer c. A sighting with associated observed_data object 17. 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 18. 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 19. For each sighting the **Respondent** may show the creation and modified dates for them and that the object has been revoked.

2.3.4.5 Respondent Test Case 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.

2.4 Data Markings

2.4.1 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, not handled. Data markings can be produced at an object level and at an attribute level.

This section describes basic tests for assigning data markings to shared data using the traffic light protocol (TLP) will also be detailed in this document. TLP is a set of designations used to define the parameters of a sharing event. It is defined by a Forum of Incident Response and Security Teams (FIRST) Special Interest Group (SIG).

2.4.2 Creation

2.4.2.1 Description

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

2.4.2.2 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 2.1.2.1 Producer Test Case Data. All personas defined in 2.1.2 Required Producer Persona Support are also defined for Data Markings producer personas.

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 provides tlp object level markings at any level. a. Producer verifies objects to be marked exist in the bundle. b. Producer must not allow to mark same indicator objects with different TLP level markings at the object level. 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” respectively marking to different objects. 4. The marking-definition must conform to mandatory attributes of marking-definition including: 1. **type** is marking-definition 2. **id** has a globally unique identifier 3. **created_by_ref** points to the organization identity creating both the indicator object and the associated marking 4. **created and modified** time at which the marking-definition was created

	5. **definition_type** open-vocab with a value of “tlp” 6. **definition** the marking object itself 5. The SDO **object_marking_refs** list of marking-definition is populated with markings created by producer and id matches the intended TLP marking. 6. All marking-definition are embedded in the bundle.

2.4.2.3 Producer Test Case Data

2.4.2.3.1 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"
      }
    }
  ]
```

```
}
```

2.4.2.3.2 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"
    }
  ]
}
```

2.4.2.3.3 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"
      }
    }
  ]
}
```

2.4.2.3.4 TLP Red + Relationship between Indicator with IPv4 Address and Malware

```
{
  "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",
      "object_marking_refs": [
        "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da"
      ]
    },
    {
      "type": "malware",
      "id": "malware--31b940d4-6f7f-459a-80ea-9c1f17b5891b",
      "created": "2016-04-06T20:07:09.000Z",
      "modified": "2016-04-06T20:07:09.000Z",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "name": "Some Malware"
      "object_marking_refs": [
        "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da"
      ]
    },
    {
      "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": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "target_ref": "malware--31b940d4-6f7f-459a-80ea-9c1f17b5891b",
      "relationship_type": "indicates",
      "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": "red"
      }
    }
  ]
}
```

2.4.2.4 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 2.1.2.2 Required Respondent Support are also defined for Data Markings.

Persona	Behavior
TIP; SIEM	1. Respondent receives the STIX bundle with 1. A bundle with an identity and indicator with the various required field pattern content 2. An identity of the producer 3. An indicator with various required fields information contained in it 4. An Indicator with data markings applied 5. Connect the associated data marking object with the correct indicator 6. If the indicator identifies a marking 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 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. 5. 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.

2.5 Custom Objects and Properties

2.5.1 Description

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

2.5.2 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 spec creator Indicators.

Persona	Behavior
All producer personas that generate custom objects	1. **Producer** allows a user to select or specify the STIX custom object content the persona supports creation for to send to a Respondent persona. 2. The following data MUST be verified in the STIX produced by the persona: f) A bundle object must conform to mandatory attributes within the bundle object including **'type'**; **'id'**; **'spec_version'** and **'objects'** where 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-**" r) 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 custom object s) 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 standard STIX TLOs	1. **Producer** allows a user to select or specify the STIX standard TLO object content the persona supports creation for to send to a Respondent persona including the custom property associated with the standard TLO. 3. The following data MUST be verified in the STIX produced by the persona: g) A bundle object must conform to mandatory attributes within the bundle object including **'type'**; **'id'**; **'spec_version'** and **'objects'** where iii) **Id** has a globally unique identifier iv) **Spec_version** is '2.0' v) Within the **objects** array

	1) at least one **identity** for the organization of the **Producer** 2) at least one **STIX standard TLO** with at least 1 custom property prefixed with "**x_**" t) 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 STIX TLO u) 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

2.5.3 Producer Test Case Data

2.5.3.1 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"
    }
]
```

2.5.3.2 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,
    }
]
```

2.5.4 Required Respondent Support

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

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 20. 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 21. For each custom object the **Respondent** is able to determine that it is a custom object and not a standard STIX TLO object including verify that the created_by_ref maps to an existing identity received or one contained within the bundle received. 22. **Respondent** must be able to ingest all other standard STIX TLO objects in the bundle 23. 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. A bundle with an identity and standard TLO with a custom properties on standard STIX object 24. Once received the **Respondent** is able to display to the user the source of

	the TLO based on the identity's attribute 'name' and the identity_class attribute 25. For each standard TLO object the **Respondent** is able to determine that it is a standard TLO object and able to ingest/parse all mandatory fields. 26. If the **Respondent** supports the custom property then the **Respondent** may show or use the custom property included in the standard STIX TLO. 27. If the **Respondent** does not support the custom property then the Respondent may discard or show to the user the STIX TLO object has been rejected due to customized properties not being supported without crashing or continuing to support other objects in the bundle that are not customized.

2.5.5 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 not reject all content that may be bundled with standard TLOs. No other data is sent from the Respondent back to the producer.

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 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 [where?]..

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 being verified.

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 for the test results.

After review and verification of the demonstration of interoperability within the submittal the OASIS CTI TC Interoperability SC will post a listing confirming such claims. Our listing will include the following:

1. Name, address and contact information of company performing the demonstration
2. Name of the product for which the demonstration was made
3. Summary of the references used to substantiate the claim on interoperability.

No independent testing will be performed directly by the Interoperability SC; rather the verification process will be to 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 may be defined as a software instance that acts as a producer of STIX 2.0 content.

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

Use Case	Test	Verification	Results
Indicator Sharing	2.1.2.1.1 Indicator IPv4 Address	Mandatory	<fill in>
Indicator Sharing	2.1.2.1.2 Indicator IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	2.1.2.1.3 Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>

Indicator Sharing	2.1.2.1.4 Indicator with IPv6 Address	Optional	<if supported, fill in>
Indicator Sharing	2.1.2.1.5 Indicator with IPv6 Address CIDR	Optional	<if supported, fill in>
Indicator Sharing	2.1.2.1.7 Indicator FQDN	Mandatory	<fill in>
Indicator Sharing	2.1.2.1.8 Indicator URL	Mandatory	<fill in>
Indicator Sharing	2.1.2.1.9 Indicator URL or FQDN	Mandatory	<fill in>
Indicator Sharing	2.1.2.1.10 Indicator File hash with SHA256 or MD5 values	Mandatory	<fill in>
Sighting Sharing	2.2.3 Producer Test Case Data	Mandatory	<fill in>
Versioning	2.3.2.3.1 Creation of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	2.3.3.3.1 Modification of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	2.3.4.3.1 Deletion of an Indicator with Identity; Dates	Mandatory	<fill in>
Versioning	2.3.4.3.2 Deletion of a Sighting and Associated Observed Data	Mandatory	<fill in>
Data Markings	2.4.2.3.1 TLP Green + Indicator with IPv4 Address	Mandatory	<fill in>
Data Markings	2.4.2.3.2 TLP Amber + Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Data Markings	2.4.2.3.3 TLP White and TLP Red + Indicator with IPv6 Address	Optional	<fill in>
Data Markings	2.4.2.3.4 TLP Red + Relationship between Indicator with IPv4 Address and Malware	Optional	<fill in>

Custom Object Creation	2.6.3.1 Custom Object Creation	Optional	<if supported, fill in>
Custom Property Creation	2.6.3.2 Custom Property Creation	Optional	<if supported, fill in>

3.2 Threat Intelligence Platform (TIP)

For the purpose of this document a TIP may be 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 tests.

Use Case	Test	Verification	Results
Indicator Sharing	2.1.2.1.1 Indicator IPv4 Address	Mandatory	<fill in>
Indicator Sharing	2.1.2.1.2 Indicator IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	2.1.2.1.3 Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	2.1.2.1.4 Indicator with IPv6 Address	Optional	<if supported, fill in>
Indicator Sharing	2.1.2.1.5 Indicator with IPv6 Address CIDR	Optional	<if supported, fill in>
Indicator Sharing	2.1.2.1.7 Indicator FQDN	Mandatory	<fill in>
Indicator Sharing	2.1.2.1.8 Indicator URL	Mandatory	<fill in>
Indicator Sharing	2.1.2.1.9 Indicator URL or FQDN	Mandatory	<fill in>
Indicator Sharing	2.1.2.1.10 Indicator File hash with SHA256 or MD5 values	Mandatory	<fill in>
Sighting Sharing	2.2.3 Producer Test Case Data	Mandatory	<fill in>
Sighting Sharing	2.2.5.1 Sighting + Indicator with IPv4 Address	Mandatory	<fill in>

Sighting Sharing	2.2.5.2 Sighting + Indicator with IPv4 Address Matching CIDR	Mandatory	<fill in>
Sighting Sharing	2.2.5.3 Sighting + Indicator with IPv6 Address Matching CIDR	Optional	<if supported, fill in>
Sighting Sharing	2.2.5.4 Sighting + Indicator with NO observed data	Mandatory	<fill in>
Sighting Sharing	2.2.5.5 Sighting + Indicator with URL	Mandatory	<fill in>
Sighting Sharing	2.2.5.6 Sighting + Indicator with File Hash	Mandatory	<fill in>
Versioning	2.3.2.3.1 Creation of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	2.3.3.3.1 Modification of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	2.3.4.3.1 Deletion of an Indicator with Identity: Dates	Mandatory	<fill in>
Versioning	2.3.4.3.2 Deletion of a Sighting and Associated Observed Data	Mandatory	<fill in>
Data Markings	2.4.2.3.1 TLP Green + Indicator with IPv4 Address	Mandatory	<fill in>
Data Markings	2.4.2.3.2 TLP Amber + Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Data Markings	2.4.2.3.3 TLP White and TLP Red + Indicator with IPv6 Address	Optional	<fill in>
Data Markings	2.4.2.3.4 TLP Red + Relationship between Indicator with IPv4 Address and Malware	Optional	<fill in>
Custom Object Creation	2.6.3.1 Custom Object Creation	Optional	<if supported, fill in>

Custom Property Creation	2.6.3.2 Custom Property Creation	Optional	<if supported, fill in>
Custom Ingestion	2.6.4 Required Respondent Support	Mandatory	<fill in>

3.3 Security Incident and Event Management (SIEM)

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

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

Use Case	Test	Verification	Results
Indicator Sharing	2.1.2.1.1 Indicator IPv4 Address	Mandatory	<fill in>
Indicator Sharing	2.1.2.1.2 Indicator IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	2.1.2.1.3 Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	2.1.2.1.4 Indicator with IPv6 Address	Optional	<if supported, fill in>
Indicator Sharing	2.1.2.1.5 Indicator with IPv6 Address CIDR	Optional	<if supported, fill in>
Indicator Sharing	2.1.2.1.7 Indicator FQDN	Mandatory	<fill in>
Indicator Sharing	2.1.2.1.8 Indicator URL	Mandatory	<fill in>
Indicator Sharing	2.1.2.1.9 Indicator URL or FQDN	Mandatory	<fill in>
Indicator Sharing	2.1.2.1.10 Indicator File hash with SHA256 or MD5 values	Mandatory	<fill in>
Sighting Sharing	2.2.3 Producer Test Case Data	Mandatory	<fill in>
Sighting Sharing	2.2.5.1 Sighting + Indicator with IPv4 Address	Mandatory	<fill in>

Sighting Sharing	2.2.5.2 Sighting + Indicator with IPv4 Address Matching CIDR	Mandatory	<fill in>
Sighting Sharing	2.2.5.3 Sighting + Indicator with IPv6 Address Matching CIDR	Optional	<if supported, fill in>
Sighting Sharing	2.2.5.4 Sighting + Indicator with NO observed data	Mandatory	<fill in>
Sighting Sharing	2.2.5.5 Sighting + Indicator with URL	Mandatory	<fill in>
Sighting Sharing	2.2.5.6 Sighting + Indicator with File Hash	Mandatory	<fill in>
Versioning	2.3.2.3.1 Creation of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	2.3.3.3.1 Modification of an Indicator with Identity and Date	Mandatory	<fill in>
Versioning	2.3.4.3.1 Deletion of an Indicator with Identity: Dates	Mandatory	<fill in>
Versioning	2.3.4.3.2 Deletion of a Sighting and Associated Observed Data	Mandatory	<fill in>
Data Markings	2.4.2.3.1 TLP Green + Indicator with IPv4 Address	Mandatory	<fill in>
Data Markings	2.4.2.3.2 TLP Amber + Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Data Markings	2.4.2.3.3 TLP White and TLP Red + Indicator with IPv6 Address	Optional	<fill in>
Data Markings	2.4.2.3.4 TLP Red + Relationship between Indicator with IPv4 Address and Malware	Optional	<fill in>
Custom Object Creation	2.6.3.1 Custom Object Creation	Optional	<if supported, fill in>

Custom Property Creation	2.6.3.2 Custom Property Creation	Optional	<if supported, fill in>
Custom Ingestion	2.6.4 Required Respondent Support	Mandatory	<fill in>

4 Appendix A. Acknowledgments

Interoperability Subcommittee Chairs:

Allan Thomson, LookingGlass,
Jason Keirstead, IBM

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:

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
Ryan Clough, Anomali
Wei Huang, Anomali
Hugh Njemanze, Anomali
Katie Pelusi, Anomali
Aaron Shelmire, Anomali
Jason Trost, 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
Humphrey Christian, Bay Dynamics
Ryan Stolte, Bay Dynamics
Owen Johnson, Blue Coat Systems, Inc.
Aubrey Merchant, Blue Coat Systems, Inc.
Sarah Kelley, Center for Internet Security (CIS)
Cory Kennedy, CenturyLink
Alexandre Dulaunoy, CIRCL
Andras Iklody, CIRCL
Raphaël Vinot, CIRCL
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
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)
Andrew Byrne, Dell
Jeff Odom, Dell
Sreejith Padmajadevi, Dell
Ravi Sharda, Dell
Will Urbanski, Dell
Jeff Williams, 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)
Richard Struse, 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
Joep Gommers, EclecticIQ
Sergey Polzunov, EclecticIQ
Rutger Prins, EclecticIQ
Andrei Sîrghi, EclecticIQ
Aukjan van Belkum, EclecticIQ
Raymon van der Velde, EclecticIQ
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.
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
Koji Yamada, Fujitsu Limited
Kunihiko Yoshimura, Fujitsu Limited

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
Mark Risher, Google Inc.
Richard Austin, Hewlett Packard Enterprise (HPE)
Tomas Sander, Hewlett Packard Enterprise (HPE)
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.
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
Ron Williams, IBM
Paul Martini, iboss, Inc.
Ashwini Jarral, IJIS Institute
Jerome Athias, Individual
Peter Brown, Individual
Joerg Eschweiler, Individual
Stefan Hagen, Individual
Elysa Jones, Individual
Sanjiv Kalkar, Individual
Terry MacDonald, Individual
Patrick Maroney, Individual
Alex Pinto, Individual
Mike Schmidt, Individual

Srinivasa Addepalli, Intel Corporation
Tim Casey, Intel Corporation
Kent Landfield, Intel Corporation
Andres More, Intel Corporation
Steve Orrin, Intel Corporation
Karin Marr, Johns Hopkins University Applied Physics Laboratory
Julie Modlin, Johns Hopkins University Applied Physics Laboratory
Mark Moss, Johns Hopkins University Applied Physics Laboratory
Mark Munoz, 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
Trey Darley, Kingfisher Operations, sprl
Jacob Hinkle, LexisNexis, a Division of Reed Elsevier
Kinshuk Pahare, LookingGlass
Allan Thomson, LookingGlass
Ian Truslove, LookingGlass
Chris Wood, LookingGlass
Greg Back, Mitre Corporation
Jonathan Baker, Mitre Corporation
Sean Barnum, Mitre Corporation
Desiree Beck, Mitre Corporation
Jen, Burns Mitre Corporation
Michael Chisholm, Mitre Corporation
Nicole Gong, Mitre Corporation
Jasen Jacobsen, Mitre Corporation
Ivan Kirillov, 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
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
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
Angelo Mendonca, Nc4
Michael Pepin, Nc4
Natalie Suarez, Nc4
Takahiro Kakumaru, NEC Corporation
Lauri Korts-Pärn, NEC Corporation
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
Cory Casanave, Object Management Group
Johnny Gau, Oracle
Sunil Ravipati, Oracle
Aharon Chernin, Perch
Josh Larkins, PhishMe Inc.
John Tolbert, Queralt Inc.
Daniel Wyschogrod, Raytheon Company-SAS
Ted Julian, Resilient Systems, Inc..
Igor Baikalov, Securonix
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
Greg Reaume, TELUS
Alan Steer, TELUS
Crystal Hayes, The Boeing Company
Wade Baker, ThreatConnect, Inc.
Cole Iliff, ThreatConnect, Inc.
Andrew Pendergast, ThreatConnect, Inc.
Ben Schmoker, ThreatConnect, Inc.
Jason Spies, ThreatConnect, Inc.
Alejandro Valdivia, ThreatConnect, Inc.
Ryan Trost, ThreatQuotient, Inc.
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
Todd Youngblood, U.S. Bank
James Bohling, US Department of Defense (DoD)
Eoghan Casey, 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
Ray-yu Chang, VeriSign
Robert Coderre, VeriSign
Haripriya Gajendran, VeriSign
Kyle Maxwell, VeriSign
Eric Osterweil, VeriSign
Ralph Thomas, VeriSign
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