STIX 2.1 Interoperability Test Document Version 1.0

Committee Specification Draft 01

23 October 2021

This stage:

https://docs.oasis-open.org/cti/stix-2.1-interop/v1.0/csd01/stix-2.1-interop-v1.0-csd01.docx (Authoritative)
https://docs.oasis-open.org/cti/stix-2.1-interop/v1.0/csd01/stix-2.1-interop-v1.0-csd01.html
https://docs.oasis-open.org/cti/stix-2.1-interop/v1.0/csd01/stix-2.1-interop-v1.0-csd01.pdf

Previous stage:

N/A

Latest stage:

https://docs.oasis-open.org/cti/stix-2.1-interop/v1.0/stix-2.1-interop-v1.0.docx (Authoritative)
https://docs.oasis-open.org/cti/stix-2.1-interop/v1.0/stix-2.1-interop-v1.0.html
https://docs.oasis-open.org/cti/stix-2.1-interop/v1.0/stix-2.1-interop-v1.0.pdf

Technical Committee:

OASIS Cyber Threat Intelligence (CTI) TC

Chairs:

Robert Coderre (robert.c.coderre@accenture.com), Accenture
Trey Darley (trey.darley@cert.be), CCB/CERT.be

Editors:

John-Mark Gurney (jgurney@copado.com), Copado
Bret Jordan (bj@ctin.us), Cyber Threat Intelligence Network, Inc.
Michael Rosa (michael.rosa@cisa.dhs.gov), DHS
Marlon Taylor (marlon.taylor@cisa.dhs.gov), DHS
Rajesh Patil (rpatil@lookingglasscyber.com), LookingGlass
Justin Stewart (jstewart@lookingglasscyber.com), LookingGlass
Kartikey Desai (khdesai@mitre.org), MITRE Corporation

Related work:

This document is related to:

- *STIX Version 2.1*. Edited by Bret Jordan, Rich Piazza, and Trey Darley. Latest stage: https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html.

Abstract:

This is the Interoperability test document to supplement the Structured Threat Information Expression (STIX) 2.1 OASIS Standard developed by the Cyber Threat Intelligence Technical Committee (CTI TC) of the Organization for the Advancement of Structured Information Systems (OASIS). This test document provides detailed requirements on how producers of products within the threat intelligence ecosystem may demonstrate STIX 2.1 interoperability compliance. There are several personas detailed in section 1 of this specification. These are: Adversary Infrastructure Mapping (AIM), Local Infrastructure Mapping (LIM), Malware Analysis System (MAS), Security Incident and Event Management (SIEM), STIX Consumer (SXC), STIX Producer (SXP), Threat Detection System (TDS), Threat Intelligence Platform (TIP), and Threat Mitigation System (TMS). This Interoperability test document defines tests of the following use cases: Attack Pattern sharing, Campaign sharing, confidence sharing, Course of Action sharing, Data Marking sharing, Grouping sharing, Indicator sharing, Infrastructure sharing, Intrusion Set sharing, Location sharing, Malware Analysis sharing, Malware sharing, Note sharing, Observed Data sharing, Opinion sharing, Report sharing, Sighting sharing, Threat Actor sharing, Tool sharing, versioning, and Vulnerability sharing. For each of these use cases the document details the Producer support and the Consumer support to be used for the test cases.

Status:

This document was last revised or approved by the OASIS Cyber Threat Intelligence (CTI) TC on the above date. The level of approval is also listed above. Check the "Latest stage" location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti#technical.

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

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

Note that any machine-readable content (Computer Language Definitions) declared Normative for this Work Product is provided in separate plain text files. In the event of a discrepancy between any such plain text file and display content in the Work Product's prose narrative document(s), the content in the separate plain text file prevails.

Key words:

The key words **"MUST"**, **"MUST NOT"**, **"REQUIRED"**, **"SHALL"**, **"SHALL NOT"**, **"SHOULD"**, **"SHOULD NOT"**, **"RECOMMENDED"**, **"NOT RECOMMENDED"**, **"MAY"**, and **"OPTIONAL"** in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Citation format:

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

[STIX-2.1-Interop-v1.0]
STIX 2.1 Interoperability Test Document Version 1.0. Edited by John-Mark Gurney, Bret Jordan, Michael Rosa, Marlon Taylor, Rajesh Patil, Justin Stewart, and Kartikey Desai. 23 October 2021. OASIS Committee Specification Draft 01. https://docs.oasis-open.org/cti/stix-2.1-interop/v1.0/csd01/stix-2.1-interop-v1.0-csd01.html. Latest stage: https://docs.oasis-open.org/cti/stix-2.1-interop/v1.0/stix-2.1-interop-v1.0.html.

Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

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

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

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

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no

representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see https://www.oasis-open.org/policies-guidelines/trademark for above guidance.

Table of Contents

1 Introduction

This document provides details of the Structured Threat Information Expression (STIX) 2.1 Interoperability Test Documents. It lists a set of use cases that a persona (see section 1.2.1) **MUST** follow as they develop minimally viable STIX-compliant tools and services. To claim STIX interoperability compliance, persona tools/services **MUST** adhere to expected behaviors and outcomes as detailed in the use cases.

The OASIS Cyber Threat Intelligence Technical Committee (CTI TC) recommends users of this test document become familiar with the STIX 2.1 OASIS Standard https://www.oasis-open.org/standard/stix-version-2-1/ (as given in the Related Work section above) prior to implementing the use cases in this document. This is what this document is referring to when it mentions “STIX 2.1 OASIS Standard”.

NOTE: The STIX 2.1 OASIS Standard contains normative references to other specifications with which an implementation may need to reference and meet in order to comply with these specifications. This document assumes that such requirements are also met.

1.1 Terminology

Security Infrastructure - Any software or hardware instance that provides a function in the support of securing networks and endpoints.
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 2.1 content to share with other systems. Note that the term Producer is used in the STIX 2.1 OASIS Standard.
Consumer - A software instance that reads STIX 2.1 content and performs some action on that received data. Note that the term Consumer is used in this Committee Note and is inclusive of the term Consumer, which is used in the STIX 2.1 OASIS Standard.

1.2 Overview

The approach that is being taken within the CTI TC is to rely primarily on well-defined, common use cases to drive the interoperability between products using STIX 2.1. Section 2 of this document outlines these common use cases for organizations seeking to develop and demonstrate interoperability.

These use cases will enable personas (see section 1.2.1) of the cyber threat intelligence information sharing community to build and test information sharing files that are compliant with STIX 2.1 best practices. Future revisions to STIX 2.1 will be incorporated into a new version of this document.

1.2.1 Personas

For an organization to demonstrate OASIS STIX interoperability compliance, their software instances will adhere to persona behavior and prescribed STIX content as detailed in the Required Producer and/or Consumer Persona Support section(s) of each use case.

For documenting interoperability compliance for each persona tested, refer to the checklist and test requirements in section 4 Persona Checklist of this document. The following system personas are used throughout this document.

1.2.1.1 Defined Personas

- Adversary Infrastructure Mapping (AIM)
  - Software or system, that consumes and produces STIX content, that is used to map out adversarial networks
- Local Infrastructure Mapping (LIM)
  - Software that scans local networks and provides STIX representations of these finds.
- Malware Analysis System (MAS)
  - Software instance, system, or set of systems that performs static and/or dynamic analysis of binary files and produces STIX content with this analysis information.
- Security Incident and Event Management system (SIEM)
  - Software instance that acts as a Producer and/or Consumer of STIX 2.1 content. A SIEM that produces STIX content will typically create Indicators and other information about incidents. A SIEM that consumes STIX content will typically consume Sightings, Indicators.
- Threat Detection System (TDS)
  - Software instance of any network product that monitors, detects and alerts such as Intrusion Detection Software (IDS), Endpoint Detection and Response (EDR) software, web proxy, etc. This is applicable for both Producers and Consumers.
- Threat Intelligence Platform (TIP)
  - Software instance that acts as a Producer and/or Consumer of STIX 2.1 content primarily used to aggregate, refine and share intelligence with other machines or security personnel operating other security infrastructure.
- Threat Mitigation System (TMS)
  - Software instance that acts on Course of Action and data from other threat mitigations such as a firewall, IPS, Endpoint Detection and Response (EDR) software, etc. This is applicable for both Producers and Consumers.

1.2.1.2 Generic Personas

- STIX Producer (SXP)
  - Software instance that acts as a Producer of STIX 2.1 content.
- STIX Consumer (SXC)
  - Software instance that consumes STIX 2.1 content in order to perform translations to domain-specific formats consumable by enforcement and/or detection systems that do not natively support STIX 2.1. A SXC will typically consume STIX content but may not produce any STIX content itself.

2 Use Case Details

2.1 Defined Persona Use Cases

Table 1 below lists the Producer and Consumer interoperability requirements for each defined persona (see section 1.2.1) as they align to the use cases (see section 3). Interoperability requirements are categorized into two levels. Level 1 contains the minimum set of required Producer and Consumer use cases for a particular persona to achieve STIX Interoperability. Level 2 indicates the required use cases, in addition to Level 1, needed for a persona to achieve a higher level of STIX Interoperability. In other words, for a persona to achieve Level 2 interoperability, that persona must first achieve Level 1 interoperability.

The levels of interoperability are based on how many different use cases are supported by a particular persona's software instance. Support for a particular use case, Producer or Consumer, is meant to ensure interoperability for that use case irrespective of persona or level. For example, a Level 1 Note Producer (e.g. AIM) will be interoperable with a Level 2 Note Consumer (e.g. SIEM). Likewise, a Level 2 Note Producer (e.g. SIEM) must be interoperable with a Level 1 Note Consumer (e.g. TIP).

As another example, in order for a TIP to achieve Level 1 interoperability, a software instance would need to comply with the requirements of all use cases for which TIP is listed in the Level 1 column of Table 1. If a TIP would like to achieve Level 2 interoperability, an instance would need to comply with the requirements of all use cases for which TIP is listed in Table 1.

If an instance complies with the requirements of all the use cases for a defined persona while supporting additional use cases, the instance can achieve:

1. SXP support for all additional Producer use cases and/or
2. SXC support for all additional Consumer use cases

See section 2.2 for more details; the following examples are provided for clarity.

As an example, a LIM may be able to (in addition to the LIM's requirements in Table 1) produce Grouping objects. In this scenario, the instance will have achieved LIM support, as well as SXP support specifically for the Grouping use case.

As another example, a SIEM may be able to (in addition to the SIEM's requirements in Table 1) consume Location objects. In this scenario, the instance will have achieved SIEM support, as well as TIS support specifically for the Location use case.

Table 1 below organizes the pertinent information by use case; to view the requirements organized by persona, see section 4 Persona Checklist.

The following use cases are captured in this document.

Table 1 - List of STIX Interoperability Use Cases

Interoperability	Level 1	Level 2

Use Case	Producer	Consumer	Producer	Consumer
Attack Pattern Sharing	TIP	AIM, TIP	AIM	
Campaign Sharing	AIM, TIP	AIM, TIP		
Confidence Sharing	TIP	TIP		
Course of Action Sharing	TIP	TIP, TMS		TDS
Data Marking Sharing	TIP	TIP		
Grouping Sharing				
Indicator Sharing	TIP	SIEM, TDS, TIP, TMS	MAS	
Infrastructure Sharing	AIM, LIM			AIM, LIM
Intrusion Set Sharing	AIM, TIP	AIM, TIP		
Location Sharing	AIM, LIM		TIP	AIM, TIP
Malware Analysis Sharing	MAS	TIP		
Malware Sharing	MAS, TIP	TIP		
Note Sharing	AIM, LIM, TIP	TIP	SIEM	AIM, SIEM
Observed Data Sharing	LIM, SIEM, TDS	SIEM, TIP	TIP	TDS, TMS
Opinion Sharing	TIP	TIP		
Report Sharing	TIP	TIP		
Sighting Sharing	SIEM, TDS	TDS, TMS	TIP	SIEM, TIP
Threat Actor Sharing	AIM, TIP	AIM, TIP		
Tool Sharing	AIM			AIM
Versioning	SIEM, TDS, TIP, TMS	TIP		SIEM, TDS, TMS
Vulnerability Sharing	LIM, TIP	TIP		LIM

2.2 Generic Persona Use Cases

If a software instance is a Producer for a set of use cases that does not align with the requirements of any particular defined persona, then the instance can be considered a SXP only for those supported use cases. Note, the software instance **MUST**, in addition to the supported use cases, also support the **confidence** sharing, Data Markings Sharing, and Versioning use cases.

For example, if a software instance supports the **confidence** Sharing, Data Markings Sharing, Versioning, and Report Sharing use cases, then this instance can be considered a SXP for Reports.

Similarly, if a software instance is a Consumer for a set of use cases that does not align with the requirements of any particular defined persona, then the instance may be considered a SXC only for those supported use cases. Note, the software instance **MUST**, in addition to the supported use cases, also support the **confidence** sharing, Data Markings Sharing, and Versioning use cases.

For example, if a software instance supports the **confidence** Sharing, Data Markings Sharing, Versioning, and Tool Sharing use cases, then this instance can be considered a SXC for Tools.

The following sections provide details on these use cases.

2.3 Common Use Case Requirements

2.3.1 Producers

All Producers **MUST** abide by the conformance requirements in the "STIX 2.1 Producer" portion of section 12.1 (Conformance for STIX Object Producers and Consumers) of the STIX 2.1 OASIS Standard. This means that all objects created by a Producer **MUST** be compliant with the associated section of the STIX 2.1 OASIS Standard in order to achieve interoperability compliance. For particular use cases, this specification may require Producer personas to support certain properties that are considered optional in the STIX 2.1 OASIS Standard but are required for interoperability compliance. Additionally, for any particular use case, the properties required of a Producer as per this interoperability spec are a minimum set of properties; a Producer is welcome to include any properties from the relevant sections of the STIX 2.1 OASIS Standard that are not already required herein of the Producer.

2.3.2 Consumers

All Consumers **MUST** conform with the “STIX 2.1 Consumer” portion of section 12.1 (Conformance for STIX Object Producers and Consumers) of the STIX 2.1 OASIS Standard. Consumers **MUST** support all properties defined in the “Required Producer Persona Support” subsections of the associated use cases in section 3.

Additionally, a Consumer **MUST** exhibit the following behavior:

1. Consumer allows a users to receive STIX content with:
    a. An Identity of the Producer
    b. One or more *<use-case sharing>* objects
    c. One or more SROs or embedded relationships

2. For each STIX Object, the Consumer **MUST** be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4
3. For each <use case> object, the Consumer can process the information about the <use case> fields to the user
4. For each <use case> object, the Consumer can process any related SDOs/SROs and associated fields

2.3.3 Bundles

The STIX 2.1 OASIS Standard allows object references that are not distributed within the same container (e.g. STIX Bundle). However, the current scope of this specification chooses to rely on all data being within the same container. All objects being referenced (i.e. all objects whose ID is provided by a reference property of another object) **MUST** also be included in the Bundle.

Please note: strictly for brevity, all of the test cases and examples in this document do not include a container to hold the associated objects.

2.3.3.1 Objects Being Referenced

All objects being referenced (as defined above) **MUST** be compliant with the associated section(s) of the STIX 2.1 OASIS Standard. It is not necessary for referenced objects to be compliant with the associated section(s) of the STIX Interoperability standard.

2.3.3.2 TLP Exception

Unlike other objects, TLP markings can be referenced without having to be included in a STIX Bundle, as these objects are formally defined in section 7.2.1.4 of the STIX 2.1 OASIS Standard.

2.3.4 Identities Created

1. All tests require the creation of an Identity for the **created_by_ref** property across all tests.
2. The Identity created should represent the organization that is responsible for the software instance under test.
3. The following properties should be filled in:
    a. **type** with value ‘identity’
    b. **name** with a value that represents the organization’s name
    c. **identity_class** with value ‘organization’
    d. **id** with a unique UUID
    e. **spec_version** with value ‘2.1’
    f. **created** with a timestamp, to millisecond granularity, of when the Identity was created
    g. **modified** with a timestamp, to millisecond granularity, of when the Identity was last modified
    h. **created_by_ref MUST** point to the Identity of the Producer. This property should point to the same UUID as the **id** of this object, if this is the same Producer.

Example:

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



```
    "spec_version": "2.1",
    "created": "2020-01-20T12:34:56.000Z",
    "modified": "2020-01-20T12:34:56.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff”
                      }
```

2.3.5 Representative objects

The objects listed in every Producer and Consumer section represent only the stated objects, unless otherwise explicitly stated. However, in certain use cases, the Producer section will only state the use of the Indicator SDO, but the description will clarify that the Indicator is representative of all SDOs. Likewise, in certain use cases, the Sighting object will be representative of all SROs.

2.3.6 Relationships

Though not required in most Interoperability use cases, Relationship objects can be created and provided by Producers to add context to the produced cyber threat intel. These objects **MUST** comply with the requirements in section 5.1 of the STIX 2.1 OASIS Standard; in particular, **type MUST** be ‘relationship’, **relationship_type MUST** be included and SHOULD be an exact value listed in the relationships for the source and target SDO/SCO (see Appendix B of the STIX 2.1 OASIS Standard), **source_ref** is the id of the source (from) object, and **target_ref** is the id of the target (to) object.

2.3.7 Test Cases vs Examples

In this document, for each use case, test cases and examples will be provided. Compliance with test cases **MUST** be established for the purposes of Interoperability compliance. However, compliance with the examples is not required for Interoperability compliance; rather, the examples are provided to demonstrate potential applications and to enhance the context of the various use cases.

2.3.8 STIX Cyber Observables

Though not required in most Interoperability use cases, STIX Cyber Observable (SCO) objects may be required to be created and provided by Producers based on the requirements within a particular use case. These objects **MUST** comply with the requirements in section 6 of the STIX 2.1 OASIS Standard.

3 Use cases

3.1 Attack Pattern Sharing

Tactics, techniques, and procedures (TTPs) describe behaviors and resources that attackers use to carry out their attacks. Attack Pattern objects are one of three types of TTPs discussed in this document (Malware is another and is discussed in section 3.12, along with Infrastructure which is discussed in section 3.8).

3.1.1 Description

Attack Patterns are a type of TTP that describe ways that adversaries attempt to compromise targets. Attack Patterns help categorize attacks, generalize specific attacks to the patterns that they follow, and provide detailed information about how attacks are performed.

An example of a general attack pattern is "spear phishing," a common type of attack where an attacker sends a carefully crafted e-mail message to a party with the intent of getting them to click a link or open an attachment to deliver malware. Attack Patterns can also be more specific: for example, spear phishing practiced by a particular threat actor who baits the victim by saying that they have won a contest.

3.1.2 Required Producer Persona Support

The Producer persona must be able to create STIX content with an Attack Pattern object; an Attack Pattern can be associated with a variety of SDOs and SROs.

Table 2 - Required Producer Support for Attack Pattern

Personas	Behavior
All Attack Pattern Producer personas	1. Producer allows a user to select or specify the STIX content to send to a Consumer persona 2. The following data must be provided by the persona: a. The Identity object must comply with the Identity object referenced in section 2.3.4 b. The Attack Pattern object must conform to the Attack Pattern specification as per section 4.1 of the STIX 2.1 OASIS Standard; specifically, these properties must be provided: i. **type** must be 'attack-pattern' ii. **spec_version** must be '2.1' iii. **id** must uniquely identify the Attack Pattern, and must be a UUID prepended with 'attack-pattern--' iv. **created_by_ref** must point to the Identity of the Producer v. **external_references** includes pointers to non-STIX information that provides more context about the Attack Pattern vi. **kill_chain_phases** is the list of Kill Chain Phases for which this Attack Pattern is used vii. **created** must match the timestamp, to millisecond granularity, of when the user created the Attack Pattern viii. **modified** must match the timestamp, to millisecond granularity, of when this particular version of the Attack Pattern was last modified ix. **name** must be a string that identifies the Attack Pattern

3.1.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.1.2.

3.1.3.1 Create Attack Pattern Object

A Producer must be able to create an Attack Pattern object, generating content such as the following.

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "attack-pattern",
    "spec_version": "2.1",
    "id": "attack-pattern--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
    "created": "2016-05-12T08:17:27.000Z",
    "modified": "2016-05-12T08:17:27.000Z",
    “created_by_ref”: “identity--f431f809-377b-45e0-aa1c-6a4751cae5ff”,
    "name": "Spear Phishing",
    "external_references": [
        {
            "source_name": "capec",
            "external_id": "CAPEC-163"
        }
    ],
    “kill_chain_phases”: [
        “kill_chain_name”: “example-kill-chain”,
        “phase_name”: “lateral-movement”
    ]
}
```

3.1.3.2 Attack Pattern Targets Vulnerability

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "attack-pattern",
```



```
    "spec_version": "2.1",
    "id": "attack-pattern--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
    "created": "2016-05-12T08:17:27.000Z",
    "modified": "2016-05-12T08:17:27.000Z",
    “created_by_ref”: “identity--f431f809-377b-45e0-aa1c-6a4751cae5ff”,
    "name": "Spear Phishing",
    "external_references": [
        {
            "source_name": "capec",
            "external_id": "CAPEC-163"
        }
    ],
    “kill_chain_phases”: [
        “kill_chain_name”: “example-kill-chain”,
        “phase_name”: “lateral-movement”
    ]
},
{
    "type": "vulnerability",
    "id": "vulnerability--99f01020-864f-4713-84d2-d1eff88a843f",
    "spec_version": "2.1",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    “name”: “CVE-2017-0199”,
    "external_references": [
        {
            "source_name": "cve",
            "external_id": "CVE-2017-0199"
        }
    ]
},
{
    "type": "relationship",
    "id": "relationship--f0afbb80-20a1-404b-a165-01dd45b32239",
    "spec_version": "2.1",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    “source_ref”: “attack-pattern--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061”,
    “target_ref”: “vulnerability--99f01020-864f-4713-84d2-d1eff88a843f”,
    “relationship_type”: “targets”
}
```

3.1.4 Producer Example Data

3.1.4.1 Add Context to Indicator

An Attack Pattern object can provide context to an Indicator. Example content is below. Note that reference is made to an external Attack Pattern identifier (CAPEC) using the property **external_references**.


```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--0c7e22ad-b099-4dc3-b0df-2ea3f49ae2e6",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2019-05-12T08:17:27.000Z",
    "modified": "2019-05-12T08:17:27.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[url:value = 'http://badsite.com/foo' OR url:value = 'http://badsite.com/bar']
    "pattern_type": "stix",
    "valid_from": "2019-01-01T00:00:00Z"
},
{
    "type": "attack-pattern",
    "spec_version": "2.1",
    "id": "attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2019-05-12T08:17:27.000Z",
    "modified": "2019-05-12T08:17:27.000Z",
    "name": "Spear Phishing as Practiced by Adversary X",
    "description": "Spear phishing where the attacker includes personal details in the email
and claims that the target had won a contest.",
    "external_references": [
        {
            "source_name": "capec",
            "external_id": "CAPEC-163"
        }
    ]
},
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--57b56a43-b8b0-4cba-9deb-34e3e1faed9e",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2019-05-12T08:17:27.000Z",
    "modified": "2019-05-12T08:17:27.000Z",
    "relationship_type": "indicates",
    "source_ref": "indicator--0c7e22ad-b099-4dc3-b0df-2ea3f49ae2e6",
    "target_ref": "attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5"
}
```

3.1.4.2 Leverage Externally Defined Frameworks

Context can be added to an SDO by defining a relationship between the SDO and one or more externally-defined Attack Pattern objects. The SRO example below, between a Malware and Attack Pattern object, references an attack pattern defined for a framework such as ATT&CK [https://github.com/mitre/cti]. See Section 2.12.5.1 for the optional discussion of how framework Attack Pattern objects can be ingested for use as a data source. Here, ATT&CK is referenced only for example purposes; Producers are not required to support any externally-defined frameworks.

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    “created_by_ref”: “identity--f431f809-377b-45e0-aa1c-6a4751cae5ff”
},
{
    "type": "malware",
    "spec_version": "2.1",
    "id": "malware--1121ffbc-364f-857a-9987-92fbcff24ab",
    "created": "2019-05-12T08:17:27.000Z",
    "modified": "2019-05-12T08:17:27.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "name": "Cryptolocker",
    "description": "A variant of the cryptolocker family",
    "malware_types": [ "ransomware" ],
    "is_family": false
},
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--11220001-3940-0405-20ff-1029b0bc922",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2020-01-16T18:52:24.277Z",
    "modified": "2020-01-16T18:52:24.277Z",
    "relationship_type": "uses",
    "source_ref": "malware--1121ffbc-364f-857a-9987-92fbcff24ab",
    "target_ref": "attack-pattern--b80d107d-fa0d-4b60-9684-b0433e8bdba0",
    "object_marking_refs": ["marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"]
},
{
    "type": "attack-pattern",
    "id": "attack-pattern--b80d107d-fa0d-4b60-9684-b0433e8bdba0",
    "spec_version": "2.1",
    "created": "2019-03-15T13:59:30.390Z",
    "modified": "2019-03-15T13:59:30.390Z",
    “created_by_ref”: “identity--f431f809-377b-45e0-aa1c-6a4751cae5ff”,
    "kill_chain_phases": [
        {
            "kill_chain_name": "mitre-attack",
```



```
            "phase_name": "impact"
        }
    ],
    "name": "Data Encrypted for Impact",
    "description": "Adversaries may encrypt data on target systems or on large numbers of
systems in a network to interrupt availability to system and network resources…”
}
```

3.1.5 Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Attack Pattern object. Additional required Consumer support for Attack Patterns is listed in the table below.

Table 3 - Required Consumer Support for Attack Patterns

Personas	Behavior
All Attack Pattern Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more Attack Pattern objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each Attack Pattern object, the Consumer can process the information about the Attack Pattern fields to the user 4. For each Attack Pattern object, the Consumer can process any related SDOs/SROs and associated fields

3.1.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the Attack Pattern Producer Test Case Data, as per the requirements in section 3.1.5.

3.1.7 Consumer Example Data

3.1.7.1 Ingest External Framework Data

A Consumer can choose to be able to ingest content from external frameworks, such as ATT&CK [https://github.com/mitre/cti]. It is not required that a Consumer be able to ingest custom properties. A Consumer may then use the framework data in a Producer role, referencing content after ingest. Alternatively, they could use the content internally to provide context to other cyber threat intelligence.

The example below corresponds to the ATT&CK technique Data Encrypted for Impact. Because a Consumer is not required to ingest custom properties, they have been omitted. Some external references were removed for brevity.

```
{
    "type": "identity",
    "id": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "spec_version": "2.1",
    "identity_class": "organization",
```



```
    "name": "The MITRE Corporation",
    "created": "2017-06-01T00:00:00.000Z",
    "modified": "2017-06-01T00:00:00.000Z",
    “created_by_ref”: “identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5"
},
{
    "type": "attack-pattern",
    "id": "attack-pattern--b80d107d-fa0d-4b60-9684-b0433e8bdba0",
    "spec_version": "2.1",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "created": "2019-03-15T13:59:30.390Z",
    "modified": "2019-07-19T14:35:12.349Z",
    "name": "Data Encrypted for Impact",
    "description": "Adversaries may encrypt data on target systems or on large numbers of
systems in a network to interrupt availability to system and network resources...",
    "kill_chain_phases": [
        {
            "kill_chain_name": "mitre-attack",
            "phase_name": "impact"
        }
    ],
    "external_references": [
        {
            "source_name": "mitre-attack",
            "external_id": "T1486",
            "url": "https://attack.mitre.org/techniques/T1486"
        },
        {
            "source_name": "US-CERT Ransomware 2016",
            "description": "US-CERT. (2016, March 31). Alert (TA16-091A): Ransomware and
Recent Variants. Retrieved March 15, 2019.",
            "url": "https://www.us-cert.gov/ncas/alerts/TA16-091A"
        }
    ]
}
```

3.2 Campaign Sharing

A Campaign is a grouping of adversarial behaviors that describes a set of malicious activities or attacks that occur over a period of time against a specific set of targets. Campaigns usually have well-defined objectives and may be part of an Intrusion Set.

3.2.1 Description

Campaigns are often attributed to an intrusion set and threat actors. The threat actors may reuse known infrastructure from the intrusion set or may set up new infrastructure specific for conducting that campaign.

Campaigns can be characterized by their objectives and the incidents they cause, people or resources they target, and the resources (infrastructure, intelligence, Malware, Tools, etc.) they use.

For example, a Campaign could be used to describe a crime syndicate's attack using a specific variant of malware and new C2 servers against the executives of ACME Bank during the summer of 2016 in order to gain secret information about an upcoming merger with another bank.

3.2.2 Required Producer Persona Support

The Producer Persona must be able to create STIX content with one or more Campaign objects.

Table 4 - Required Producer Support for Campaign

Personas	Behavior
All Campaign Producer personas	1. Producer allows a user to select or specify the STIX content to send to a Consumer persona 2. The following data must be provided by the persona: a. The Identity object must comply with the Identity object referenced in section 2.3.4 b. The Campaign object must conform to the Campaign specification as per section 4.2 of the STIX 2.1 OASIS Standard; specifically, these properties must be provided: i. **type** must be 'threat-actor' ii. **spec_version** must be '2.1' iii. **id** must uniquely identify the Campaign, and must be a UUID prepended with 'campaign--' iv. **created_by_ref** must point to the Identity of the Producer v. **created** must match the timestamp, to millisecond granularity, of when the Campaign was originally created vi. **modified** must match the timestamp, to millisecond granularity, of when this particular version of the Campaign was last modified vii. **name** is populated with the name of the Campaign

3.2.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.2.2.

3.2.3.1 Campaign Test Case

A producer must be able to create an Identity and a Campaign.

```
{
    "type": "identity",
    "name": "ACME Corp, Inc.",
    "identity_class": "organization",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
```



```
    "created": "2015-01-20T12:34:56.000Z",
    "modified": "2015-01-20T12:34:56.000Z",
    “created_by_ref”: "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "campaign",
    "spec_version": "2.1",
    "id": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-04-06T20:03:00.000Z",
    "modified": "2016-04-06T20:03:00.000Z",
    "name": "Green Group Attacks Against Finance"
}
```

3.2.3.2 Campaign Attributed to Intrusion Set

```
{
    "type": "identity",
    "name": "ACME Corp, Inc.",
    "identity_class": "organization",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "created": "2015-01-20T12:34:56.000Z",
    "modified": "2015-01-20T12:34:56.000Z",
    “created_by_ref”: "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "campaign",
    "spec_version": "2.1",
    "id": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-04-06T20:03:00.000Z",
    "modified": "2016-04-06T20:03:00.000Z",
    "name": "Green Group Attacks Against Finance"
},
{
    "type": "intrusion-set",
    "id": "intrusion-set--9352cbaf-b3b8-4be5-9304-5bd7a8400255",
    "spec_version": "2.1",
    "created": "2015-01-20T12:34:56.000Z",
    "modified": "2015-01-20T12:34:56.000Z",
    “created_by_ref”: "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    “name”: “Cheetah Breakin”,
    “resource_level”: “club”,
    “primary_motivation”: “notoriety”
},
{
    "type": "relationship",
    "id": "relationship-7f6bb959-6288-417d-9fd6-bac8cf994bcc",
    "spec_version": "2.1",
    "created": "2015-01-20T12:34:56.000Z",
    "modified": "2015-01-20T12:34:56.000Z",
    “created_by_ref”: "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
```



```
    “source_ref”: “campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f”,
    “target_ref”: “intrusion-set--9352cbaf-b3b8-4be5-9304-5bd7a8400255”,
    “relationship_type”: “attributed-to”
},
```

3.2.4 Producer Example Data

3.2.4.1 Campaign Uses an Attack Pattern

One use case for the Campaign SDO is to describe the malicious activities associated with an attack. This example captures the attack pattern used as part of a campaign.

```
{
    "type": "identity",
    "id": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "spec_version": "2.1",
    "created": "2015-04-14T13:07:49.812Z",
    "modified": "2015-04-14T13:07:49.812Z",
    "name": "Oscorp Industries",
    "identity_class": "organization",
    “created_by_ref”: "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c"
},
{
    "type": "campaign",
    "spec_version": "2.1",
    "id": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2016-08-08T15:50:10.983Z",
    "modified": "2016-08-08T15:50:10.983Z",
    "name": "Operation Bran Flakes",
    "description": "A concerted effort to insert false information into the BPP's web pages.",
    "aliases": [
        "OBF"
    ],
    "first_seen": "2016-01-08T12:50:40.123Z",
    "objective": "Hack www.bpp.bn"
},
{
    "type": "attack-pattern",
    "spec_version": "2.1",
    "id": "attack-pattern--19da6e1c-71ab-4c2f-886d-d620d09d3b5a",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2016-08-08T15:50:10.983Z",
    "modified": "2017-01-30T21:15:04.127Z",
    "name": "Content Spoofing",
    "external_references": [
        {
            "source_name": "capec",
            "url": "https://capec.mitre.org/data/definitions/148.html",
            "external_id": "CAPEC-148"
        }
    ]
},
```



```
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--33c22977-d104-45d8-be19-273f7ab03de1",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2020-02-29T17:41:44.940Z",
    "modified": "2020-02-29T17:41:44.940Z",
    "relationship_type": "uses",
    "source_ref": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
    "target_ref": "attack-pattern--19da6e1c-71ab-4c2f-886d-d620d09d3b5a"
}
```

3.2.4.2 Campaign Attributed to Threat Actor

This example demonstrates how a Campaign SDO can be linked to the threat actor carrying out attacks against targets.

```
{
    "type": "identity",
    "id": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "spec_version": "2.1",
    "created": "2015-04-14T13:07:49.812Z",
    "modified": "2015-04-14T13:07:49.812Z",
    "name": "Oscorp Industries",
    "identity_class": "organization",
    "contact_information": "norman@oscorp.com",
    "sectors": [
        "technology"
    ]
},
{
    "type": "campaign",
    "spec_version": "2.1",
    "id": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2016-08-08T15:50:10.983Z",
    "modified": "2016-08-08T15:50:10.983Z",
    "name": "Operation Bran Flakes",
    "description": "A concerted effort to insert false information into the BPP's web pages.",
    "aliases": [
        "OBF"
    ],
    "first_seen": "2016-01-08T12:50:40.123Z",
    "objective": "Hack www.bpp.bn"
},
{
    "type": "threat-actor",
    "spec_version": "2.1",
    "id": "threat-actor--9a8a0d25-7636-429b-a99e-b2a73cd0f11f",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2015-05-07T14:22:14.760Z",
    "modified": "2015-05-07T14:22:14.760Z",
    "name": "Adversary Bravo",
```



```
    "description": "Adversary Bravo is known to use phishing attacks to deliver remote access
malware to the targets.",
    "threat_actor_types": [
        "spy",
        "criminal"
    ]
},
{
    "type": "relationship",
    "spec_version": "2.1",
    id": "relationship--33c22977-d104-45d8-be19-273f7ab03de1",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2020-02-29T17:41:44.940Z",
    "modified": "2020-02-29T17:41:44.940Z",
    "relationship_type": "attributed-to",
    "source_ref": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
    "target_ref": "threat-actor--9a8a0d25-7636-429b-a99e-b2a73cd0f11f"
}
```


3.2.5 Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Campaign object. Additional required Consumer support for Campaigns is listed in the table below.

Table 5 - Required Consumer Support for Campaigns

Persona	Behavior
All Campaign Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more Campaign objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each Campaign object, the Consumer can process the information about the Campaign fields to the user 4. For each Campaign object, the Consumer can process any related SDOs/SROs and associated fields

3.2.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the Campaign Producer Test Case Data, as per the requirements in section 3.2.5.

3.3 Confidence Sharing

3.3.1 Description

Unlike the previous sections that address SDOs and SROs, this section addresses a common property—confidence. The **`confidence`** property identifies the confidence that the Producer has in the correctness

of their data. The confidence value **MUST** be a number in the range of 0-100 (the STIX confidence scale); the property is of type `integer`. Appendix A of the STIX 2.1 OASIS Standard document contains normative mappings to five confidence scales: None/Low/Medium/High, 0-10 Scale, Admiralty Credibility, Words of Estimative Probability (WEP), and Director of National Intelligence (DNI) Scale.

The associated STIX confidence value (`integer`) **MUST** be used when capturing a confidence value from one of these scales. If the **`confidence`** property is not present, then the confidence of the content is unspecified.

3.3.2 Required Producer Persona Support

The Producer persona must be able to create STIX content with the **`confidence`** property defined on one or more SDOs/SROs.

*Table 6 - Required Producer Support for **confidence***

Personas	Behavior
All confidence Producer personas	1. Producer allows a user to select or specify the STIX content to send to a Consumer persona 2. The following data must be provided by the persona: a. The Identity object must comply with the Identity object referenced in section 2.3.4 b. The SDO/SRO object(s) must conform to the requirements in the relevant section(s) of the STIX 2.1 OASIS Standard

3.3.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.3.2.

3.3.3.1 Confidence about Indicator, External Validation

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "id": "indicator--76fa276c-1984-4bb1-938f-7834a6b30090",
    "spec_version": "2.1",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2020-02-06T20:03:48.000Z",
    "modified": "2020-02-06T20:03:48.000Z",
    "confidence": 85,
    "indicator_types": [ "benign" ],
    "name": "Benign site",
```



```
    "pattern": "[ url:value = 'http://weibo.com']",
    "pattern_type": "stix",
    "valid_from": "2020-01-01T00:00:00Z"
}
```

3.3.4 Producer Example Data

3.3.4.1 Confidence about Indicator, Internal Validation

Prior to releasing an Indicator object, a cybersecurity team writes and deploys signatures and tests to confirm the accuracy of the Indicator pattern. Upon completion of their tests, the team releases an Indicator conveying the level of accuracy via the confidence value.

Given that a level of confidence can be validated, the Producer can produce content as shown below:

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2019-04-06T20:03:48.000Z",
    "modified": "2019-04-06T20:03:48.000Z",
    "confidence": 95,
    "indicator_types": ["malicious-activity"],
    "name": "Poison Ivy Malware",
    "description": "This file is part of Poison Ivy",
    "pattern": "[ file:hashes.'SHA-256' =
'4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877' ]",
    "pattern_type": "stix",
    "valid_from": "2019-01-01T00:00:00Z"
},
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--44298a74-ba52-4f0c-87a3-1824e67d7fad",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2019-04-06T20:06:37.000Z",
    "modified": "2019-04-06T20:06:37.000Z",
    "confidence": 90,
    "relationship_type": "indicates",
    "source_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "target_ref": "malware--31b940d4-6f7f-459a-80ea-9c1f17b5891b"
```



```
},
{
    "type": "malware",
    "spec_version": "2.1",
    "id": "malware--31b940d4-6f7f-459a-80ea-9c1f17b5891b",
    "created": "2019-04-06T20:07:09.000Z",
    "modified": "2019-04-06T20:07:09.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "name": "Poison Ivy",
    "malware_types": ["trojan"]
}
```

3.3.4.2 Confidence on Translation

A STIX Language Content Object can be used to capture a translation of a STIX Object into another language[1]; the confidence property reflects confidence in the accuracy of the translation.

In the example below, the confidence score is 100 because the simple text is easily translated into German, French, and Japanese:

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref: "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "campaign",
    "id": "campaign--12a111f0-b824-4baf-a224-83b80237a094",
    "lang": "en",
    "spec_version": "2.1",
    "created": "2017-02-08T21:31:22.007Z",
    "modified": "2017-02-08T21:31:22.007Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "name": "Bank Attack",
    "description": "More information about bank attack"
},
{
    "type": "language-content",
    "id": "language-content--b86bd89f-98bb-4fa9-8cb2-9ad421da981d",
    "spec_version": "2.1",
    "created": "2017-02-08T21:31:22.007Z",
    "modified": "2017-02-08T21:31:22.007Z",
    "confidence": 100,
    "object_ref": "campaign--12a111f0-b824-4baf-a224-83b80237a094",
    "object_modified": "2017-02-08T21:31:22.007Z",
    "contents": {
```

[1] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_z9r1cwtu8jja


```
        "de": {
            "name": "Bank Angriff",
            "description": "Weitere Informationen über Banküberfall"
        }
    }
},
{
    "type": "language-content",
    "id": "language-content--a2cd6c46-d999-4a79-95ae-0c6cb2fc0648",
    "spec_version": "2.1",
    "created": "2017-02-08T21:31:22.007Z",
    "modified": "2017-02-08T21:31:22.007Z",
    "confidence": 90,
    "object_ref": "campaign--12a111f0-b824-4baf-a224-83b80237a094",
    "object_modified": "2017-02-08T21:31:22.007Z",
    "contents": {
        "fr": {
            "name": "Attaque Bank",
            "description": "Plus d'informations sur la crise bancaire"
        }
    }
},
{
    "type": "language-content",
    "id": "language-content--fe76d222-40f1-4c7d-8dd1-643681356df7",
    "spec_version": "2.1",
    "created": "2017-02-08T21:31:22.007Z",
    "modified": "2017-02-08T21:31:22.007Z",
    "confidence": 95,
    "object_ref": "campaign--12a111f0-b824-4baf-a224-83b80237a094",
    "object_modified": "2017-02-08T21:31:22.007Z",
    "contents": {
        "ja": {
            "name": "銀行への攻撃",
            "description": "銀行への攻撃の追加情報"
        }
    }
}
```

3.3.5 Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the **confidence** property. Additional required Consumer support for **confidence** is listed in the table below.

*Table 7 - Required Consumer Support for **confidence***

Personas	Behavior
All confidence Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more SDOs or SROs with **confidence** specified c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields

	within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each STIX object, the Consumer can process the information about the object's fields to the user 4. For each STIX object, the Consumer can process any related SDOs/SROs and associated fields

3.3.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the **confidence** Producer Test Case Data, as per the requirements in section 3.3.5.

3.3.7 Consumer Example Data

The following subsections provide examples to illustrate potential uses of the confidence property.

3.3.7.1 Convert to Different Confidence Scales

A Consumer should be able to convert the value of the **confidence** property to the different scales described in Appendix A of the STIX 2.1 OASIS Standard. The confidence scales mapped to the STIX 0-100 confidence scale are: None/Low/Medium/High, 0-10 Scale, Admiralty Credibility, Words of Estimative Probability (WEP), Director of National Intelligence (DNI) Scale.

A Consumer can parse STIX content containing the **confidence** property and map the value to other confidence scales. In this example, the STIX confidence value of 70 would map to "2 - Probably True" under the Admiralty Credibility scale and "Likely / Probable" under the WEP scale.

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "campaign",
    "spec_version": "2.1",
    "id": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2019-04-06T20:03:00.000Z",
    "modified": "2019-04-06T20:03:00.000Z",
    "confidence": 70,
    "name": "Green Group Attacks Against Finance",
    "description": "Campaign by Green Group against a series of targets in the financial
services sector."
}
```

3.4 Course Of Action Sharing

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

3.4.1 Description

However, the COA object in STIX 2.1 is a stub. It is included to support basic use cases (such as sharing prose courses of action) but, at this time, it does not support the ability to represent automated courses of action or contain properties to represent metadata about courses of action.

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

3.4.2 Required Producer Persona Support

Table 8 - Required Producer Support for Course of Action

Personas	Behavior
All Course of Action Producer personas	1. Producer allows a user to select or specify the STIX content to send to a Consumer persona 2. The following data must be provided by the persona: a) The Identity object must comply with the Identity object referenced in section 2.3.4 b) The Course of Action object must conform to the Course of Action specification as per section 4.3 of the STIX 2.1 OASIS Standard; specifically, these properties must be provided: i) **type** must be 'course-of-action' ii) **spec_version** must be '2.1' iii) **id** must uniquely identify the Course of Action, and must be a UUID prepended with 'course-of-action--' iv) **created_by_ref** must point to the Identity of the Producer; v) **created** must match the timestamp, to millisecond granularity, of when the user created the Course of Action vi) **modified** must match the timestamp, to millisecond granularity, of when this particular version of the Course of Action was last modified vii) **name** is used to identify the Course of Action

3.4.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.4.2.

3.4.3.1 Create Course of Action

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
```



```
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "course-of-action",
    "id": "course-of-action--97250bf1-7ab6-4c79-b8c0-b59f6fc62e9d",
    "spec_version": "2.1",
    "name": "Add TCP port 80 Filter Rule to the existing Block UDP 1434 Filter",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z"
}
```

3.4.4 Producer Example Data

3.4.4.1 Create COA with Relationship

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "course-of-action",
    "id": "course-of-action--17ce1618-0aab-4366-a93a-9d290282995e",
    "spec_version": "2.1",
    "name": "Add TCP port 80 Filter Rule to the existing Block UDP 1434 Filter",
    "description": "This is how to add a filter rule to block inbound access to TCP port 80 to
the existing UDP 1434 filter..",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z"
},
{
    "type": "relationship",
    "id": "relationship--1d79e2b8-c4e2-4f64-a9b3-739de42bc1c6",
    "spec_version": "2.1",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "source_ref": "course-of-action--17ce1618-0aab-4366-a93a-9d290282995e",
    "target_ref": "indicator--bc7a2301-d711-465d-a8bf-97d50e1cb68f",
    "relationship_type": "mitigates"
},
{
    "type": "indicator",
    "id": "indicator--bc7a2301-d711-465d-a8bf-97d50e1cb68f",
```



```
    "spec_version": "2.1",
    "name": "Poison Ivy Malware",
    "description": "Popular remote access tool.",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[file:hashes.MD5 = '3773a88f65a5e780c8dff9cdc3a056f3']",
    "pattern_type": "stix"
}
```

3.4.5 Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Course of Action object. Additional required Consumer support for Courses of Action is listed in the table below.

Table 9 - Required Consumer Support for Course of Action

Persona	Behavior
All Course of Action Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more Course of Action objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the created_by_ref, as enumerated in section 2.3.4 3. For each Course of Action object, the Consumer can process the information about the Course of Action fields to the user 4. For each Course of Action object, the Consumer can process any related SDOs/SROs and associated fields

3.4.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the Course of Action Producer Test Case Data, as per the requirements in section 3.4.5.

3.5 Data Markings Sharing

A STIX 2.1 Producer or Consumer must support markings applied to objects and the related operations around them. The Data Markings use case focuses on how markings should be represented. This specification does not prescribe *how* Consumers are to interpret markings and provide any marking-specified mitigations. Data Markings can be produced at an object level.

3.5.1 Description

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

3.5.2 Required Producer Persona Support

Producers should allow users to apply object level markings to an SDO or SRO at all TLP levels.

Table 10 - Required Producer Support for Data Marking

Persona	Behavior
All Data Markings Producer personas	1. Producer allows a user or an administrator to apply object level markings to Indicators that are being shared 2. Producer may provide TLP object level markings at any TLP designation a. Producer must NOT mark Indicator objects with more than one TLP level marking 3. The Producer references the existing Marking Definition object for the request: a. For different objects, the user can apply different TLP designations including: **tlp** "green"; **tlp** "amber"; **tlp** "red"; **tlp** "white", as defined in the STIX 2.1 OASIS Standard

3.5.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.5.2.

3.5.3.1 TLP White + Indicator with IPv4 Address

```
{
    "type": "identity",
    "id": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "name": "Bad IP1",
    "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "spec_version": "2.1",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "object_marking_refs": ["marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"],
    "pattern": "[ipv4-addr:value = '198.51.100.1']",
    "pattern_type": "stix"
}
```

3.5.3.2 TLP Green + Indicator with IPv4 Address

```
{
    "type": "identity",
    "id": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "name": "Bad IP2",
    "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "spec_version": "2.1",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "object_marking_refs": ["marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da"],
    "pattern": "[ipv4-addr:value = '198.51.102.2']",
    "pattern_type": "stix"
}
```

3.5.3.3 TLP Amber + Indicator with IPv4 Address CIDR

```
{
    "type": "identity",
    "id": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "id": "indicator--2713b690-877e-4d25-a992-6e80efefa49f",
    "spec_version": "2.1",
    "name": "Bad IP Subnets",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "object_marking_refs": ["marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"],
    "pattern": "[ipv4-addr:value ISSUBSET '198.51.100.0/24' OR ipv4-addr:value ISSUBSET
'196.45.200.0/24']",
    "pattern_type": "stix"
}
```


3.5.3.4 TLP Red + Indicator with IPv6 Address

```
{
    "type": "identity",
    "id": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "id": "indicator--c6b3dbc6-f279-4193-90c2-2967a0a16485",
    "spec_version": "2.1",
    "name": "Bad IPv6-1",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[ipv6-addr:value = '2001:0db8:85a3:0000:0000:8a2e:0370:7334']",
    "object_marking_refs": ["marking-definition--5e57c739-391a-4eb3-b6be-7d15ca92d5ed"],
    "pattern_type": "stix"
}
```

3.5.4 Producer Example Data

3.5.4.1 Copyright Statement

```
{
    "type": "identity",
    "id": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "id": "indicator--c6b3dbc6-f279-4193-90c2-2967a0a16485",
    "spec_version": "2.1",
    "name": "Bad IPv6-1",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[ipv6-addr:value = '2001:0db8:85a3:0000:0000:8a2e:0370:7334']",
    "object_marking_refs": ["marking-definition--3556db42-ad8e-47ec-a696-9b1695d7760f"],
```



```
    "pattern_type": "stix"
},
{
    "type": "marking-definition",
    "spec_version": "2.1",
    "id": "marking-definition--3556db42-ad8e-47ec-a696-9b1695d7760f",
    "created": "2021-01-01T00:00:00.000Z",
    "definition_type": "statement",
    "definition": {
        "statement": "Copyright 2021, Example Corp"
    }
}
```

3.5.5 Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Data Markings object. Additional required Consumer support for Data Markings is listed in the table below.

Table 11 - Required Consumer Support for Data Markings

Persona	Behavior
All Data Marking Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more Data Marking objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each Data Marking object, the Consumer can process the information about the Data Marking fields to the user 4. For each Data Marking object, the Consumer can process any related SDOs/SROs and associated fields

3.5.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the Data Marking Producer Test Case Data, as per the requirements in section 3.5.5.

3.6 Grouping Sharing

A Grouping object explicitly asserts that the referenced STIX Objects have a shared context, unlike a STIX Bundle (which explicitly conveys no context). A Grouping object should not be confused with an intelligence product, which should be conveyed via a STIX Report.

3.6.1 Description

A STIX Grouping object might represent a set of data that, in time, given sufficient analysis, would mature to convey an incident or threat report as a STIX Report object. For example, a Grouping could be used to characterize an ongoing investigation into a security event or incident. A Grouping object could also be used to assert that the referenced STIX Objects are related to an ongoing analysis process, such as

when a threat analyst is collaborating with others in their trust community to examine a series of Campaigns and Indicators. The Grouping SDO contains a list of references to SDOs, SCOs, and SROs, along with an explicit statement of the context shared by the content, a textual description, and the name of the grouping.

3.6.2 Required Producer Persona Support

The Producer persona must be able to create STIX content that contains a Grouping object.

Table 12 - Required Producer Support for Grouping

Personas	Behavior
All Grouping Producer personas	1. Producer allows a user to select or specify the STIX content to send to a Consumer persona 2. The following data must be provided by the persona: a. The Identity object must comply with the Identity object referenced in section 2.3.4 b. The Grouping object must conform to the Grouping specification as per section 4.4 of the STIX 2.1 OASIS Standard; specifically, these properties must be provided: i. **type** must be 'grouping' ii. **spec_version** must be '2.1' iii. **id** must uniquely identify the Grouping, and must be a UUID prepended with 'grouping--' iv. **created_by_ref** must point to the Identity of the Producer v. **created** must match the timestamp, to millisecond granularity, of when the Grouping was originally created vi. **modified** must match the timestamp, to millisecond granularity, of when this particular version of the Grouping was last modified vii. **context** must contain a short descriptor of the context referenced by the Grouping. Values **SHOULD** be from the grouping-context-ov open vocabulary viii. **object_refs** must specify the object(s) that the Grouping references c. The object(s) referenced in the Grouping's **object_refs**. The object(s) must comply with the relevant section(s) of the STIX 2.1 OASIS Standard

3.6.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.6.2.

3.6.3.1 Grouping Test Case

A Producer must be able to create an Identity and Grouping object as per the Producer requirements in Table x of section 2.18.2, such as the below content.

```
{
    "type": "identity",
    "name": "ACME Corp, Inc.",
    "identity_class": "organization",
    "id": "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283",
    "spec_version": "2.1",
    "created": "2012-01-20T12:34:56.000Z",
    "modified": "2012-01-20T12:34:56.000Z",
```



```
    “created_by_ref”: "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283"
},
{
    "type": "grouping",
    "spec_version": "2.1",
    "id": "grouping--84e4d88f-44ea-4bcd-bbf3-b2c1c320bcb3",
    "created_by_ref": "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283",
    "created": "2015-12-21T19:59:11.000Z",
    "modified": "2015-12-21T19:59:11.000Z",
    "context": "suspicious-activity",
    "object_refs": [
        "indicator--26ffb872-1dd9-446e-b6f5-d58527e5b5d2"
    ]
},
{
    "type": "indicator",
    "id": "indicator--26ffb872-1dd9-446e-b6f5-d58527e5b5d2",
    "spec_version": "2.1",
    "name": "Bad IP1",
    "created_by_ref": "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283",
    "created": "2014-01-17T11:11:13.000Z",
    "modified": "2014-01-17T11:11:13.000Z",
    "valid_from": "2013-01-01T00:00:00.000Z",
    "indicator_types": [ "malicious-activity" ],
    "pattern": "[ipv4-addr:value = '198.51.100.1']",
    "pattern_type": "stix"
}
```

3.6.4 Producer Example Data

3.6.4.1 Suspicious Event Grouping

This use case involves multiple Observed Data SDOs that, together, represent a suspicious event, where the **context** property is "suspicious-activity" (see Figure 1). Grouping with this higher order context provides initial steps towards clustering and event-based analysis. Hence, in this use case, the Grouping object represents user and entity behavior analytics (UEBA) or similar event-level analysis.

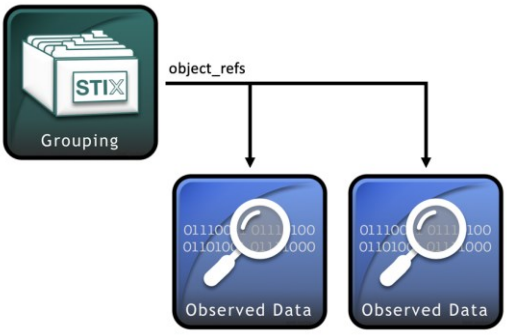

Figure 1. Suspicious event Grouping diagram

For example, the producer might produce the following Grouping object:

```
{
```

```
    "type": "identity",
    "id": "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    “created_by_ref”: "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283"
},
{
    "type": "grouping",
    "spec_version": "2.1",
    "id": "grouping--84e4d88f-44ea-4bcd-bbf3-b2c1c320bcb3",
    "created_by_ref": "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283",
    "created": "2020-04-21T19:59:11.000Z",
    "modified": "2020-04-21T19:59:11.000Z",
    "name": "Suspicious event Grouping",
    "context": "suspicious-activity",
    "object_refs": [
        "observed-data--26ffb872-1dd9-446e-b6f5-d58527e5b5d2",
        "observed-data--83422c77-904c-4dc1-aff5-5c38f3a2c55c"
    ]
},
{
    "type": "observed-data",
    "spec_version": "2.1",
    "id": "observed-data--26ffb872-1dd9-446e-b6f5-d58527e5b5d2",
    "created_by_ref": "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283",
    "created": "2020-04-18T09:34:11.000Z",
    "modified": "2020-04-18T09:34:11.000Z"
    "first_observed": "2020-04-18T06:14:10.000Z",
    "last_observed": "2020-04-18T09:12:31.000Z",
    "number_observed": 50,
    "object_refs": [
        "ipv4-address--efcd5e80-570d-4131-b213-62cb18eaa6a8",
        "domain-name--ecb120bf-2694-4902-a737-62b74539a41b"
    ]
},
{
    "type": "domain-name",
    "spec_version": "2.1",
    "id": "domain-name--ecb120bf-2694-4902-a737-62b74539a41b",
    "value": "suspiciousplace.com",
    "resolves_to_refs": [ "ipv4-addr--efcd5e80-570d-4131-b213-62cb18eaa6a8" ]
},
{
    "type": "sighting",
    "spec_version": "2.1",
    "id": "sighting--49247b1f-6158-480f-ad26-6a2f9303f22b",
    "created_by_ref": "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283",
    "created": "2020-04-22T03:51:01.000Z",
    "modified": "2020-04-22T03:51:01.000Z",
    “sighting_of_ref”: "grouping--84e4d88f-44ea-4bcd-bbf3-b2c1c320bcb3",
```



```
    “observed_data_refs”: [ "observed-data--83422c77-904c-4dc1-aff5-5c38f3a2c55c" ]
},
{
    "type": "ipv4-addr",
    "spec_version": "2.1",
    "id": "ipv4-addr--efcd5e80-570d-4131-b213-62cb18eaa6a8",
    "value": "198.51.100.3"
},
{
    "type": "observed-data",
    "spec_version": "2.1",
    "id": "observed-data--83422c77-904c-4dc1-aff5-5c38f3a2c55c",
    "created_by_ref": "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283",
    "created": "2020-04-21T03:51:01.000Z",
    "modified": "2020-04-21T03:51:01.000Z"
    "first_observed": "2020-04-21T02:11:01.000Z",
    "last_observed": "2020-04-21T02:11:01.000Z",
    "number_observed": 1,
    "object_refs": [
        "network-traffic--2568d22a-8998-58eb-99ec-3c8ca74f527d"
    ]
},
{
    "type": "ipv4-addr",
    "spec_version": "2.1",
    "id": "ipv4-addr--4d22aae0-2bf9-5427-8819-e4f6abf20a53",
    "value": "128.29.99.14"
},
{
    "type": "network-traffic",
    "spec_version": "2.1",
    "id": "network-traffic--2568d22a-8998-58eb-99ec-3c8ca74f527d",
    "src_ref": "ipv4-addr--efcd5e80-570d-4131-b213-62cb18eaa6a8",
    "dst_ref": "ipv4-addr--4d22aae0-2bf9-5427-8819-e4f6abf20a53",
    "protocols": [
        "tcp"
    ]
}
```

3.6.4.2 Malware Analysis Grouping

This use case comprises a combination of SDOs and SROs that describe the analysis of a specific Malware SDO or collection of malware samples (see Figure 2). It is important to note that a Grouping object with the **context** property set to "malware-analysis" does not replace the Malware Analysis object; rather, it provides a wider context to group relevant objects, which may (or may not) include a Malware Analysis object.

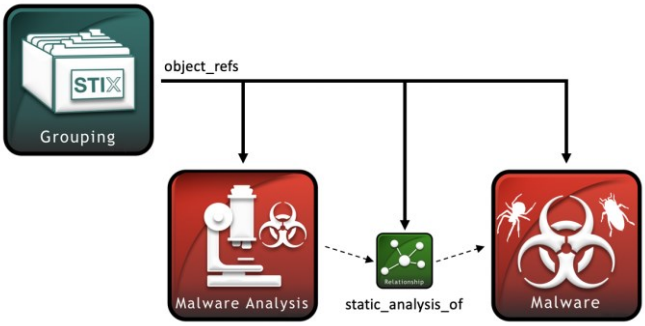

Figure 2. Malware analysis Grouping diagram

For example, the producer might produce the following Grouping object:

```
{
    "type": "identity",
    "id": "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z"
},
{
    "type": "grouping",
    "spec_version": "2.1",
    "id": "grouping--83745900-3485-1204-3495-34958ff94b22",
    "created_by_ref": "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283",
    "created": "2020-05-05T19:59:11.000Z",
    "modified": "2020-05-05T19:59:11.000Z",
    "name": "Malware Analysis Grouping",
    "context": "malware-analysis",
    "object_refs": [
        "malware--bd839453-0334-12bb-3cde-18473be4d73fa",
        "malware-analysis--8475bdef-0345-34be-3921-3847bef26a78",
        "relationship--3746283c-cde7-be73-2736-e8df93f92001"
    ]
},
{
    "type": "malware",
    "spec_version": "2.1",
    "id": "malware--bd839453-0334-12bb-3cde-18473be4d73fa",
    "created_by_ref": "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283",
    "created": "2018-08-18T23:55:56.000Z",
    "modified": "2018-09-03T05:38:32.000Z",
    "name": "zeus",
    "malware_types": [ "password-stealer" ],
    "is_family": true,
    "sample_refs": [ "file--32d46183-b04a-53f4-a610-fbb4be60c4f6" ]
},
{
```



```
    "type": "file",
    "id": "file--32d46183-b04a-53f4-a610-fbb4be60c4f6",
    "spec_version": "2.1",
    "size": 95744,
    "hashes": {
        "SHA-256": "d912d711520f9b44a249cc098f05f9618731f84d922a9c30916db6d6ba73fe22",
        "SHA-1": "dcab07b13eb4eb5b90a2bc5f947ddf0f7d8ad6f9"
    }
},
{
    "type": "malware-analysis",
    "spec_version": "2.1",
    "id": "malware-analysis--8475bdef-0345-34be-3921-3847bef26a78",
    "created_by_ref": "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283",
    "created": "2020-03-16T18:52:24.277Z",
    "modified": "2020-03-16T18:52:24.277Z",
    "product": "av-tool",
    "analysis_engine_version": "5.1.0",
    "analysis_definition_version": "053514-0062",
    "analysis_started": "2020-03-16T06:12:00Z",
    "analysis_ended": "2020-03-16T06:14:08Z",
    "result": "malicious",
    "sample_ref": "file--32d46183-b04a-53f4-a610-fbb4be60c4f6"
},
{
    "type": "relationship",
    "spec_version": "2.1"
    "id": "relationship--3746283c-cde7-be73-2736-e8df93f92001",
    "created": "2020-05-04T08:25:26.000Z",
    "modified": "2020-05-04T08:25:26.000Z",
    “created_by_ref”: “identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283”,
    "relationship_type": "static-analysis-of",
    "source_ref": "malware-analysis--8475bdef-0345-34be-3921-3847bef26a78",
    "target_ref": "malware--bd839453-0334-12bb-3cde-18473be4d73fa"
}
```

3.6.4.3 Duplicate Sightings Grouping

With inside knowledge, CTI clearinghouses may determine receipt of the same Sighting from different organizations. This use case uses a Grouping object to convey duplicate Sightings as a single STIX object. It is necessary to use a Grouping object because STIX 2.1 does not allow relationships between SROs.

An example Grouping object is below.

```
{
    "type": "grouping",
    "spec_version": "2.1",
    "id": "grouping--84e4d88f-44ea-4bcd-bbf3-b2c1c320bcb3",
    "created_by_ref": "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283",
    "created": "2020-04-21T19:59:11.000Z",
    "modified": "2020-04-21T19:59:11.000Z",
    "name": "Sighting Grouping",
    "description": "The referenced Sightings are duplicates and represent a single sighting",
```



```
    "context": "duplicate-of",
    "object_refs": [
        "sighting--613f2e26-407d-48c7-9eca-b8e91df99dc9",
        "sighting--34098fce-860f-48ae-8e50-ebd3cc5e41da",
        "sighting--37362738-fe00-342b-3451-8748338deee9",
        "sighting--f88d31f6-486f-44da-b317-01333bde0b82"
    ]
},
{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator–88574fb3-ce02-aaf2-2984bbb84993",
    "created": "2019-12-01T00:00:00.000Z",
    "modified": "2019-12-01T00:00:00.000Z",
    "valid_from": "2020-02-20T22:28:19.313Z",
    "pattern": "[file:hashes.MD5 = 'd41d8cd98f00b204e9800998ecf8427e']",
    "pattern_type": "stix"
},
{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator–74654fff-2435-463b-bd41-36444453febd",
    "created": "2019-12-01T00:00:00.000Z",
    "modified": "2019-12-01T00:00:00.000Z",
    "valid_from": "2020-02-20T22:28:19.313Z",
    "pattern": "[file:hashes.MD5 = '79054025255fb1a26e4bc422aef54eb4']",
    "pattern_type": "stix"
},
{
    "type": "identity",
    "id": "identity--73737483-3212-0495-45bb-03b4b23b43bd",
    "spec_version": "2.1",
    "created": "2019-08-11T15:07:09.000Z",
    "modified": "2019-08-11T15:07:09.000Z",
    "name": "ISAO",
    "description": "An ISAO"
    "identity_class": "organization"
},
{
    "type": "identity",
    "id": "identity--8493bf90-3475-6654-dfefa857b432",
    "spec_version": "2.1",
    "created": "2017-11-11T10:07:12.000Z",
    "modified": "2017-11-11T10:07:12.000Z",
    "name": "Vendor",
    "description": "A threat intel vendor"
    "identity_class": "organization"
},
{
    "type": "identity",
    "id": "identity--74756489-bed8-de0a-ad23-abe9d90ed126",
    "spec_version": "2.1",
    "created": "2018-06-08T08:07:00.000Z",
```

```
    "modified": "2018-06-08T08:07:00.000Z",
    "name": "Researcher",
    "description": "A threat intel researcher"
    "identity_class": "organization"
},
{
    "type": "identity",
    "id": "identity--b4b23b43-0002-374b-3876-befd647a4200",
    "spec_version": "2.1",
    "created": "2017-12-29T15:05:19.000Z",
    "modified": "2017-12-29T15:05:19.000Z",
    "name": "SIEM",
    "description": "A SIEM tool",
    "identity_class": "organization"
},
{
    "type": "sighting",
    "id": "sighting--613f2e26-407d-48c7-9eca-b8e91df99dc9",
    "spec_version": "2.1",
    "created_by_ref": "identity--73737483-3212-0495-45bb-03b4b23b43bd",
    "created": "2020-03-01T09:11:13.000Z",
    "modified": "2020-03-01T09:11:13.000Z",
    "sighting_of_ref": "indicator—88574fb3-ce02-aaf2-2984bbb84993",
    "count": 10
},
{
    "type": "sighting",
    "id": "sighting--34098fce-860f-48ae-8e50-ebd3cc5e41da",
    "spec_version": "2.1",
    "created_by_ref": "identity--8493bf90-3475-6654-dfefa857b432",
    "created": "2020-03-02T07:15:58.160Z",
    "modified": "2020-03-02T07:15:58.160Z",
    "sighting_of_ref": "indicator—88574fb3-ce02-aaf2-2984bbb84993",
    "count": 20
},
{
    "type": "sighting",
    "id": "sighting--37362738-fe00-342b-3451-8748338deee9",
    "spec_version": "2.1",
    "created_by_ref": "identity--74756489-bed8-de0a-ad23-abe9d90ed126",
    "created": "2020-03-03T11:14:35.000Z",
    "modified": "2020-03-03T11:14:35.000Z",
    "sighting_of_ref": "indicator—74654fff-2435-463b-bd41-36444453febd",
    "count": 30
},
{
    "type": "sighting",
    "id": "sighting--f88d31f6-486f-44da-b317-01333bde0b82",
    "spec_version": "2.1",
    "created_by_ref": "identity--b4b23b43-0002-374b-3876-befd647a4200",
    "created": "2020-03-01T10:04:20.244Z",
    "modified": "2020-03-01T10:04:20.244Z",
    "sighting_of_ref": "indicator—88574fb3-ce02-aaf2-2984bbb84993",
```



```
    "count": 40
}
```

3.6.5 Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Grouping object. Additional required Consumer support for Groupings is listed in the table below.

Table 13 - Required Consumer Support for Grouping

Persona	Behavior
All Grouping Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more Grouping objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each Grouping object, the Consumer can process the information about the Grouping fields to the user 4. For each Grouping object, the Consumer can process any related SDOs/SROs and associated fields

3.6.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the Grouping Producer Test Case Data, as per the requirements in section 3.6.5.

3.7 Indicator Sharing

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

IOCs and other STIX objects (SDOs, SCOs, SROs, etc.), as defined in the STIX 2.1 OASIS Standard, 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 2.1 data model. Some TIPs also provide for data enrichment, analysis and indexing, visualization and bi-directional IOC sharing with other security products through well-crafted application programming interfaces (APIs). The Consumers of the SDOs include both the personas documented in this Committee Note for machine readable threat intelligence (MRTI) and human analysts including, but not limited to: threat intelligence analysts, fraud and risk analysts, malware analysts, and network and endpoint guardians, among others. This high-level view is useful for illustrating how a use case (in this case, sharing of Indicator objects) and a persona will work together within this Committee Note for the purpose of interoperability demonstration.

The following sections provide more detailed descriptions of how a STIX 2.1 Indicator object may be used for the purpose of demonstrating interoperability.

3.7.1 Description

A STIX 2.1 Indicator is an object primarily used to identify malicious content, which is represented as a pattern. There are several common characteristics of the data that can be verified. An analyst can identify one or more Indicators that indicate malicious content on the Internet. That content may be an entity of interest to consider for monitoring activity. Also, for example, a TIP may produce and include the Indicator as part of a STIX Bundle that is sent to a TMS. The TMS could then potentially create a new firewall rule based on the **pattern** content.

3.7.2 Required Producer Persona Support

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

Table 14 - Required Producer Support for Indicator

Personas	Behavior
All Indicator Producer Personas	1. Producer allows a user to select or specify the STIX content to send to a Consumer persona 2. The following data must be provided by the persona: a) The Identity object must comply with the Identity object referenced in section 2.3.4 b) The Indicator object must conform to the Indicator specification as per section 4.7 of the STIX 2.1 OASIS Standard; specifically, these properties must be provided: i) **type** must be 'indicator' ii) **spec_version** must be '2.1' iii) **id** must uniquely identify the Indicator, and must be a UUID prepended with 'indicator--' iv) **created_by_ref** must point to the Identity of the Producer v) **created** must match the timestamp, to millisecond granularity, of when the Indicator was originally created vi) **modified** must match the timestamp, to millisecond granularity, of when this particular version of the Indicator was last modified vii) **valid_from** is the time from which this Indicator is considered a valid indicator of the behaviors it is related to or represents viii) **name** identifies the Indicator to help products and analysts understand what the Indicator actually does ix) **pattern** is the detection pattern for this Indicator that may be expressed as a STIX Pattern as specified in section 9 of the STIX 2.1 OASIS Standard, or another appropriate language such as SNORT, YARA, etc. x) **pattern_type** is the pattern language used in this Indicator xi) **indicator_types** is a list of type open-vocab that contains categorizations for this indicator. The values for this property **SHOULD** come from the indicator-type-ov open vocab. The default value should be ['unknown']

3.7.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.7.2.

3.7.3.1 Indicator IPv4 Address

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "id": "indicator--12fd1bad-8306-4ed4-8c9b-7dfdd8ad5eb8",
    "spec_version": "2.1",
    "name": "Bad IP1",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[ipv4-addr:value = '198.51.100.1']",
    "pattern_type": "stix”
}
```

3.7.3.2 Indicator IPv4 Address CIDR

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "id": "indicator--86449d6c-c47a-4320-bb94-2eb7340928e8",
    "spec_version": "2.1",
    "name": "Bad IP CIDR",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[ipv4-addr:value ISSUBSET '198.51.100.0/24']",
```



```
    "pattern_type": "stix"
}
```

3.7.3.3 Indicator with two IPv4 Address CIDRs

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "id": "indicator--1b0eb2d2-cce4-4c18-a58d-cf238ceea505",
    "spec_version": "2.1",
    "name": "Bad IP Subnets",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[ipv4-addr:value ISSUBSET '198.51.100.0/24' OR ipv4-addr:value ISSUBSET
'196.45.200.0/24']",
    "pattern_type": "stix"
}
```

3.7.3.4 Indicator with IPv6 Address

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "id": "indicator--919974fa-2461-4476-91ae-dd033c700f49",
    "spec_version": "2.1",
    "name": "Bad IPv6-1",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[ipv6-addr:value = '2001:0db8:85a3:0000:0000:8a2e:0370:7334']",
    "pattern_type": "stix"
```



```
}
```

3.7.3.5 Indicator with IPv6 Address CIDR

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "id": "indicator--b5dcc585-bf19-4ace-aa56-1e004448ee2a",
    "spec_version": "2.1",
    "name": "Bad IPv6-CIDR",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[ipv6-addr:value ISSUBSET '2001:DB8::0/120']",
    "pattern_type": "stix"
}
```

3.7.3.6 Multiple Indicators

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "id": "indicator--674aae52-d49b-412e-ab61-514e31f8021e",
    "spec_version": "2.1",
    "name": "Bad IP Subnets",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[ipv4-addr:value ISSUBSET '198.51.100.0/24' OR ipv4-addr:value ISSUBSET
'196.45.200.0/24']",
    "pattern_type": "stix"
},
```



```
{
    "type": "indicator",
    "id": "indicator--e40f9107-9a76-4c92-89c0-d512fde1c120",
    "spec_version": "2.1",
    "name": "Bad IP1",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[ipv4-addr:value = '198.51.100.12']",
    "pattern_type": "stix"
}
```

3.7.3.7 Indicator FQDN

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "id": "indicator--69a4eedb-05c5-463b-ba59-65257d652cf4",
    "spec_version": "2.1",
    "name": "Bad Domain",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[domain-name:value = 'www.5z8.info']",
    "pattern_type": "stix"
}
```

3.7.3.8 Indicator URL

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
```



```
    "id": "indicator--21edc30b-11c9-406d-867a-42fb4bdeedda",
    "spec_version": "2.1",
    "name": "Bad URL",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[url:value = 'https://www.5z8.info/foo']",
    "pattern_type": "stix"
}
```

3.7.3.9 Indicator URL or FQDN

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "id": "indicator--81090d66-3036-4ff9-8032-c5facb50b20f",
    "spec_version": "2.1",
    "name": "Bad URL or Domain",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[url:value = 'https://www.5z8.info/foo' OR domain-name:value =
'www.5z8.info']",
    "pattern_type": "stix"
}
```

3.7.3.10 Indicator File hash with SHA256 or MD5 values

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "id": "indicator--0cddd4c0-411a-47a7-8ccc-d0473d690a6f",
```



```
    "spec_version": "2.1",
    "name": "Bad File1",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[file:hashes.'SHA-256' =
'bf07a7fbb825fc0aae7bf4a1177b2b31fcf8a3feeaf7092761e18c859ee52a9c' OR file:hashes.MD5 =
'cead3f77f6cda6ec00f57d76c9a6879f']",
    "pattern_type": "stix"
}
```

3.7.4 Producer Example Data

3.7.4.1 Indicator with Description

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "id": "indicator--0cddd4c0-411a-47a7-8ccc-d0473d690a6f",
    "spec_version": "2.1",
    "name": "Bad File1",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "description": "This is an Indicator associated with malicious activity, with the included
SHA-256 hash",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[file:hashes.'SHA-256' =
'bf07a7fbb825fc0aae7bf4a1177b2b31fcf8a3feeaf7092761e18c859ee52a9c' OR file:hashes.MD5 =
'cead3f77f6cda6ec00f57d76c9a6879f']",
    "pattern_type": "stix"
}
```

3.7.5 Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Indicator object. Additional required Consumer support for Indicators is listed in the table below. Also, the Consumer must be able to handle an Indicator with **pattern_type** of "stix".

Table 15 - Required Consumer Support for Indicator

Persona	Behavior
All Indicator Consumer personas	1. Consumer allows a users to receive STIX content with: a. An Identity of the Producer b. One or more Indicator objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each Indicator object, the Consumer can process the information about the Indicator fields to the user 4. For each Indicator object, the Consumer can process any related SDOs/SROs and associated fields

3.7.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the Indicator Producer Test Case Data, as per the requirements in section 3.7.5.

3.7.7 Consumer Example Data

These examples aim to provide further context to the potential behaviors an Indicator Consumer may exhibit. In particular, the ability for a Consumer to exhibit unique behaviors based on their persona is shown in these examples.

3.7.7.1 TIP Indicator Consumer

The below Indicator's pattern contains an IPv4 address that is believed to be compromised by the Producer of this content. The TIP Consumer can display this IPv4 address as an Indicator of Compromise.

```
{
    "type": "identity",
    "id": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
    "created": "2015-01-20T12:34:56.000Z",
    "modified": "2015-01-20T12:34:56.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--a5b23aa5-76cc-45ca-9b06-be2d65defabc",
    "created_by_ref": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "created": "2015-01-21T12:34:56.000Z",
    "modified": "2015-01-21T12:34:56.000Z",
    "description": “Example of what a TIP Indicator Consumer can do”,
    "valid_from": "2015-01-01T00:00:00.000Z",
    "pattern": "[ipv4-addr:value = '198.51.100.1']",
    "pattern_type": "stix",
```

```
    "indicator_types": [ "compromised" ]
}
```

3.7.7.2 TMS Indicator Consumer

The below Indicator's pattern contains the SHA-256 hash of a file that is believed to be associated with malicious remote execution activity. A TMS Consumer could update its rules to match on this hash, and then act on any matches found in captured network traffic.

```
{
    "type": "identity",
    "id": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
    "created": "2015-01-20T12:34:56.000Z",
    "modified": "2015-01-20T12:34:56.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--aaabbbcc-cddd-eeef-fff6-be2d65defabc",
    "created_by_ref": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "created": "2015-01-21T12:34:56.000Z",
    "description": “Example of what a TMS Indicator Consumer can do”,
    "modified": "2015-01-21T12:34:56.000Z",
    "valid_from": "2015-01-01T00:00:00.000Z",
    "pattern": "[file:hashes.'SHA-256' =
'112233443bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877']",
    "pattern_type": "stix",
    "indicator_types": [ "malicious-activity" ]
}
```

3.7.7.3 TDS Indicator Consumer

The below Indicator's pattern contains the FQDN on which the Producer has noticed anomalous activity. Seeing this, a TMS Consumer may be suspicious of the FQDN and could update its rules to match on this hash, including in captured network traffic.

```
{
    "type": "identity",
    "id": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
    "created": "2015-01-20T12:34:56.000Z",
    "modified": "2015-01-20T12:34:56.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--abcabcab-cdef-defd-ef12-342d65defabc",
    "created_by_ref": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
```



```
    "created": "2015-01-21T12:34:56.000Z",
    "description": “Example of what a TDS Indicator Consumer can do”,
    "modified": "2015-01-21T12:34:56.000Z",
    "valid_from": "2015-01-01T00:00:00.000Z",
    "pattern": "[domain-name:value = 'www.fake-acme-corp.info']",
    "pattern_type": "stix",
    "indicator_types": [ "anomalous-activity" ]
}
```

3.7.7.4 SXC Indicator Consumer

The below Indicator's pattern contains an IPv6 address for which the Producer has noticed anomalous activity. Seeing this, a TIS Consumer may check that the Indicator has not been previously received, and then update its rules to match on this IPv6 address.

```
{
    "type": "identity",
    "id": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
    "created": "2015-01-20T12:34:56.000Z",
    "modified": "2015-01-20T12:34:56.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--baeabcaa-cdef-defd-ef12-342d65defabc",
    "created_by_ref": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "created": "2015-01-21T12:34:56.000Z",
    "description": “Example of what a TIS Indicator Consumer can do”,
    "modified": "2015-01-21T12:34:56.000Z",
    "valid_from": "2015-01-01T00:00:00.000Z",
    "pattern": "[ipv6-addr:value = '2001:0db8:85a3:0000:0000:8a2e:0370:7334']",
    "pattern_type": "stix",
    "indicator_types": [ "anomalous-activity" ]
}
```

3.7.7.5 SIEM Indicator Consumer

The below Indicator's pattern contains a URL for which the Producer has noticed malicious activity. Receiving this, a SIEM could ensure that the Indicator has not been previously applied to its event correlation and display functions, along with updating its rules to match on the Indicator content. A SIEM may also display and/or alert upon other relevant security information it has from other event log sources (e.g. firewalls, sensors). A SIEM may also generate a Sighting instance based on the Indicator.

```
{
    "type": "identity",
    "id": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
    "created": "2015-01-20T12:34:56.000Z",
```



```
    "modified": "2015-01-20T12:34:56.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--baeabcaa-cdef-defd-ef12-342d65defabc",
    "created_by_ref": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "created": "2015-01-21T12:34:56.000Z",
    "description": “Example of what a SIEM Indicator Consumer can do”,
    "modified": "2015-01-21T12:34:56.000Z",
    "valid_from": "2015-01-01T00:00:00.000Z",
    "pattern": "[url:value = 'https://www.evilsite.info/foo']",
    "pattern_type": "stix",
    "indicator_types": [ "malicious-activity" ]
}
```

3.8 Infrastructure Sharing

Tactics, techniques, and procedures (TTPs) describe behaviors and resources that attackers use to carry out their attacks. Infrastructure objects are one of three types of TTPs discussed in this document (Attack Patterns and Malware are the others, discussed in sections 3.1 and 3.12, respectively).

3.8.1 Description

The Infrastructure SDO describes systems, software services and any associated physical or virtual resources intended to support some purpose (e.g., C2 servers used as part of an attack, device or server that are part of defense, database servers targeted by an attack). While elements of an attack can be represented by other SDOs or SCOs, the Infrastructure SDO represents a named group of related data that constitutes the infrastructure.

3.8.2 Required Producer Persona Support

The Producer persona must be able to create STIX content that contains an Infrastructure object.

Table 16 - Required Producer Support for Infrastructure

Personas	Behavior
All Infrastructure Producer personas	1. Producer allows a user to select or specify the STIX content to send to a Consumer persona 2. The following data must be provided by the persona: a. The Identity object must comply with the Identity object referenced in section 2.3.4 b. The Infrastructure object must conform to the Infrastructure specification as per section 4.8 of the STIX 2.1 OASIS Standard; specifically, these properties must be provided: i. **type** must be ‘infrastructure’ ii. **spec_version** must be ‘2.1’ iii. **id** must uniquely identify the Infrastructure object and must be a UUID prepended with ‘infrastructure--’ iv. **created_by_ref** must point to the Identity of the Producer v. **created** is the time at which the Infrastructure was originally created

	vi. **modified** is the time at which this particular version of the Infrastructure was last modified vii. **name** must contain the name or characterizing text used to identify the Infrastructure viii. **infrastructure_types** is the type of infrastructure being described. The values for this property SHOULD come from the infrastructure-type-ov open vocabulary

3.8.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.8.2.

3.8.3.1 Infrastructure Test Case

A Producer must be able to create an Identity and Infrastructure objects as per the Producer requirements in Table x of section 2.17.2, such as the below content.

```
{
    "type": "identity",
    "name": "ACME Corp, Inc.",
    "identity_class": "organization",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "created": "2020-01-20T12:34:56.000Z",
    "modified": "2020-01-20T12:34:56.000Z",
    “created_by_ref”: "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "infrastructure",
    "spec_version": "2.1",
    "id": "infrastructure--38c47d93-d984-4fd9-b87b-d69d0841628d",
    "created": "2016-05-07T11:22:30.000Z",
    "modified": "2016-05-07T11:22:30.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "name": "Poison Ivy C2",
    "infrastructure_types": [ "command-and-control" ]
}
```

3.8.4 Producer Example Data

3.8.4.1 Vulnerabilities Discovered in Scans

An Infrastructure object can be used to capture vulnerabilities discovered in scans that are produced as a data feed. For example, a logical server or other infrastructure with multiple IP addresses or other means of identification can be captured as an Infrastructure object.

Consider the example feed data shown in Figure 3.

```
"ip": 1572395042,
"domains": ["example.com"],
"ip_str": "93.184.216.34",
```

```
...
"vulns": {
    "CVE-1019-1234": {
        "verified": false,
        "references": [],
        "summary": ""
    }
},
```

Figure 3. Example feed data

This data can be captured in an Infrastructure object as shown below:

```
{
    "type": "identity",
    "spec_version": "2.1",
    "id": "identity--c00275a5-4423-46c6-bb79-235654096f8a",
    "created": "2019-02-15T13:29:42.904Z",
    "modified": "2019-09-19T20:21:59.961Z",
    "name": "Example Shodan Inferred Vulnerability",
    "identity_class": "organization",
    “created_by_ref”: "identity--c00275a5-4423-46c6-bb79-235654096f8a"
},
{
    "spec_version": "2.1",
    "type": "vulnerability",
    "id": "vulnerability--fa4ca8dd-1248-5fef-8828-1bd2d935fa58",
    "created": "2019-07-22T12:34:02.602Z",
    "modified": "2019-07-22T12:34:02.602Z",
    "created_by_ref": "identity--c00275a5-4423-46c6-bb79-235654096f8a",
    "name": "CVE-2019-1234",
    "external_references": [
        {
            "source_name": "cve",
            "external_id": "CVE-2019-1234",
            "url": "https://nvd.nist.gov/vuln/detail/CVE-1019-1234"
        }
    ]
},
{
    "type": "infrastructure",
    "spec_version": "2.1",
    "id": "infrastructure--a927d4b3-3396-5c01-998b-08733784ab5e",
    "created": "2019-07-22T12:34:02.602Z",
    "modified": "2019-07-22T12:34:02.602Z",
    "created_by_ref": "identity--c00275a5-4423-46c6-bb79-235654096f8a",
    "name": "93.184.216.34",
    "infrastructure_types": ["exfiltration"]
},
{
    "type": "ipv4-addr",
    "id": "ipv4-addr--a927d4b3-3396-5c01-998b-08733784ab5e",
    "spec_version": "2.1",
```



```
    "value": "93.184.216.34"
},
{
    "type": "domain-name",
    "id": "domain-name--98e751b4-e47f-56f1-9d5d-f60001e5ac84",
    "spec_version": "2.1",
    "value": "example.com"
},
{
    "spec_version": "2.1",
    "type": "relationship",
    "id": "relationship--a502bd26-42d1-4020-b652-70ec37797cb6",
    "created": "2019-07-22T12:34:02.602Z",
    "modified": "2019-07-22T12:34:02.602Z",
    "created_by_ref": "identity--c00275a5-4423-46c6-bb79-235654096f8a",
    "relationship_type": "has",
    "source_ref": "infrastructure--a927d4b3-3396-5c01-998b-08733784ab5e",
    "target_ref": "vulnerability--fa4ca8dd-1248-5fef-8828-1bd2d935fa58"
},
{
    "spec_version": "2.1",
    "type": "relationship",
    "id": "relationship--91420849-09b2-4ba4-8769-30d258749ae8",
    "created": "2019-07-22T12:34:02.602Z",
    "modified": "2019-07-22T12:34:02.602Z",
    "created_by_ref": "identity--c00275a5-4423-46c6-bb79-235654096f8a",
    "relationship_type": "consists-of",
    "source_ref": "infrastructure--a927d4b3-3396-5c01-998b-08733784ab5e",
    "target_ref": "ipv4-addr--a927d4b3-3396-5c01-998b-08733784ab5e"
},
{
    "spec_version": "2.1",
    "type": "relationship",
    "id": "relationship--8371387d-2e54-443a-8aec-99e763e1a0d8",
    "created": "2019-07-22T12:34:02.602Z",
    "modified": "2019-07-22T12:34:02.602Z",
    "created_by_ref": "identity--c00275a5-4423-46c6-bb79-235654096f8a",
    "relationship_type": "resolves-to",
    "source_ref": "domain-name--98e751b4-e47f-56f1-9d5d-f60001e5ac84",
    "target_ref": "ipv4-addr--a927d4b3-3396-5c01-998b-08733784ab5e"
}
```

3.8.4.2 Botnet Infrastructure

Information gathered from monitoring botnets (e.g., network resources, malware delivered) can be captured in an Infrastructure object. An example is given below.

```
{
    "type": "identity",
    "spec_version": "2.1",
    "id": "identity--93607fcf-a0cc-572f-bcc6-92082f856b37",
    "created": "2017-02-15T13:29:42.904Z",
    "modified": "2017-02-15T13:29:42.904Z",
```



```
    "name": "HelloInteropWorld Inc.",
    "identity_class": "organization",
    “created_by_ref”: "identity--93607fcf-a0cc-572f-bcc6-92082f856b37"
},
{
    "spec_version": "2.1",
    "type": "infrastructure",
    "id": "infrastructure--bb054b70-d97e-5451-aa68-e31c72c791d1",
    "created": "2019-11-10T10:01:15.000Z",
    "modified": "2019-11-10T10:01:15.000Z",
    "created_by": "identity--93607fcf-a0cc-572f-bcc6-92082f856b37",
    "infrastructure_types": [ "c2" ],
    "name": "c2--https://corpcougar.com/mexzi/Panel/five/fre.php"
},
{
    "spec_version": "2.1",
    "type": "malware",
    "id": "malware--77362faf-ac50-5479-a9ec-d70dfc830850",
    "created": "2018-10-18T09:26:03.235Z",
    "modified": "2019-02-11T01:46:23.000Z",
    "created_by": "identity--93607fcf-a0cc-572f-bcc6-92082f856b37",
    "name": "LOKIBOT",
    "is_family": true,
    "malware_types": ["bot"],
    "external_references": [
        {
            "source_name": "FireEye",
            "external_id": "17-00005991",
            "description": "LokiBot Malware Overview"
        }
    ]
},
{
    "spec_version": "2.1",
    "type": "url",
    "id": "url--7c9374bc-0ccf-511d-a8f2-0af7965fe06e",
    "value": "https://corpcougar.com/mexzi/Panel/five/fre.php"
},
{
    "spec_version": "2.1",
    "type": "indicator",
    "id": "indicator--2b254bc2-5da2-56c0-9e24-d19342934f63",
    "created": "2019-11-11T10:01:15.000Z",
    "modified": "2019-11-11T10:01:15.000Z",
    "created_by": "identity--93607fcf-a0cc-572f-bcc6-92082f856b37",
    "infrastructure_type": "malicious-activity",
    "pattern_type": "stix",
    "pattern": "[url:value='https://corpcougar.com/mexzi/Panel/five/fre.php']",
    "valid_from": "2019-11-16T10:00:57.147Z",
    "valid_until": "2019-11-23T10:00:57.000Z"
},
{
    "spec_version": "2.1",
```

```
    "type": "relationship",
    "id": "relationship--445ba3b4-1e46-48cd-9e31-3491894373b5",
    "created": "2019-11-16T10:01:15.001Z",
    "modified": "2019-11-16T10:01:15.001Z",
    "created_by": "identity--93607fcf-a0cc-572f-bcc6-92082f856b37",
    "relationship_type": "delivers",
    "target_ref": "infrastructure--bb054b70-d97e-5451-aa68-e31c72c791d1",
    "source_ref": "malware--77362faf-ac50-5479-a9ec-d70dfc830850"
},
{
    "spec_version": "2.1",
    "type": "relationship",
    "id": "relationship--13d8a9d0-d968-446d-b9e3-9f18b208ebbb",
    "created": "2019-11-16T10:01:15.002Z",
    "modified": "2019-11-16T10:01:15.002Z",
    "created_by": "identity--93607fcf-a0cc-572f-bcc6-92082f856b37",
    "relationship_type": "indicates",
    "source_ref": "indicator--2b254bc2-5da2-56c0-9e24-d19342934f63",
    "target_ref": "infrastructure--bb054b70-d97e-5451-aa68-e31c72c791d1"
},
{
    "spec_version": "2.1",
    "type": "relationship",
    "id": "relationship--1f6bd9159-0548-4ea0-8c4e-e20f20b994c7",
    "created": "2019-11-16T10:01:15.005Z",
    "modified": "2019-11-16T10:01:15.005Z",
    "created_by": "identity--93607fcf-a0cc-572f-bcc6-92082f856b37",
    "relationship_type": "consists-of",
    "source_ref": "infrastructure--bb054b70-d97e-5451-aa68-e31c72c791d1",
    "target_ref": "url--7c9374bc-0ccf-511d-a8f2-0af7965fe06e"
}
```

3.8.5 Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Infrastructure object. Additional required Consumer support for Infrastructure is listed in the table below.

*Table 17 - Required Consumer Support for **Infrastructure***

Personas	Behavior
All Infrastructure Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more Infrastructure objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each Infrastructure object, the Consumer can process the information about the Infrastructure fields to the user 4. For each Infrastructure object, the Consumer can process any related SDOs/SROs and associated fields

3.8.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the Infrastructure Producer Test Case Data, as per the requirements in section 3.8.5.

3.9 Intrusion Set Sharing

An Intrusion Set is a grouped set of adversarial behaviors and resources with common properties that is believed to be orchestrated by a single organization. An Intrusion Set may capture multiple Campaigns or other activities that are all tied together by shared attributes indicating a commonly known or unknown Threat Actor. New activity can be attributed to an Intrusion Set even if the Threat Actors behind the attack are not known. Threat Actors can move from supporting one Intrusion Set to supporting another, or they may support multiple Intrusion Sets.

3.9.1 Description

Where a Campaign is a set of attacks over a period of time against a specific set of targets to achieve some objective, an Intrusion Set is the entire attack package and may be used over a very long period of time in multiple Campaigns to achieve potentially multiple purposes.

While sometimes an Intrusion Set is not active, or changes focus, it is usually difficult to know if it has truly disappeared or ended. Analysts may have varying levels of fidelity on attributing an Intrusion Set back to Threat Actors and may be able to only attribute it back to a nation state or perhaps back to an organization within that nation state.

3.9.2 Required Producer Persona Support

The Producer Persona must be able to create STIX content with one or more Intrusion Set objects.

Table 18 - Required Producer Support for Intrusion Set

Personas	Behavior

All Intrusion Set Producer personas	1. Producer allows a user to select or specify the STIX content to send to a Consumer persona 2. The following data must be provided by the persona: a. The Identity object must comply with the Identity object referenced in section 2.3.4 b. The Intrusion Set object must conform to the Intrusion Set specification as per section 4.9 of the STIX 2.1 OASIS Standard; specifically, these properties must be provided: i. **type** must be 'intrusion-set' ii. **spec_version** must be '2.1' iii. **id** must uniquely identify the Intrusion Set, and must be a UUID prepended with 'intrusion-set--' iv. **created_by_ref** must point to the Identity of the Producer v. **created** must match the timestamp, to millisecond granularity, of when the Intrusion Set was originally created vi. **modified** must match the timestamp, to millisecond granularity, of when this particular version of the Intrusion Set was last modified vii. **name** is populated with the name of the Intrusion Set viii. **resource_level** specifies the organizational level at which this Intrusion Set typically works, which in turn determines the resources available to this Intrusion Set for use in an attack. The value for this property SHOULD come from the attack-resource-level-ov open vocabulary ix. **primary_motivation** is the primary reason, motivation, or purpose behind this Intrusion Set. The motivation is why the Intrusion Set wishes to achieve the goal (what they are trying to achieve). The value for this property SHOULD come from the attack-motivation-ov open vocabulary

3.9.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.9.2.

3.9.3.1 Intrusion Set Test Case

A Producer must be able to create an Identity and Intrusion Set objects, such as the below content.

```
{
    "type": "identity",
    "name": "ACME Corp, Inc.",
    "identity_class": "organization",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "created": "2020-01-20T12:34:56.000Z",
    "modified": "2020-01-20T12:34:56.000Z",
```



```
    “created_by_ref”: "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "intrusion-set",
    "spec_version": "2.1",
    "id": "intrusion-set--4e78f46f-a023-4e5f-bc24-71b3ca22ec29",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-04-06T20:03:48.000Z",
    "modified": "2016-04-06T20:03:48.000Z",
    "name": "Bobcat Breakin",
    “resource_level”: “organization”,
    “prinary_motivation”: “ideology”
}
```

3.9.4 Producer Example Data

3.9.4.1 Intrusion Set Owns Infrastructure

This example demonstrates a command-and-control server leveraged by a threat actor across an intrusion set.

```
{
    "type": "identity",
    "id": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "spec_version": "2.1",
    "created": "2015-04-14T13:07:49.812Z",
    "modified": "2015-04-14T13:07:49.812Z",
    "name": "Oscorp Industries",
    "identity_class": "organization"
},
{
    "type": "intrusion-set",
    "spec_version": "2.1",
    "id": "intrusion-set--4e78f46f-a023-4e5f-bc24-71b3ca22ec29",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2016-04-06T20:03:48.000Z",
    "modified": "2016-04-06T20:03:48.000Z",
    "name": "Bobcat Breakin",
    "description": "Incidents usually feature a shared TTP of a bobcat being released within
the building containing network access, scaring users to leave their computers without locking
them first. Still determining where the threat actors are getting the bobcats.",
},
{
    "type": "infrastructure",
    "spec_version": "2.1",
    "id": "infrastructure--e5268b6e-4931-42f1-b379-87f48eb41b1e",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2016-08-08T15:50:10.983Z",
    "modified": "2016-08-08T15:50:10.983Z",
    "name": "Bobcat Infrastructure",
    "description": "A C2 server for computers that were accessed after bobcats were
released.",
```



```
    "infrastructure_types": [ "command-and-control" ]
},
{
    "type": "ipv4-addr",
    "spec_version": "2.1",
    "id": "ipv4-addr--b4e29b62-2053-47c4-bab4-bbce39e5ed67",
    "value": "198.51.100.3"
},
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--a6e9345f-5a15-4c29-8bb3-7dcc5d168d64",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2020-02-29T17:41:44.940Z",
    "modified": "2020-02-29T17:41:44.940Z",
    "relationship_type": "owns",
    "source_ref": "intrusion-set--4e78f46f-a023-4e5f-bc24-71b3ca22ec29",
    "target_ref": "infrastructure--e5268b6e-4931-42f1-b379-87f48eb41b1e"
},
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--7aebe2f0-28d6-48a2-9c3e-b0aaa60266ef",
    "created": "2016-09-09T08:17:27.000Z",
    "modified": "2016-09-09T08:17:27.000Z",
    "relationship_type": "consists-of",
    "source_ref": "infrastructure--e5268b6e-4931-42f1-b379-87f48eb41b1e",
    "target_ref": "ipv4-addr--b4e29b62-2053-47c4-bab4-bbce39e5ed67"
}
```

3.9.4.2 Intrusion Set Originates from Location

This example shows how an intrusion set can be associated with a specific location in the world.

```
{
    "type": "identity",
    "id": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "spec_version": "2.1",
    "created": "2015-04-14T13:07:49.812Z",
    "modified": "2015-04-14T13:07:49.812Z",
    "name": "Oscorp Industries",
    "identity_class": "organization"
},
{
    "type": "intrusion-set",
    "spec_version": "2.1",
    "id": "intrusion-set--4e78f46f-a023-4e5f-bc24-71b3ca22ec29",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2016-04-06T20:03:48.000Z",
    "modified": "2016-04-06T20:03:48.000Z",
    "name": "Bobcat Breakin",
```



```
    "description": "Incidents usually feature a shared TTP of a bobcat being released within
the building containing network access, scaring users to leave their computers without locking
them first. Still determining where the threat actors are getting the bobcats."
},
{
    "type": "location",
    "spec_version": "2.1",
    "id": "location--a6e9345f-5a15-4c29-8bb3-7dcc5d168d64",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2016-04-06T20:03:00.000Z",
    "modified": "2016-04-06T20:03:00.000Z",
    "region": "northern-america"
},
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--a6e9345f-5a15-4c29-8bb3-7dcc5d168d64",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2020-02-29T17:41:44.940Z",
    "modified": "2020-02-29T17:41:44.940Z",
    "relationship_type": "originates-from",
    "source_ref": "intrusion-set--4e78f46f-a023-4e5f-bc24-71b3ca22ec29",
    "target_ref": "location--a6e9345f-5a15-4c29-8bb3-7dcc5d168d64"
}
```


3.9.5 Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Intrusion Set object. Additional required Consumer support for Intrusion Sets is listed in the table below.

Table 19 - Required Consumer Support for Intrusion Set

Persona	Behavior
All Intrusion Set Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more Intrusion Set objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each Intrusion Set object, the Consumer can process the information about the Intrusion Set fields to the user 4. For each Intrusion Set object, the Consumer can process any related SDOs/SROs and associated fields

3.9.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the Intrusion Set Producer Test Case Data, as per the requirements in section 3.9.5.

3.10 Location Sharing

A STIX 2.1 Location object represents a geographic location. The location may be described as any, some, or all of the following: region, country, civic address (e.g. New York, US), latitude and longitude.

3.10.1 Description

Locations are primarily used to give context or enrichment to other SDOs. For example, a Location object can be used in a relationship to describe that an Intrusion Set originates from a certain country. A Location object can also be related to a Malware or Attack Pattern to indicate that one and/or the other targets victims in that location.

3.10.2 Required Producer Persona Support

The Producer persona must be able to create STIX content with one or more Locations.

Table 20 - Required Producer Support for Location

Persona	Behavior
All Location Producer personas	1. Producer allows a user to select or specify the STIX content to create and send to a Consumer persona 2. The following data must be provided by the persona: a. The Identity object must comply with the Identity object referenced in section 2.3.4 b. The Location object must conform to the Location specification as per section 4.10 of the STIX 2.1 OASIS Standard; specifically, these properties must be provided: i. **type** must be 'location' ii. **spec_version** must be '2.1' iii. **id** must uniquely identify the Location, and must be a UUID prepended with 'location--' iv. **created_by_ref** must point to the Identity of the Producer v. **created** must match the timestamp, to millisecond granularity, of when the Producer created the Location object vi. **modified** must match the timestamp, to millisecond granularity, of when this particular version of the Location was last modified vii. **region** is the region that this Location describes. The value for this property SHOULD come from the region-ov open vocabulary

3.10.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.10.2.

3.10.3.1 Producing a Location Object

```
{
```



```
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2016-01-17T11:11:13.000Z",
    "modified": "2016-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "location",
    "spec_version": "2.1",
    "id": "location--a6e9345f-5a15-4c29-8bb3-7dcc5d168d64",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-04-06T20:03:00.000Z",
    "modified": "2016-04-06T20:03:00.000Z",
    "region": "south-eastern-asia"
}
```

3.10.3.2 Location Hosting Infrastructure

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2016-01-17T11:11:13.000Z",
    "modified": "2016-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "location",
    "spec_version": "2.1",
    "id": "location--a6e9345f-5a15-4c29-8bb3-7dcc5d168d64",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-04-06T20:03:00.000Z",
    "modified": "2016-04-06T20:03:00.000Z",
    "region": "caribbean"
},
{
    “type”: “infrastructure”,
    “id”: "infrastructure--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-04-06T20:03:00.000Z",
    "modified": "2016-04-06T20:03:00.000Z",
    “name”: “Annoying Botnet”,
    “infrastructure_types”: [
        “botnet”
    ]
},
{
```



```
    “type”: “relationship”,
    “id”: "relationship--e827b109-377b-45e0-aa1c-6a4751cac7dd",
    "spec_version": "2.1",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-04-06T20:03:00.000Z",
    "modified": "2016-04-06T20:03:00.000Z",
    “source_ref”: “infrastructure--f431f809-377b-45e0-aa1c-6a4751cae5ff”,
    “target_ref”: “location--a6e9345f-5a15-4c29-8bb3-7dcc5d168d64”,
    “relationship_type”: “located-at”
}
```

3.10.4 Producer Example Data

3.10.4.1 Threat Actor Location

The location of a threat actor can be captured with a relationship between a Location object and the corresponding Threat Actor SDO. Locations of Identity and Infrastructure SDOs could be captured similarly.

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2016-01-17T11:11:13.000Z",
    "modified": "2016-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "location",
    "spec_version": "2.1",
    "id": "location--a6e9345f-5a15-4c29-8bb3-7dcc5d168d64",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-04-06T20:03:00.000Z",
    "modified": "2016-04-06T20:03:00.000Z",
    "region": "south-eastern-asia",
    "country": "TH"
},
{
    "type": "threat-actor",
    "spec_version": "2.1",
    "id": "threat-actor--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",
    "threat_actor_types": [ "crime-syndicate" ],
    "name": "Evil Org"
},
{
    "type": "relationship",
    "spec_version": "2.1",
```



```
    "id": "relationship--014841f8-eb38-4673-9904-70f67c92dd8b",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-04-06T20:08:00.000Z",
    "modified": "2016-04-06T20:08:00.000Z",
    "relationship_type": "targets",
    "source_ref": "threat-actor--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "target_ref": "location--a6e9345f-5a15-4c29-8bb3-7dcc5d168d64"
}
```

3.10.4.2 Malware Originates from Location

The location that malware originates can be captured with a relationship between a Location object and the corresponding Malware SDO. Origination locations of Intrusion Set and Campaign SDOs could be captured similarly.

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2016-01-17T11:11:13.000Z",
    "modified": "2016-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "location",
    "spec_version": "2.1",
    "id": "location--a6e9345f-5a15-4c29-8bb3-7dcc5d168d64",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-04-06T06:03:00.000Z",
    "modified": "2016-04-06T06:03:00.000Z",
    "country": "CN"
},
{
    "type": "malware",
    "spec_version": "2.1",
    "id": "malware--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-05-12T08:17:27.000Z",
    "modified": "2016-05-12T08:17:27.000Z",
    "name": "UglyRAT",
    "malware_types": ["rootkit"],
    "is_family": false
},
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--014841f8-eb38-4673-9904-70f67c92dd8b",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-05-12T08:20:27.000Z",
    "modified": "2016-05-12T08:20:27.000Z",
    "relationship_type": "originates-from",
```



```
    "source_ref": "malware--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
    "target_ref": "location--a6e9345f-5a15-4c29-8bb3-7dcc5d168d64"
}
```

3.10.4.3 Campaign Targets Location

The location that a campaign targets can be captured with a relationship between a Location object and the corresponding Campaign SDO. Locations targeted by Attack Pattern, Intrusion Set, Malware, Threat Actor, and Tool SDOs could be captured similarly.

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2016-01-17T11:11:13.000Z",
    "modified": "2016-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "location",
    "spec_version": "2.1",
    "id": "location--b222345f-5a15-4c29-8bb3-7dcc5d168d64",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-04-06T06:03:00.000Z",
    "modified": "2016-04-06T06:03:00.000Z",
    "country": "US"
},
{
    "type": "campaign",
    "spec_version": "2.1",
    "id": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-05-12T08:17:27.000Z",
    "modified": "2016-05-12T08:17:27.000Z",
    "name": "Blue Attacks Against Farmers"
},
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--014841f8-eb38-4673-9904-70f67c92dd8b",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-05-12T08:20:27.000Z",
    "modified": "2016-05-12T08:20:27.000Z",
    "relationship_type": "targets",
    "source_ref": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "target_ref": "location--b222345f-5a15-4c29-8bb3-7dcc5d168d64"
}
```


3.10.5 Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Location object. Additional required Consumer support for Locations is listed in the table below.

When a combination of properties is provided (e.g. a region and a latitude & longitude) the more precise properties are what the location describes.

Table 21 - Required Consumer Support for Location

Persona	Behavior
All Location Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more Location objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each Location object, the Consumer can process the information about the Location fields to the user 4. For each Location object, the Consumer can process any related SDOs/SROs and associated fields

3.10.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the Location Producer Test Case Data, as per the requirements in section 3.10.5.

3.10.7 Consumer Example Data

Possible examples are described below, to provide potential uses of the Location object.

3.10.7.1 Map a Location

The Consumer could visualize a Location object by parsing it and generating a URL depicting that location . For example, consider the STIX 2.1 content:

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "location",
    "spec_version": "2.1",
    "id": "location--8db2245f-5a15-723d-8bb3-7dcc5d1600cc",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2020-01-16T21:00:00.000Z",
```



```
    "modified": "2020-02-01T08:05:00.000Z",
    "latitude": "33.8567944",
    "longitude": "151.2152967"
}
```

Processing the STIX content results in the following URL and the map shown in Figure 4:

https://www.google.com/maps/search/?api=1&query=-33.8567844%2C151.2152967

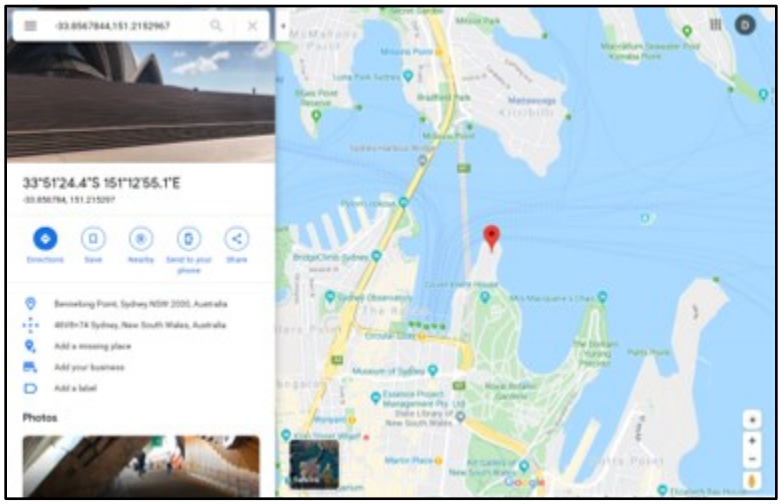

Figure 4. Example Location object visualization

3.11 Malware Analysis Sharing

Malware Analysis captures the metadata and results of a particular static or dynamic analysis performed on a malware instance or family.

3.11.1 Description

Malware Analysis may include captured SCOs.

3.11.2 Required Producer Persona Support

The Producer Persona must be able to create STIX content with one or more Malware Analysis objects.

Table 22 - Required Producer Support for Malware Analysis

Personas	Behavior

All Malware Analysis Producer personas	1. Producer allows a user to select or specify the STIX content to send to a Consumer persona 2. The following data must be provided by the persona: a. The Identity object must comply with the Identity object referenced in section 2.3.4 b. The Malware Analysis object must conform to the Malware Analysis specification as per section 4.12 of the STIX 2.1 OASIS Standard; specifically, these properties must be provided: i. **type** must be 'malware-analysis' ii. **spec_version** must be '2.1' iii. **id** must uniquely identify the Malware Analysis, and must be a UUID prepended with 'malware-analysis--' iv. **created_by_ref** must point to the Identity of the Producer v. **created** must match the timestamp, to millisecond granularity, of when the Malware Analysis was originally created vi. **modified** must match the timestamp, to millisecond granularity, of when this particular version of the Malware Analysis was last modified vii. **product** is the name of the analysis engine or product that was used. Product names SHOULD be all lowercase with words separated by a dash "-". For cases where the name of a product cannot be specified, a value of "anonymized" MUST be used viii. **version** is the version of the analysis product that was used to perform the analysis ix. **submitted** is the date and time that the malware was first submitted for scanning or analysis. This value will stay constant while the scanned date can change x. **analysis_started** is the date and time that the malware analysis was initiated xi. **analysis_ended** is the date and time that the malware analysis was ended xii. **result** (the classification result as determined by the scanner or tool analysis process)

3.11.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.11.2.

3.11.3.1 Malware Analysis without References

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



```
    "spec_version": "2.1",
    "created": "2018-01-20T12:34:56.000Z",
    "modified": "2018-01-20T12:34:56.000Z",
    “created_by_ref”: "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "malware-analysis",
    "spec_version": "2.1",
    "id": "malware-analysis--d25167b7-fed0-4068-9ccd-a73dd2c5b07c",
    "created": "2020-01-16T18:52:24.277Z",
    "modified": "2020-01-16T18:52:24.277Z",
    “created_by_ref”: “identity--f431f809-377b-45e0-aa1c-6a4751cae5ff”,
    "product": "microsoft",
    "version": "5.1.0",
    "submitted": "2020-01-15T18:52:24.277Z",
    "analysis_started": "2020-01-11T08:36:14Z",
    "analysis_ended": "2020-01-11T08:36:14Z",
    "result": "malicious"
}
```

3.11.4 Producer Example Data

3.11.4.1 Malware Analysis with a Reference

```
{
    "type": "identity",
    "name": "ACME Corp, Inc.",
    "identity_class": "organization",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "created": "2018-01-20T12:34:56.000Z",
    "modified": "2018-01-20T12:34:56.000Z",
    “created_by_ref”: "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "malware-analysis",
    "spec_version": "2.1",
    "id": "malware-analysis--d25167b7-fed0-4068-9ccd-a73dd2c5b07c",
    "created": "2020-01-16T18:52:24.277Z",
    "modified": "2020-01-16T18:52:24.277Z",
    “created_by_ref”: “identity--f431f809-377b-45e0-aa1c-6a4751cae5ff”,
    "product": "microsoft",
    "analysis_engine_version": "5.1.0",
    "analysis_definition_version": "053514-0062",
    "analysis_started": "2020-01-11T08:36:14Z",
    "analysis_ended": "2020-01-11T08:36:14Z",
    "result": "malicious",
    "analysis_sco_refs": [ "file--1190f2c9-166f-55f1-9706-eea3971d8082" ],
},
{
    "type": "file",
    "id": "file--1190f2c9-166f-55f1-9706-eea3971d8082",
    "spec_version": "2.1",
```



```
    "size": 77312,
    "name": "a92e5b2bae.exe"
}
```

3.11.4.2 Malware Analysis of Malware

One major use case associated with Malware Analysis is characterizing a piece of malware to better understand how it operates. In this example, a piece of malware is analyzed and the hashes of the associated file are determined.

```
{
    "type": "identity",
    "id": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "spec_version": "2.1",
    "created": "2017-04-14T13:07:49.812Z",
    "modified": "2017-04-14T13:07:49.812Z",
    "name": "Oscorp Industries",
    "identity_class": "organization",
    "contact_information": "norman@oscorp.com",
    "sectors": [
        "technology"
    ]
},
{
    "type": "malware",
    "spec_version": "2.1",
    "id": "malware--8bcf14e9-2ba2-44ef-9e32-fbbc9d2608b2",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2020-01-16T18:52:24.277Z",
    "modified": "2020-01-16T18:52:24.277Z",
    "name": "a92e5b2bae.exe",
    "malware_types": [
        "unknown"
    ],
    "is_family": false,
    "sample_refs": [ "file--1190f2c9-166f-55f1-9706-eea3971d8082" ]
},
{
    "type": "malware-analysis",
    "spec_version": "2.1",
    "id": "malware-analysis--b67d30ff-02ac-498a-92f9-32f845f448cf",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2020-01-16T18:52:24.277Z",
    "modified": "2020-01-16T18:52:24.277Z",
    "product": "microsoft",
    "analysis_engine_version": "5.1.0",
    "analysis_definition_version": "053514-0062",
    "analysis_started": "2012-02-11T08:36:14Z",
    "analysis_ended": "2012-02-11T08:36:14Z",
    "result": "malicious",
    "analysis_sco_refs": [
        "file--1190f2c9-166f-55f1-9706-eea3971d8082",
        "directory--255cb0e4-8bdb-5d63-bb32-9c6f0b733ab2"
```



```
    ],
    "sample_ref": "file--1190f2c9-166f-55f1-9706-eea3971d8082"
},
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--014841f8-eb38-4673-9904-70f67c92dd8b",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2020-01-16T18:52:24.277Z",
    "modified": "2020-01-16T18:52:24.277Z",
    "relationship_type": "analysis-of",
    "source_ref": "malware-analysis--d25167b7-fed0-4068-9ccd-a73dd2c5b07c",
    "target_ref": "malware--8bcf14e9-2ba2-44ef-9e32-fbbc9d2608b2"
},
{
    "type": "file",
    "id": "file--1190f2c9-166f-55f1-9706-eea3971d8082",
    "spec_version": "2.1",
    "hashes": {
        "MD5": "a92e5b2bae0b4b3a3d81c85610b95cd4",
        "SHA-1": "5374e08903744ceeaedd8f5e1bfc06b2c4688e76"
    },
    "size": 77312,
    "name": "a92e5b2bae.exe",
    "parent_directory_ref": "directory--255cb0e4-8bdb-5d63-bb32-9c6f0b733ab2"
},
{
    "type": "directory",
    "id": "directory--255cb0e4-8bdb-5d63-bb32-9c6f0b733ab2",
    "spec_version": "2.1",
    "path": "C:\\"
}
```

3.11.5 Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Malware Analysis object. Additional required Consumer support for Malware Analysis is listed in the table below.

Table 23 - Required Consumer Support for Malware Analysis

Persona	Behavior
All Malware Analysis Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more Malware Analysis objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each Malware Analysis object, the Consumer can process the information about the Malware Analysis fields to the user

	4. For each Malware Analysis object, the Consumer can process any related SDOs/SROs and associated fields

3.11.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the Malware Analysis Producer Test Case Data, as per the requirements in section 3.11.5.

3.12 Malware Sharing

Tactics, techniques, and procedures (TTPs) describe behaviors and resources that attackers use to carry out their attacks. Malware objects are one of three types of TTPs discussed in this document (Attack Patterns is another and is discussed in section 3.1, along with Infrastructure which is discussed in section 3.8).

3.12.1 Description

Malware is a type of TTP that represents malicious code; it generally refers to a program that is inserted into a system, usually covertly. The intent of malware is to compromise the confidentiality, integrity, and/or availability of the victim's data, applications, or operating system, or to otherwise annoy or disrupt the victim.

The Malware object characterizes, identifies, and categorizes malware instances and families using data derived from analysis. The information captured may provide context to other SDOs. Fuller analysis can be captured by the Malware Analysis SDO; however the Malware object may be used on its own.

3.12.2 Required Producer Persona Support

Table 24 - Required Producer Support for Malware

Personas	Behavior
All Malware Producer personas	1. Producer allows a user to select or specify the STIX content to send to a Consumer persona 2. The following data must be provided by the persona: a. The Identity object must comply with the Identity object referenced in section 2.3.4 b. The Malware object must conform to the Malware specification as per section 4.11 of the STIX 2.1 OASIS Standard; specifically, these properties must be provided: i. **type** must be 'malware' ii. **spec_version** must be '2.1' iii. **id** must uniquely identify the Malware, and must be a UUID prepended with 'malware' iv. **created_by_ref** must point to the Identity of the Producer; v. **created** must match the timestamp, to millisecond granularity, of when the user created the Malware vi. **is_family** must contain a boolean value reflecting whether the malware represents an instance (`false`) or a family (`true`) vii. **name** that identifies the Malware instance or family viii. **malware_types** lists the categorizations for the malware being

	described. Values **SHOULD** come from the malware-type-ov open vocabulary ix. **capabilities** is a list of the capabilities identified for the malware instance or family. Values **SHOULD** come from the malware-capabilities-ov open vocabulary x. **first_seen** is the time that the malware instance or family was first seen xi. **last_seen** is the time that the malware instance or family was last seen xii. **implementation_languages** are the programming language(s) used to implement the malware instance or family. The values for this property SHOULD come from the implementation-language-ov open vocabulary xiii. **architecture_execution_envs** is the processor architectures (e.g., x86, ARM, etc.) that the malware instance or family is executable on. The values for this property SHOULD come from the processor-architecture-ov open vocabulary

3.12.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.12.2.

3.12.3.1 Create Malware Object

A Producer must be able to create a Malware object, generating content such as the following content.

```
{
    "type": "identity",
    "id": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "XYZA Corp, Inc.",
    "created": "2017-01-17T11:11:13.000Z",
    "modified": "2017-01-17T11:11:13.000Z",
    “created_by_ref”: “identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5”
},
{
    "type": "malware",
    "spec_version": "2.1",
    "id": "malware--1121ffbc-364f-857a-9987-92fbcff24ab",
    "created": "2019-05-12T08:17:27.000Z",
    "modified": "2019-05-12T08:17:27.000Z",
    “created_by_ref”: "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "name": "Cryptolocker",
    "malware_types": ["ransomware"],
    "is_family": false,
    “capabilities”: [ “anti-vm” ],
    “first_seen”: “2017-01-18T11:11:13.000Z”,
    “last_seen”: “2017-01-18T11:11:13.000Z”,
    “implementation_langauges”: [ “python”, “c”],
    “architecture_execution_envs”: [ “mips”, “x86” ]
}
```

3.12.4 Producer Example Data

3.12.4.1 Provide Actionable Intelligence Data via Threat Feed

A Producer may create content—SDO and associated SROs—which can be made available for query by Consumers (e.g,. via an Intelligence Platform API), enabling Consumers to access actionable threat intelligence.

The Malware object provides detailed information about how the malware works and what it does. However, it is purposely minimalistic, allowing Consumers to pivot and correlate associated cyber threat intelligence (related objects often contain the bulk of the actionable intelligence). For example, the Producer should be able to produce the following content:

```
{
    "type": "identity",
    "id": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "XYZA Corp, Inc.",
    "created": "2017-01-17T11:11:13.000Z",
    "modified": "2017-01-17T11:11:13.000Z",
    “created_by_ref”: "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5"
},
{
    "type": "malware",
    "spec_version": "2.1",
    "id": "malware--417757e7-01f9-5464-bf88-6fda0644d1e9",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "created": "2018-08-18T23:55:56.000Z",
    "modified": "2018-09-03T05:38:32.000Z",
    "name": "zeus",
    "malware_types": [ "password-stealer" ],
    "is_family": true
},
{
    "type": "relationship",
    "spec_version": "2.1"
    "id": "relationship--404b4404-8461-55e3-a6e5-1b685b98bdcd",
    "created": "2018-08-31T00:32:04.000Z",
    "modified": "2018-08-31T00:32:04.000Z",
    “created_by_ref”: “identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5”,
    "relationship_type": "indicates",
    "source_ref": "indicator--63863f0b-44ed-5ec4-8b7c-1bba50a8ae0e",
    "target_ref": "malware--417757e7-01f9-5464-bf88-6fda0644d1e9",
},
{
    "type": "relationship",
    "spec_version": "2.1"
    "id": "relationship--73339fd6-b3f5-5876-af09-d4ba3c75345a",
    "created": "2018-08-29T08:25:26.000Z",
    "modified": "2018-08-29T08:25:26.000Z",
    “created_by_ref”: “identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5”,
    "relationship_type": "communicates-with",
```



```
    "source_ref": "malware--417757e7-01f9-5464-bf88-6fda0644d1e9",
    "target_ref": "url--76820a5f-a2d4-56b8-ae2d-16334b195b19",
},
{
    "type": "relationship",
    "spec_version": "2.1"
    "id": "relationship--f88d31f6-486f-44da-b317-01333bde0b82",
    "created": "2018-08-31T00:32:04.000Z",
    "modified": "2018-08-31T00:32:04.000Z",
    “created_by_ref”: “identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5”,
    "relationship_type": "communicates-with",
    "source_ref": "malware--417757e7-01f9-5464-bf88-6fda0644d1e9",
    "target_ref": "ipv4-addr--c9f929f7-21e4-5fa1-8d55-b4d739f451fb",
},
{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--63863f0b-44ed-5ec4-8b7c-1bba50a8ae0e",
    "created": "2018-08-15T05:12:40.000Z",
    "modified": "2018-08-15T05:12:40.000Z",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "indicator_types": ["malicious-activity"],
    "pattern": "[ipv4-addr:value='113.11.194.167']",
    "pattern_type": "stix",
    "valid_from": "2018-08-15T05:12:40.000Z",
    "valid_until": "2019-01-14T00:12:22.000Z",
},
{
    "type": "url",
    "spec_version": "2.1"
    "id": "url--76820a5f-a2d4-56b8-ae2d-16334b195b19",
    "description": "Zeus controllers",
    "created": "2018-08-29T08:25:26.000Z",
    "modified": "2018-08-29T08:25:26.000Z",
    "value": "http://xiaofamily.instantfreesite.com/update.bin"
},
{
    "type": "ipv4-addr",
    "spec_version": "2.1"
    "id": "ipv4-addr--c9f929f7-21e4-5fa1-8d55-b4d739f451fb",
    "created": "2018-08-29T08:25:29.000Z",
    "modified": "2018-08-29T08:25:29.000Z",
    "value": "216.59.18.11"
}
```

3.12.5 Required Consumer Persona

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Malware object. Additional required Consumer support for Malware is listed in the table below.

Table 25 - Required Consumer Support for Malware

Personas	Behavior

All Malware Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more Malware objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each Malware object, the Consumer can process the information about the Malware fields to the user 4. For each Malware object, the Consumer can process any related SDOs/SROs and associated fields

3.12.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the Malware Producer Test Case Data, as per the requirements in section 3.12.5.

3.12.7 Consumer Example Data

The Consumer must be able to parse and display fields of Malware objects received, such as the example content shown in Sections 2.13.3.1 and 2.13.3.2. No data is sent from the Consumer back to the Producer. A possible use case is described below.

3.12.7.1 Ingest Threat Intelligence Data

The Responder queries a Producer's threat intelligence data center (see Figure 5) and ingests Malware object data into its threat intelligence platform, demonstrating the value of the SDOs and SROs through visualization. The representation would include the Malware object, as well as multiple associated relationships to other SDOs, such as Malware Analysis objects and Attack Pattern objects.

Figure 5. Query Malware Object

3.13 Note Sharing

STIX Note objects can be used to enrich STIX Objects with additional information (e.g., intelligence, comments, etc.) that may not be directly expressible in the STIX object. For example, an analyst may observe an Indicator, but also notice additional context around it that would be useful to others, which can be shared with partnering organizations.

3.13.1 Description

In STIX 2.1, a Note object conveys informative text that provides further context and analysis not contained in the STIX object or STIX relationship that it relates to. The Note object consists of several fields including **content** and **object_refs**. An analyst could, via a SIEM, enrich the Sighting of a particular Indicator by combining a Note with the original Sighting and Indicator objects, into a STIX Bundle. This Bundle could then be published to a TIP.

3.13.2 Required Producer Persona Support

Table 26 - Required Producer Support for Note

Persona	Behavior
All Note Producer personas	1. Producer allows a user to select or specify the STIX content to send to a Consumer persona 2. The following data must be provided by the persona: a. The Identity object must comply with the Identity object referenced in section 2.3.4 b. The Note object must conform to the Note specification as per section 4.13 of the STIX 2.1 OASIS Standard; specifically, these properties must be provided: i. **type** must be 'note' ii. **spec_version** must be '2.1' iii. **id** must uniquely identify the Note, and must be a UUID prepended with 'note--' iv. **created_by_ref** must point to the Identity of the Producer v. **created** must match the timestamp, to millisecond granularity, of when the user created the Note vi. **modified** must match the timestamp, to millisecond granularity, of when this particular version of the Note was last modified vii. **content** must convey the informative text that corresponds to the specified SROs/SDOs/SCOs viii. **object_refs** is a list containing the ID of each SRO/SDO/SCO referenced by this Note c. The object(s) referenced in the Note's **object_refs**. The object(s) must comply with the relevant section(s) of the STIX 2.1 OASIS Standard

3.13.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.13.2.

3.13.3.1 Note on Threat Actor

```
{
    "type": "identity",
    "id": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "spec_version": "2.1",
    "created": "2017-04-14T13:07:49.812Z",
    "modified": "2017-04-14T13:07:49.812Z",
    "name": "Oscorp Industries",
    "identity_class": "organization",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c"
},
{
    "type": "note",
    "spec_version": "2.1",
    "id": "note--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
    "created": "2016-05-12T08:17:27.000Z",
```



```
    "modified": "2016-05-12T08:17:27.000Z",
    “created_by_ref”: “987eeee1-413a-44ac-96cc-0a8acdcc2f2c”,
    "content": "This note indicates the various steps taken by the threat actor to instigate particular attacks. Step 1) Do a scan 2) Review scanned results for identified hosts not known by external intel…etc."
    "object_refs": ["threat-actor--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f"]
},
{
    "type": "threat-actor",
    "spec_version": "2.1",
    "id": "threat-actor--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2016-04-06T20:03:48.000Z",
    "modified": "2016-04-06T20:03:48.000Z",
    "threat_actor_types": [ "crime-syndicate"],
    "name": "Evil Org",
    "roles": ["director"],
    "sophistication": "advanced",
    "resource_level": "team",
    "primary_motivation": "organizational-gain"
}
```

3.13.4 Producer Example Data

3.13.4.1 Note on Sighting of Malware

```
{
    "type": "identity",
    "id": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "spec_version": "2.1",
    "created": "2017-04-14T13:07:49.812Z",
    "modified": "2017-04-14T13:07:49.812Z",
    "name": "Oscorp Industries",
    "identity_class": "organization",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c"
},
{
    "type": "identity",
    "id": "identity--7865b6d2-a4af-45c5-b582-afe5ec376c33",
    "spec_version": "2.1",
    "created": "2017-04-14T13:07:49.812Z",
    "modified": "2017-04-14T13:07:49.812Z",
    "name": "Pym Technologies",
    "identity_class": "organization",
    "created_by_ref": "identity--7865b6d2-a4af-45c5-b582-afe5ec376c33"
},
{
    "type": "malware",
    "id": "malware--ae560258-a5cb-4be8-8f05-013d6712295f",
    "spec_version": "2.1",
    "created_by_ref": "identity--7865b6d2-a4af-45c5-b582-afe5ec376c33",
    "created": "2014-02-20T09:16:08.989Z",
    "modified": "2014-02-20T09:16:08.989Z",
```



```
    "name": "Online Job Site Trojan",
    "description": "Trojan that is disguised as the executable file resume.pdf., it also
creates a registry key.",
    "malware_types": [
        "remote-access-trojan"
    ]
},
{
    "type": "sighting",
    "id": "sighting--779c4ae8-e134-4180-baa4-03141095d971",
    "spec_version": "2.1",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2017-02-28T19:37:11.213Z",
    "modified": "2017-02-28T19:37:11.213Z",
    "first_seen": "2017-02-28T19:07:24.856Z",
    "last_seen": "2017-02-28T19:07:24.856Z",
    "count": 1,
    "sighting_of_ref": "malware--ae560258-a5cb-4be8-8f05-013d6712295f"
},
{
    "type": "note",
    "id": "note--8db2245f-5a15-723d-8bb3-7dcc5d1600cc",
    "spec_version": "2.1",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2017-02-28T19:37:11.213Z",
    "modified": "2017-02-28T19:37:11.213Z",
    "content": "This is a high-priority sighting that needs to be investigated immediately by
threat analysis teams.",
    "object_refs": [
        "sighting--779c4ae8-e134-4180-baa4-03141095d971"
    ]
}
```

3.13.5 Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Note object. Additional required Consumer support for Notes is listed in the table below.

Table 27 - Required Consumer Support for Note

Persona	Behavior
All Note Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more Note objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each Note object, the Consumer can process the information about the Note fields to the user 4. For each Note object, the Consumer can process any related SDOs/SROs and associated fields

3.13.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the Note Producer Test Case Data, as per the requirements in section 3.13.5.

3.14 Observed Data Sharing

Observed Data can be used to capture raw information about cyber security related entities such as files, systems, and networks using the STIX Cyber-observable Objects (SCOs). Some examples include information about IP addresses, network connections, files, and registry keys which can be collected from analyst reports, sandboxes, and network and host-based detection tools.

3.14.1 Description

In STIX 2.1, an observed data object conveys raw information about cyber security related entities that can be combined with other information to create actionable threat intelligence.

3.14.2 Required Producer Persona Support

Table 28 - Required Producer Support for Observed Data

Personas	Behavior

All Observed Data Producer personas	1. Producer allows a user to select or specify the STIX content to send to a Consumer persona 2. The following data must be provided by the persona: a. The Identity object must comply with the Identity object referenced in section 2.3.4 b. The Observed Data object must conform to the Observed Data specification as per section 4.14 of the STIX 2.1 OASIS Standard; specifically, these properties must be provided: i. **type** must be 'observed-data' ii. **spec_version** must be '2.1' iii. **id** must uniquely identify the Observed Data, and must be a UUID prepended with 'observed-data--' iv. **created_by_ref** must point to the Identity of the Producer v. **created** must match the timestamp, to millisecond granularity, of when the Observed Data was originally created vi. **modified** must match the timestamp, to millisecond granularity, of when this particular version of the Observed Data was last modified vii. **first_observed** is populated with the timestamp of the beginning of the time window during which the data was seen viii. **last_observed** is populated with the timestamp of the end of the time window during which the data was seen ix. **number_observed** specifies the number of times each cyber-observable object(s) represented in **object_refs** was seen x. **object_refs** contains the identifiers of SCOs and SROs representing the observation. At least one SCO **MUST** be included c. The SCO(s) referenced in the Observed Data's **object_refs**. The SCO(s) must comply with the relevant subsection(s) within section 6 of the STIX 2.1 OASIS Standard d. If referencing any SRO(s), the SRO(s) must comply with the relevant subsection(s) within section 5 of the STIX 2.1 OASIS Standard

3.14.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.14.2.

3.14.3.1 Observed Data of File Hash

The primary use case for Observed Data is to capture raw information about cyber security related entities. In this example, the analyst captures the file hash of a DLL associated with a cyber incident.

```
{
    "type": "identity",
    "id": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "spec_version": "2.1",
    "created": "2015-04-14T13:07:49.812Z",
    "modified": "2015-04-14T13:07:49.812Z",
    "name": "Oscorp Industries",
    "identity_class": "organization",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c"
},
{
    "type": "observed-data",
    "id": "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb1",
    "spec_version": "2.1",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2017-02-28T19:37:11.213Z",
    "modified": "2017-02-28T19:37:11.213Z",
    "first_observed": "2017-02-27T21:37:11.213Z",
    "last_observed": "2017-02-27T21:37:11.213Z",
    "number_observed": 1,
    "object_refs": [ "file--e277603e-1060-5ad4-9937-c26c97f1ca68" ]
},
{
    "type": "file",
    "spec_version": "2.1",
    "id": "file--e277603e-1060-5ad4-9937-c26c97f1ca68",
    "hashes": {
        "SHA-256": "fe90a7e910cb3a4739bed9180e807e93fa70c90f25a8915476f5e4bfbac681db"
    },
    "size": 25536,
    "name": "foo.dll"
}
```

3.14.3.2 Observed Data of Domain Name and IP Address

Similarly, in this example, the analyst captures an IP address and corresponding domain name identified while investigating a cyber incident.

```
{
    "type": "identity",
    "id": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "spec_version": "2.1",
    "created": "2017-04-14T13:07:49.812Z",
    "modified": "2017-04-14T13:07:49.812Z",
    "name": "Oscorp Industries",
    "identity_class": "organization",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c"
},
```



```
{
    "type": "observed-data",
    "spec_version": "2.1",
    "id": "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2016-04-06T19:58:16.000Z",
    "modified": "2016-04-06T19:58:16.000Z",
    "first_observed": "2015-12-21T19:00:00Z",
    "last_observed": "2015-12-21T19:00:00Z",
    "number_observed": 50,
    "object_refs": [
        "ipv4-address--efcd5e80-570d-4131-b213-62cb18eaa6a8",
        "domain-name--ecb120bf-2694-4902-a737-62b74539a41b",
        “relationship--7ca2d678-c8c7-4947-a730-bfbc2cc5aa0a”
    ]
},
{
    "type": "domain-name",
    "spec_version": "2.1",
    "id": "domain-name--ecb120bf-2694-4902-a737-62b74539a41b",
    "value": "example.com",
    "resolves_to_refs": ["ipv4-addr--efcd5e80-570d-4131-b213-62cb18eaa6a8"]
},
{
    "type": "ipv4-addr",
    "spec_version": "2.1",
    "id": "ipv4-addr--efcd5e80-570d-4131-b213-62cb18eaa6a8",
    "value": "198.51.100.3"
},
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--7ca2d678-c8c7-4947-a730-bfbc2cc5aa0a",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2016-04-06T19:58:16.000Z",
    "modified": "2016-04-06T19:58:16.000Z",
    “source_ref”: “domain-name--ecb120bf-2694-4902-a737-62b74539a41b”,
    “target_ref”: “ipv4-addr--efcd5e80-570d-4131-b213-62cb18eaa6a8”,
    “relationship_type”: “resolves-to”
}
```

3.14.4 Producer Example Data

3.14.4.1 Observed Data with Several SCOs

```
{
    "type": "identity",
    "id": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "spec_version": "2.1",
    "created": "2017-04-14T13:07:49.812Z",
    "modified": "2017-04-14T13:07:49.812Z",
    "name": "Oscorp Industries",
    "identity_class": "organization",
```



```
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c"
},
{
    "type": "observed-data",
    "spec_version": "2.1",
    "id": "observed-data--359d9ff7-1d08-4af6-92e4-e9df5b1bad88",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2016-04-06T19:58:16.000Z",
    "modified": "2016-04-06T19:58:16.000Z",
    "first_observed": "2015-12-21T19:00:00Z",
    "last_observed": "2015-12-21T19:00:00Z",
    "number_observed": 50,
    "object_refs": [
        "ipv4-addr--ea9484e7-673d-4756-bcd6-844749024a27",
        "ipv6-addr--3d4f0428-0f9c-430f-b1ab-16a795f1894e",
        "domain-name--0c248491-69e9-43e5-8e90-23f5ce22e3e7",
        "relationship--cb878d74-1d04-4707-88a1-e1d90eb85737"
    ]
},
{
    "type": "ipv6-addr",
    "spec_version": "2.1",
    "id": "ipv6-addr--3d4f0428-0f9c-430f-b1ab-16a795f1894e",
    "value": "2001:0db8:85a3:0000:0000:8a2e:0370:7334"
},
{
    "type": "domain-name",
    "spec_version": "2.1",
    "id": "domain-name--0c248491-69e9-43e5-8e90-23f5ce22e3e7",
    "value": "forinstance.com",
    "resolves_to_refs": ["ipv4-addr--ea9484e7-673d-4756-bcd6-844749024a27"]
},
{
    "type": "ipv4-addr",
    "spec_version": "2.1",
    "id": "ipv4-addr--ea9484e7-673d-4756-bcd6-844749024a27",
    "value": "202.1.24.9"
},
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--cb878d74-1d04-4707-88a1-e1d90eb85737",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "created": "2016-04-06T19:58:16.000Z",
    "modified": "2016-04-06T19:58:16.000Z",
    "source_ref": "domain-name--0c248491-69e9-43e5-8e90-23f5ce22e3e7",
    "target_ref": "ipv4-addr--ea9484e7-673d-4756-bcd6-844749024a27",
    "relationship_type": "resolves-to"
}
```


3.14.5 Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Observed Data object. Additional required Consumer support for Observed Data is listed in the table below.

Table 29 - Required Consumer Support for Observed Data

Persona	Behavior
All Observed Data Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more Observed Data objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each Observed Data object, the Consumer can process the information about the Observed Data fields to the user 4. For each Observed Data object, the Consumer can process any related SDOs/SROs and associated fields

3.14.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the Observed Data Producer Test Case Data, as per the requirements in section 3.14.5.

3.15 Opinion Sharing

An Opinion is an assessment of the correctness of the information in a STIX Object produced by a different entity. Opinions are used by entities to provide a level of agreement or disagreement on one or more SDOs, SCOs or SROs through embedded references to these objects.

3.15.1 Description

For example, an analyst from a consuming organization might say that they "strongly disagree" with a Campaign object and provide an explanation about why. In a more automated workflow, a SOC operator might give an Indicator "one star" in their TIP (expressing "strongly disagree") because it is considered to be a false positive within their environment. Opinions are subjective, and the STIX 2.1 OASIS Standard does not address how best to interpret them. Sharing communities are encouraged to provide clear guidelines to their constituents regarding best practice for the use of Opinion objects within the community.

3.15.2 Required Producer Persona Support

The Producer persona must be able to create STIX content with one or more Opinions on at least one SDO, SCO, or SRO.

Table 30 - Required Producer Support for Opinion

Personas	Behavior

All Opinion Producer personas	1. Producer allows a user to select or specify the STIX content to send to a Consumer persona 2. The following data must be provided by the persona: a) The Identity object must comply with the Identity object referenced in section 2.3.4 b) The Opinion object must conform to the Opinion specification as per section 4.15 of the STIX 2.1 OASIS Standard; specifically, these properties must be provided: i) **type** must be 'opinion' ii) **spec_version** must be '2.1' iii) **id** must uniquely identify the Opinion, and must be a UUID prepended with 'opinion--' iv) **created_by_ref** must point to the Identity of the Producer v) **created** must match the timestamp, to millisecond granularity, of when the user created the Opinion vi) **modified** must match the timestamp, to millisecond granularity, of when this particular version of the Opinion was last modified vii) **opinion** must convey the level of agreement or disagreement about all of the STIX object(s) listed in object_refs, using a value from the opinion-enum viii) **object_refs** is a list containing the IDs of each STIX Object to which this Opinion applies c) The object(s) referenced in the Opinion's **object_refs**. The object(s) must comply with the relevant section(s) of the STIX 2.1 OASIS Standard

3.15.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.15.2.

3.15.3.1 Opinion on Indicator Created by Different Identity

A common use case for Opinions is providing agreement/disagreement on the validity of Indicators with respect to whether they are detecting activity or artifacts that are actually malicious. In this case, the Producer creates an Opinion which disagrees with the validity of an Indicator for a malicious domain name.

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "identity",
    "id": "identity--a562f809-377b-45e0-aa1c-6a4751abc5dd",
    "spec_version": "2.1",
```

```
    "identity_class": "organization",
    "name": "EMCA Corp, Inc.",
    "created": "2016-02-29T12:34:56.000Z",
    "modified": "2016-02-29T12:34:56.000Z",
    "created_by_ref": "identity--a562f809-377b-45e0-aa1c-6a4751abc5dd"
},
{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-04-06T20:03:48.000Z",
    "modified": "2018-04-06T20:03:48.000Z",
    "indicator_types": ["malicious-activity"],
    "name": "Malicious Domain Name",
    "pattern": "[ domain-name:value = 'www.example.com']",
    "pattern_type": "stix",
    "valid_from": "2016-01-01T00:00:00Z"
},
{
    "type": "opinion",
    "spec_version": "2.1",
    "id": "opinion--b01efc25-77b4-4003-b18b-f6e24b5cd9f7",
    "created_by_ref": "identity--a562f809-377b-45e0-aa1c-6a4751abc5dd",
    "created": "2019-05-12T08:17:27.000Z",
    "modified": "2019-05-12T08:17:27.000Z",
    "object_refs": ["indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f"],
    "opinion": "strongly-disagree"
}
```

3.15.3.2 Opinion on Malware Created by Different Identity

Another use case for Opinions is providing agreement/disagreement on the validity of Malware with regards to whether the SDO is in fact malware or just a benign file. In this case, the Producer creates an Opinion which disagrees with the assertion that a Malware SDO references a malicious file.

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "identity",
    "id": "identity--7e4e8c59-b592-47fd-b90b-4827370e088a",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "BDNF Corp, Inc.",
    "created": "2019-01-17T11:11:13.000Z",
```



```
    "modified": "2019-01-17T11:11:13.000Z",
    "created_by_ref": "identity--7e4e8c59-b592-47fd-b90b-4827370e088a"
},
{
    "type": "opinion",
    "spec_version": "2.1",
    "id": "opinion--037754a3-cbc4-472e-a258-ddd91e767aa5",
    "created_by_ref": "identity--7e4e8c59-b592-47fd-b90b-4827370e088a",
    "created": "2019-07-22T10:05:02.000Z",
    "modified": "2019-07-22T10:05:02.000Z",
    "object_refs": ["malware--bf781134-1da9-4058-8faa-d5a58a181805"],
    "opinion": "disagree"
},
{
    "type": "malware",
    "spec_version": "2.1",
    "id": "malware--bf781134-1da9-4058-8faa-d5a58a181805",
    "created": "2019-06-27T15:03:11.000Z",
    "modified": "2019-06-27T15:03:11.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
    "name": "Foobot",
    "malware_types": ["trojan"],
    "is_family": false,
    “capabilities”: [
        “accesses-remote-machines”, “determines-c2-server”
    ],
    “first_seen”: “2019-05-27T15:03:11.000Z”,
    “last_seen”: “2019-06-26T15:03:11.000Z”,
    “implementation_languages”: [
        “python”
    ],
    “architecture_execution_envs”: [
        “mips”
    ]
}
```

3.15.4 Producer Example Data

3.15.4.1 Opinion with Explanation and Authors

```
{
    "type": "identity",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "identity",
    "id": "identity--a562f809-377b-45e0-aa1c-6a4751abc5dd",
```



```
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "EMCA Corp, Inc.",
    "created": "2016-02-29T12:34:56.000Z",
    "modified": "2016-02-29T12:34:56.000Z",
    "created_by_ref": "identity--a562f809-377b-45e0-aa1c-6a4751abc5dd"
},
{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-04-06T20:03:48.000Z",
    "modified": "2018-04-06T20:03:48.000Z",
    "indicator_types": ["malicious-activity"],
    "name": "Malicious Domain Name",
    "pattern": "[ domain-name:value = 'www.example.com']",
    "pattern_type": "stix",
    "valid_from": "2016-01-01T00:00:00Z"
},
{
    "type": "opinion",
    "spec_version": "2.1",
    "id": "opinion--b01efc25-77b4-4003-b18b-f6e24b5cd9f7",
    "created_by_ref": "identity--a562f809-377b-45e0-aa1c-6a4751abc5dd",
    "created": "2019-05-12T08:17:27.000Z",
    "modified": "2019-05-12T08:17:27.000Z",
    "object_refs": ["indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f"],
    "opinion": "strongly-disagree",
    "explanation": "This doesn't seem like it is feasible. We've seen how PandaCat has
attacked Spanish infrastructure over the last 3 years, so this change in targeting seems too
great to be viable. The methods used are more commonly associated with the FlameDragonCrew.",
    “authors”: [
        “Alice”,
        “Bob”
    ]
}
```

3.15.5 Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Opinion object. Additional required Consumer support for Opinions is listed in the table below.

Table 31 - Required Consumer Support for Opinion

Persona	Behavior
All Opinion Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more Opinion objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as

	enumerated in section 2.3.4 3. For each Opinion object, the Consumer can process the information about the Opinion fields to the user 4. For each Opinion object, the Consumer can process any related SDOs/SROs and associated fields

3.15.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the Opinion Producer Test Case Data, as per the requirements in section 3.15.5.

3.16 Report Sharing

Reports are collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including context and related details. Reports group related threat intelligence together so that it can be published as a comprehensive cyber threat story.

3.16.1 Description

The Report SDO contains a list of references to STIX Objects (the CTI objects included in the report) along with a textual description and the name of the report.

3.16.2 Required Producer Persona Support

Table 32 - Required Producer Support for Report

Personas	Behavior
All Report Producer personas	1. Producer allows a user to select or specify the STIX content to send to a Consumer persona 2. The following data must be provided by the persona: a. The Identity object must comply with the Identity object referenced in section 2.3.4 b. The Report object must conform to the Report specification as per section 4.16 of the STIX 2.1 OASIS Standard; specifically, these properties must be provided: i. **type** must be 'report' ii. **spec_version** must be '2.1' iii. **id** must uniquely identify the Report, and must be a UUID prepended with 'report--' iv. **created_by_ref** must point to the Identity of the Producer v. **created** is the time at which the Report object was originally created vi. **modified** is the time at which this particular version of the Report was last modified vii. **name** must be a string that identifies the name of the Report viii. **published** must be a timestamp that corresponds to the date the Report was officially published ix. **object_refs** must specify the object(s) that the Report references x. **report_types** is the primary type(s) of content found in this report. The values for this property SHOULD come from the report-type-ov open vocabulary c. The SDO(s) referenced in the Report's **object_refs**. The SDO(s) must

	comply with the relevant subsection(s) within section 4 of the STIX 2.1 OASIS Standard

3.16.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.16.2.

3.16.3.1 Create Report Object

A Campaign object is created, with an Indicator object included and referenced by the Campaign's object_refs.

```
{
    "type": "identity",
    "id": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "XYZA Corp, Inc.",
    "created": "2017-01-17T11:11:13.000Z",
    "modified": "2017-01-17T11:11:13.000Z",
    “created_by_ref”: "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5"
},
{
    "type": "report",
    "spec_version": "2.1",
    "id": "report--84e4d88f-44ea-4bcd-bbf3-b2c1c320bcbd",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5,
    "created": "2019-12-21T19:59:11.000Z",
    "modified": "2020-05-21T19:59:11.000Z",
    "name": "Glass Gazelle Campaign",
    "published": "2020-01-201T17:00:00Z",
    "report_types": [ "campaign" ],
    "object_refs": [
        "indicator--26ffb872-1dd9-446e-b6f5-d58527e5b5d2"
    ]
},
{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--26ffb872-1dd9-446e-b6f5-d58527e5b5d2",
    "created": "2019-12-21T19:59:17.000Z",
    "modified": "2020-05-21T19:59:17.000Z",
    "name": "Some indicator",
    "indicator_types": ["malicious-activity"],
    "pattern": "[ file:hashes.MD5 = '3773a88f65a5e780c8dff9cdc3a056f3' ]",
    "pattern_type": "stix",
    "valid_from": "2015-12-21T19:59:17Z",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5"
}
```

3.16.4 Producer Example Data

3.16.4.1 Campaign Report

A threat report discussing a campaign can be represented using a Report object. As shown below, the Report **description** property contains the narrative of the report while the Campaign object and any related SDOs (e.g., Indicators for the Campaign, Malware it uses, and the associated Relationships) is referenced in the **objects_refs** property.

```
{
    "type": "identity",
    "id": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "XYZA Corp, Inc.",
    "created": "2017-01-17T11:11:13.000Z",
    "modified": "2017-01-17T11:11:13.000Z",
    “created_by_ref”: "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5"
},
{
    "type": "report",
    "spec_version": "2.1",
    "id": "report--84e4d88f-44ea-4bcd-bbf3-b2c1c320bcbd",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "created": "2019-12-21T19:59:11.000Z",
    "modified": "2020-05-21T19:59:11.000Z",
    "name": "Glass Gazelle Campaign",
    "description": "This report includes details related to the Glass Gazelle campaign,
including a key indicator.",
    "published": "2020-01-201T17:00:00Z",
    "report_types": ["campaign"],
    "object_refs": [
        "indicator--26ffb872-1dd9-446e-b6f5-d58527e5b5d2",
        "campaign--83422c77-904c-4dc1-aff5-5c38f3a2c55c",
        "relationship--f82356ae-fe6c-437c-9c24-6b64314ae68a"
    ]
},
{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--26ffb872-1dd9-446e-b6f5-d58527e5b5d2",
    "created": "2019-12-21T19:59:17.000Z",
    "modified": "2020-05-21T19:59:17.000Z",
    "name": "Some indicator",
    "indicator_types": ["malicious-activity"],
    "pattern": "[ file:hashes.MD5 = '3773a88f65a5e780c8dff9cdc3a056f3' ]",
    "pattern_type": "stix",
    "valid_from": "2015-12-21T19:59:17Z",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5"
},
{
    "type": "campaign",
```



```
    "spec_version": "2.1",
    "id": "campaign--83422c77-904c-4dc1-aff5-5c38f3a2c55c",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "created": "2019-12-21T19:59:17.000Z",
    "modified": "2020-05-21T19:59:17.000Z",
    "name": "Glass Gazelle Campaign"
},
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--f82356ae-fe6c-437c-9c24-6b64314ae68a",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "created": "2015-12-21T19:59:17.000Z",
    "modified": "2015-12-21T19:59:17.000Z",
    "source_ref": "indicator--26ffb872-1dd9-446e-b6f5-d58527e5b5d2",
    "target_ref": "campaign--26ffb872-1dd9-446e-b6f5-d58527e5b5d2",
    "relationship_type": "indicates"
}
```

3.16.4.2 Malware Analysis Report

A threat report discussing the analysis of a malware sample can be represented using a Report object. An example is shown below.

```
{
    "type": "identity",
    "id": "identity--826d4837-a92b-44a3-91c9-107ec7982c1d",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "XYZA Corp, Inc.",
    "created": "2017-01-17T11:11:13.000Z",
    "modified": "2017-01-17T11:11:13.000Z",
    “created_by_ref’: "identity--826d4837-a92b-44a3-91c9-107ec7982c1d"
},
{
    "type": "report",
    "spec_version": "2.1",
    "id": "report--980275a5-4423-46c6-bb79-235654096f8a",
    "created_by_ref": "identity--826d4837-a92b-44a3-91c9-107ec7982c1d",
    "created": "2020-01-24T19:59:11.000Z",
    "modified": "2020-01-24T19:59:11.000Z",
    "name": "Malware Analysis Report",
    "description": "This report contains analysis results of the ReallyBad banking trojan.",
    "published": "2020-01-251T17:00:00Z",
    "report_types": ["malware"],
    "object_refs": [
        "malware--bb4ca8dd-1248-5fef-8828-9bd2d935fa58",
        "malware-analysis--332ca8f0-1888-0bef-8828-54d2d935fb27",
        "malware-analysis--bf43a8f0-0078-034f-c828-735dfb15f008",
        "malware-analysis--bd32a072-bf32-445f-c828-111dfb15fbba",
        "file--876275a5-b223-2394-b009-8384fc2536ba",
        "domain-name--b67d30ff-02ac-498a-92f9-32f845f448cf",
        "ipv4-addr--2320065d-2555-424f-ad9e-0f8428623c33",
```



```
        "url--9020065d-b255-114b-a33e-0394fc243ab4",
        "relationship--93049345-93bc-3920-493b-032bc238ad23",
        "relationship--9403bd85-35dd-09dd-091d-9302fb23ae9e",
        "relationship--bc238ad2-3b32-04ff-1023-74bdf3811882"
    ]
},
{
    "type": "malware",
    "spec_version": "2.1",
    "id": "malware--bb4ca8dd-1248-5fef-8828-9bd2d935fa58",
    "created_by_ref": "identity--826d4837-a92b-44a3-91c9-107ec7982c1d",
    "created": "2020-01-16T18:52:24.277Z",
    "modified": "2020-01-16T18:52:24.277Z",
    "name": "a92e5b2bae.exe",
    "first_seen": "2019-03-16T18:52:24.277Z",
    "last_seen": "2020-01-01T23:52:24.277Z",
    "malware_types": [ "unknown" ],
    "is_family": false,
    "sample_refs": ["file--876275a5-b223-2394-b009-8384fc2536ba"]
},
{
    "type": "malware-analysis",
    "spec_version": "2.1",
    "id": "malware-analysis--332ca8f0-1888-0bef-8828-54d2d935fb27",
    "created_by_ref": "identity--826d4837-a92b-44a3-91c9-107ec7982c1d",
    "created": "2020-01-16T18:52:24.277Z",
    "modified": "2020-01-16T18:52:24.277Z",
    "product": "av-analysis-tool",
    "version": "1.3",
    "analysis_started": "2020-02-11T09:36:14Z",
    "analysis_ended": "2020-02-11T09:36:14Z",
    "result": "malicious",
    "sample_ref": "file--876275a5-b223-2394-b009-8384fc2536ba"
},
{
    "type": "malware-analysis",
    "spec_version": "2.1",
    "id": "malware-analysis--bf43a8f0-0078-034f-c828-735dfb15f008",
    "created_by_ref": "identity--826d4837-a92b-44a3-91c9-107ec7982c1d",
    "created": "2020-01-16T18:52:24.277Z",
    "modified": "2020-01-16T18:52:24.277Z",
    "product": "static-analysis-tool",
    "version": "1.2.3",
    "analysis_sco_refs": [ "file--876275a5-b223-2394-b009-8384fc2536ba" ],
    "sample_ref": "file--876275a5-b223-2394-b009-8384fc2536ba"
},
{
    "type": "malware-analysis",
    "spec_version": "2.1",
    "id": "malware-analysis--bd32a072-bf32-445f-c828-111dfb15fbba",
    "created_by_ref": "identity--826d4837-a92b-44a3-91c9-107ec7982c1d",
    "created": "2020-01-16T18:52:24.277Z",
    "modified": "2020-01-16T18:52:24.277Z",
```



```
    "product": "dynamic-analysis-tool",
    "version": "3.2.1",
    "analysis_started": "2020-01-24T10:23:40Z",
    "analysis_ended": "2020-01-24T10:24:08Z",
    "result": "malicious",
    "analysis_sco_refs": [
        "domain-name--b67d30ff-02ac-498a-92f9-32f845f448cf",
        "ipv4-addr--2320065d-2555-424f-ad9e-0f8428623c33",
        "url--9020065d-b255-114b-a33e-0394fc243ab4"
    ],
    "sample_ref": "file--876275a5-b223-2394-b009-8384fc2536ba"
},
{
    "type": "file",
    "id": "file--876275a5-b223-2394-b009-8384fc2536ba",
    "created_by_ref": "identity--826d4837-a92b-44a3-91c9-107ec7982c1d",
    "spec_version": "2.1",
    "name": "badtrojan.exe"
},
{
    "type": "domain-name",
    "spec_version": "2.1",
    "id": "domain-name--b67d30ff-02ac-498a-92f9-32f845f448cf",
    "value": "badplace.com",
    "resolves_to_refs": ["ipv4-addr--2320065d-2555-424f-ad9e-0f8428623c33"]
},
{
    "type": "ipv4-addr",
    "spec_version": "2.1",
    "id": "ipv4-addr--2320065d-2555-424f-ad9e-0f8428623c33",
    "value": "198.192.1.3"
},
{
    "type": "url",
    "spec_version": "2.1",
    "id": "url--9020065d-b255-114b-a33e-0394fc243ab4",
    "value": "http://badplace.com/index.html"
},
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--93049345-93bc-3920-493b-032bc238ad23",
    "created_by_ref": "identity--826d4837-a92b-44a3-91c9-107ec7982c1d",
    "created": "2020-01-16T18:52:24.277Z",
    "modified": "2020-01-16T18:52:24.277Z",
    "relationship_type": "av-analysis-of",
    "source_ref": "malware-analysis--332ca8f0-1888-0bef-8828-54d2d935fb27",
    "target_ref": "malware--bb4ca8dd-1248-5fef-8828-9bd2d935fa58"
},
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--9403bd85-35dd-09dd-091d-9302fb23ae9e",
```



```
    "created_by_ref": "identity--826d4837-a92b-44a3-91c9-107ec7982c1d",
    "created": "2020-01-16T18:52:24.277Z",
    "modified": "2020-01-16T18:52:24.277Z",
    "relationship_type": "static-analysis-of",
    "source_ref": "malware-analysis--bf43a8f0-0078-034f-c828-735dfb15f008",
    "target_ref": "malware--bb4ca8dd-1248-5fef-8828-9bd2d935fa58"
},
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--bc238ad2-3b32-04ff-1023-74bdf3811882",
    "created_by_ref": "identity--826d4837-a92b-44a3-91c9-107ec7982c1d",
    "created": "2020-01-16T18:52:24.277Z",
    "modified": "2020-01-16T18:52:24.277Z",
    "relationship_type": "dynamic-analysis-of",
    "source_ref": "malware-analysis--bd32a072-bf32-445f-c828-111dfb15fbba",
    "target_ref": "malware--bb4ca8dd-1248-5fef-8828-9bd2d935fa58"
}
```

3.16.5 Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Report object. Additional required Consumer support for Reports is listed in the table below.

Table 33 - Required Consumer Support for Report

Personas	Behavior
All Report Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more Report objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each Report object, the Consumer can process the information about the Report fields to the user 4. For each Report object, the Consumer can process any related SDOs/SROs and associated fields

3.16.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the Report Producer Test Case Data, as per the requirements in section 3.16.5.

3.17 Sighting Sharing

Another important scenario that will provide for crowdsourcing in the context of a sharing community is the use of a Sighting STIX Relationship Object (SRO). This is a unique form of a Relationship object that denotes the confirmation that something in CTI (e.g. an indicator, malware, tool, etc.) was seen. The full power of the use of trust communities within the ISAC and/or ISAO context cannot be realized without the use of this SRO.

3.17.1 Description

A STIX 2.1 Sighting object is an SRO primarily used to capture documentation that some entity in the network has been seen by an intelligence source. An analyst could select for sharing one or more Sightings observed by a supporting SIEM tool. The SIEM could then publish STIX Sightings content for various Consumer personas.

3.17.2 Required Producer Persona Support

The Producer persona must be able to create one or more Sighting objects along with associated STIX object(s) representing what was actually seen on the systems and networks.

Table 34 - Required Producer Support for Sighting

Persona	Behavior
All Sighting Producer personas	1. Producer allows a user to select or specify the STIX content to send to a Consumer persona 2. The following data must be provided by the persona: a) The Identity object must comply with the Identity object referenced in section 2.3.4 b) The Sighting object must conform to the Sighting specification as per section 5.2 of the STIX 2.1 OASIS Standard; specifically, these properties must be provided: i) **type** must be 'sighting' ii) **spec_version** must be '2.1' iii) **id** must uniquely identify the Sighting, and must be a UUID prepended with "sighting--" iv) **created_by_ref** must point to the Identity of the entity publishing the Sighting v) **created** is the time at which the Sighting was originally created vi) **modified** is the time at which this particular version of the Sighting was last modified vii) **sighting_of_ref** is an ID reference to the SDO that was sighted viii) **count** is an integer between 0 and 999,999,999 inclusive and represents the number of times the SDO referenced by the sighting_of_ref property was sighted ix) **first_seen** and **last_seen**, respectively, are the beginning and end of the time window during which the SDO referenced by the sighting_of_ref property was sighted c) The SDO object referenced by **sighting_of_ref** must conform to that object's specification from the STIX 2.1 OASIS Standard

3.17.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.17.2.

3.17.3.1 Sighting of Indicator

```
{
```



```
    "type": "identity",
    "id": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
    "created": "2015-01-20T12:34:56.000Z",
    "modified": "2015-01-20T12:34:56.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    “type”: “indicator”,
    “id”: “indicator--12fd1bad-8306-4ed4-8c9b-7dfdd8ad5eb8”,
    “spec_version”: “2.1”,
    “created”: “2018-05-20T12:34:56.000Z”,
    “modified”: “2018-05-20T12:34:56.000Z”,
    “created_by_ref”: “identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb”,
    “valid_from”: “2017-12-21T19:00:00.000Z”,
    “name”: “Poison Ivy Malware”,
    “pattern”: “[ file:hashes.’SHA-256’ =
'4bac27393bdd9777ce02453256c5577cd02275510b2227f473d03f533924f877']”,
    “pattern_type”: “stix”
},
{
    "type": "sighting",
    "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c75",
    "spec_version": "2.1",
    "created_by_ref": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "created": "2021-01-17T11:11:13.000Z",
    "modified": "2021-01-17T11:11:13.000Z",
    "first_seen": "2017-12-21T19:00:00.000Z",
    "last_seen": "2018-01-06T19:00:00.000Z",
    “count”: 50,
    "sighting_of_ref": "indicator--12fd1bad-8306-4ed4-8c9b-7dfdd8ad5eb8"
}
```

3.17.4 Producer Example Data

3.17.4.1 Sighting of Indicator with Observed Data

The following example shows how a Sighting object could be used to demonstrate that a particular Indicator’s pattern content was seen on a network, along with the File object associated with the pattern.

```
{
    "type": "identity",
    "id": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
    "created": "2015-01-20T12:34:56.000Z",
    "modified": "2015-01-20T12:34:56.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
```



```
    "type": "sighting",
    "spec_version": "2.1",
    "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c75",
    "created_by_ref": "identity--f431f809-377b-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",
    "spec_version": "2.1",
    "id": "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-04-06T19:58:16.000Z",
    "modified": "2016-04-06T19:58:16.000Z",
    "first_observed": "2015-12-21T19:00:00Z",
    "last_observed": "2016-04-06T19:58:16Z",
    "number_observed": 50,
    "object_refs": [
        "file--30038539-3eb6-44bc-a59e-d0d3fe84695a"
    ]
},
{
    "type": "file",
    "spec_version": "2.1",
    "id": "file--30038539-3eb6-44bc-a59e-d0d3fe84695a",
    "hashes": {
        "SHA-256": "fe90a7e910cb3a4739bed9180e807e93fa70c90f25a8915476f5e4bfbac681db"
    },
    "size": 25536,
    "name": "foo.dll"
}
```


3.17.5 Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Sighting object. Additional required Consumer support for Sightings is listed in the table below.

Table 35 - Required Consumer Support for Sighting

Persona	Behavior
All Sighting Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more Sighting objects c. One or more SROs or embedded relationships

	2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each Sighting object, the Consumer can process the information about the Sighting fields to the user 4. For each Sighting object, the Consumer can process any related SDOs/SROs and associated fields

3.17.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the Sighting Producer Test Case Data, as per the requirements in section 3.17.5.

3.18 Threat Actor Sharing

Threat Actors are individuals, groups, or organizations believed to be operating with malicious intent. Threat Actors leverage their resources, and possibly the resources of an Intrusion Set, to conduct attacks and run Campaigns against targets.

3.18.1 Description

Furthermore, Threat Actors can be characterized by their motives, capabilities, goals, sophistication level, past activities, resources they have access to, and their role in the organization.

3.18.2 Required Producer Persona Support

The Producer Persona must be able to create STIX content with one or more Threat Actor objects.

Table 36 - Required Producer Support for Threat Actor

Personas	Behavior

All Threat Actor Producer personas	1. Producer allows a user to select or specify the STIX content to send to a Consumer persona 2. The following data must be provided by the persona: a. The Identity object must comply with the Identity object referenced in section 2.3.4 b. The Threat Actor object must conform to the Threat Actor specification as per section 4.17 of the STIX 2.1 OASIS Standard; specifically, these properties must be provided: i. **type** must be 'threat-actor' ii. **spec_version** must be '2.1' iii. **id** must uniquely identify the Threat Actor, and must be a UUID prepended with 'threat-actor--' iv. **created_by_ref** must point to the Identity of the Producer v. **created** must match the timestamp, to millisecond granularity, of when the Threat Actor was originally created vi. **modified** must match the timestamp, to millisecond granularity, of when this particular version of the Threat Actor was last modified vii. **name** is used to identify this Threat Actor or Threat Actor group viii. **threat_actor_types** is the type(s) of this threat actor. The values for this property SHOULD come from the threat-actor-type-ov open vocabulary ix. **roles** is a list of roles the Threat Actor plays. The values for this property SHOULD come from the threat-actor-role-ov open vocabulary x. **sophistication** is the skill, specific knowledge, special training, or expertise a Threat Actor must have to perform the attack. The value for this property SHOULD come from the threat-actor-sophistication-ov open vocabulary xi. **resource_level** is the organizational level at which this Threat Actor typically works, which in turn determines the resources available to this Threat Actor for use in an attack. This attribute is linked to the sophistication property — a specific resource level implies that the Threat Actor has access to at least a specific sophistication level. The value for this property SHOULD come from the attack-resource-level-ov open vocabulary xii. **primary_motivation** is the primary reason, motivation, or purpose behind this Threat Actor. The motivation is why the Threat Actor wishes to achieve the goal (what they are trying to achieve). For example, a Threat Actor with a goal

		to disrupt the finance sector in a country might be motivated by ideological hatred of capitalism. The value for this property SHOULD come from the attack-motivation-ov open vocabulary

3.18.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.18.2.

3.18.3.1 Threat Actor Test Case

A Producer must be able to create Identity and Threat Actor objects, such as the below content.

```
{
    "type": "identity",
    "name": "ACME Corp, Inc.",
    "identity_class": "organization",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "created": "2020-01-20T12:34:56.000Z",
    "modified": "2020-01-20T12:34:56.000Z",
```

```
    “created_by_ref”: "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "threat-actor",
    "spec_version": "2.1",
    "id": "threat-actor--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",
    "threat_actor_types": [ "crime-syndicate"],
    "name": "Evil Org",
    "description": "The Evil Org threat actor group",
    "roles": [ "director" ],
    "sophistication": "advanced",
    "resource_level": "team",
    "primary_motivation": "organizational-gain"
}
```

3.18.3.2 Campaign Attributed to Threat Actor

```
{
    "type": "identity",
    "name": "ACME Corp, Inc.",
    "identity_class": "organization",
    "id": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "spec_version": "2.1",
    "created": "2020-01-20T12:34:56.000Z",
    "modified": "2020-01-20T12:34:56.000Z",
    “created_by_ref”: "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "threat-actor",
    "spec_version": "2.1",
    "id": "threat-actor--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",
    "threat_actor_types": [ "crime-syndicate"],
    "name": "Evil Org",
    "roles": [ "director" ],
    "sophistication": "advanced",
    "resource_level": "team",
    "primary_motivation": "organizational-gain"
},
{
    "type": "campaign",
    "spec_version": "2.1",
    "id": "campaign--555d5f47-5a6a-442d-915a-04097ca98a73",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-04-06T20:03:00.000Z",
    "modified": "2016-04-06T20:03:00.000Z",
    "name": "Green Group Attacks Against Finance"
},
```



```
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--12bb26f9-ceb7-46f4-952f-b24f7b1f78c0",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-04-06T20:03:00.000Z",
    "modified": "2016-04-06T20:03:00.000Z",
    "source_ref": "campaign--555d5f47-5a6a-442d-915a-04097ca98a73",
    “target_ref”: "threat-actor--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f"
    “relationship_type”: “attributed-to”
}
```

3.18.4 Producer Example Data

3.18.4.1 Threat Actor Attributed to an Identity

When investigating cyber related incidents, it is beneficial to capture information about the threat actor perpetrating the attack. This example links an Identity SDO to a Threat Actor SDO providing attribution.

```
{
    "type": "identity",
    "id": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "spec_version": "2.1",
    "created": "2015-04-14T13:07:49.812Z",
    "modified": "2015-04-14T13:07:49.812Z",
    "name": "Oscorp Industries",
    "identity_class": "organization"
},
{
    "type": "threat-actor",
    "spec_version": "2.1",
    "id": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500",
    "created": "2016-08-08T15:50:10.983Z",
    "modified": "2016-08-08T15:50:10.983Z",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "name": "Fake BPP (Branistan Peoples Party)",
    "threat_actor_types": [
        "nation-state"
    ],
    "roles": [
        "director"
    ],
    "goals": [
        "Influence the election in Branistan"
    ],
    "sophistication": "strategic",
    "resource_level": "government",
    "primary_motivation": "ideology",
    "secondary_motivations": [
        "dominance"
    ]
},
```



```
{
    "type": "identity",
    "spec_version": "2.1",
    "id": "identity--8c6af861-7b20-41ef-9b59-6344fd872a8f",
    "created": "2016-08-08T15:50:10.983Z",
    "modified": "2016-08-08T15:50:10.983Z",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "name": "Franistan Intelligence",
    "identity_class": "organization"
},
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--4bd67b9e-d112-4ea6-98bb-080a051667c7",
    "created": "2020-02-29T17:41:44.941Z",
    "modified": "2020-02-29T17:41:44.941Z",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "relationship_type": "attributed-to",
    "source_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500",
    "target_ref": "identity--8c6af861-7b20-41ef-9b59-6344fd872a8f"
}
```


3.18.4.2 Threat Actor Uses Malware

Another use case for the Threat Actor SDO is to describe how a threat actor operates. This example demonstrates how a threat actor leverages malware to carry out its cyber attacks.


```
{
    "type": "identity",
    "id": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "spec_version": "2.1",
    "created": "2015-04-14T13:07:49.812Z",
    "modified": "2015-04-14T13:07:49.812Z",
    "name": "Oscorp Industries",
    "identity_class": "organization"
},
{
    "type": "threat-actor",
    "spec_version": "2.1",
    "id": "threat-actor--9a8a0d25-7636-429b-a99e-b2a73cd0f11f",
    "created": "2015-05-07T14:22:14.760Z",
    "modified": "2015-05-07T14:22:14.760Z",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "name": "Adversary Bravo",
    "description": "Adversary Bravo is known to use phishing attacks to deliver remote access
malware to the targets.",
    "threat_actor_types": [
        "spy",
        "criminal"
    ]
},
{
    "type": "malware",
```

```
    "spec_version": "2.1",
    "id": "malware--d1c612bc-146f-4b65-b7b0-9a54a14150a4",
    "created": "2015-04-23T11:12:34.760Z",
    "modified": "2015-04-23T11:12:34.760Z",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "name": "Poison Ivy Variant d1c6",
    "malware_types": [
        "remote-access-trojan"
    ],
    "is_family": false,
    "kill_chain_phases": [
        {
            "kill_chain_name": "mandiant-attack-lifecycle-model",
            "phase_name": "initial-compromise"
        }
    ]
},
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--d44019b6-b8f7-4cb3-837e-7fd3c5724b87",
    "created": "2020-02-29T17:41:44.941Z",
    "modified": "2020-02-29T17:41:44.941Z",
    "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    "relationship_type": "uses",
    "source_ref": "threat-actor--9a8a0d25-7636-429b-a99e-b2a73cd0f11f",
    "target_ref": "malware--d1c612bc-146f-4b65-b7b0-9a54a14150a4"
}
```

3.18.5 Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Threat Actor object. Additional required Consumer support for Threat Actors is listed in the table below.

Table 37 - Required Consumer Support for Threat Actor

Persona	Behavior
All Threat Actor Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more Threat Actor objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each Threat Actor object, the Consumer can process the information about the Threat Actor fields to the user 4. For each Threat Actor object, the Consumer can process any related SDOs/SROs and associated fields

3.18.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the Threat Actor Producer Test Case Data, as per the requirements in section 3.18.5.

3.19 Tool Sharing

Tools are legitimate software that can be used by threat actors to perform attacks. Knowing how and when th3.14reat actors use such tools can be important for understanding how campaigns are executed. Unlike malware, these tools or software packages are often found on a system and have legitimate purposes for power users, system administrators, network administrators, or even normal users. Remote access tools (e.g., RDP) and network scanning tools (e.g., Nmap) are examples of Tools that may be used by a Threat Actor during an attack.

3.19.1 Description

The Tool SDO characterizes the properties of these software tools and can be used as a basis for making an assertion about how a Threat Actor uses them during an attack. It contains properties to name and describe the tool, a list of Kill Chain Phases the tool can be used to carry out, and the version of the tool.

This SDO **MUST NOT** be used to characterize malware. Further, Tool **MUST NOT** be used to characterize tools used as part of a course of action in response to an attack.

3.19.2 Required Producer Persona Support

The Producer persona must be able to create STIX content that contains a Tool object.

Table 38 - Required Producer Support for Tool

Personas	Behavior
All Tool Producer personas	1. Producer allows a user to select or specify the STIX content to send to a Consumer persona 2. The following data must be provided by the persona: a. The Identity object must comply with the Identity object referenced in section 2.3.4 b. The Tool object must conform to the Tool specification as per section 4.18 of the STIX 2.1 OASIS Standard; specifically, these properties must be provided: i. **type** must be 'tool' ii. **spec_version** must be '2.1' iii. **id** must uniquely identify the Tool, and must be a UUID prepended with 'tool--' iv. **created_by_ref** must point to the Identity of the Producer v. **created** is the time at which the Tool was originally created vi. **modified** is the time at which this particular version of the Tool was last modified vii. **name** must contain the name used to identify the Tool viii. **tool_types** are the kind(s) of tool(s) being described. The values for this property SHOULD come from the tool-type-ov open vocabulary

3.19.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.19.2.

3.19.3.1 Remote Access Tool

A Producer must be able to create Identity and Tool objects, such as the below content. A remote access tool can be captured in a Tool object as shown below.

```
{
    "type": "identity",
    "id": "identity--826d4837-a92b-44a3-91c9-107ec7982c1d",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "XYZA Corp, Inc.",
    "created": "2017-01-17T11:11:13.000Z",
    "modified": "2017-01-17T11:11:13.000Z",
    “created_by_ref”: "identity--826d4837-a92b-44a3-91c9-107ec7982c1d"
},
{
    "type": "tool",
    "spec_version": "2.1",
    "id": "tool--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "created_by_ref": "identity--826d4837-a92b-44a3-91c9-107ec7982c1d",
    "created": "2020-04-06T20:03:48.000Z",
    "modified": "2020-04-06T20:03:48.000Z",
    "tool_types": [ "remote-access" ],
    "name": "VNC"
}
```

3.19.4 Producer Example Data

3.19.4.1 Tool Drops Malware

Although a Tool object must not be used to characterize malware, a tool may drop malware, as illustrated in the example below.

```
{
    "type": "identity",
    "id": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "XYZA Corp, Inc.",
    "created": "2017-01-17T11:11:13.000Z",
    "modified": "2017-01-17T11:11:13.000Z".
    “created_by_ref”: "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5"
},
{
    "type": "tool",
    "spec_version": "2.1",
    "id": "tool--44322d2b-ffd4-b1bf-123f-008e46b3cd12",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "created": "2019-04-06T20:03:48.000Z",
```



```
    "modified": "2019-04-06T20:03:48.000Z",
    "tool_types": ["remote-access"],
    "name": "ftp"
},
{
    "type": "malware",
    "spec_version": "2.1",
    "id": "malware--bbb757e7-9bf9-3364-bf88-29dc0644d1e9",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "created": "2018-08-18T23:55:56.000Z",
    "modified": "2018-09-03T05:38:32.000Z",
    "name": "zeus",
    "malware_types": ["password-stealer"],
    "is_family": true
},
{
    "spec_version": "2.1",
    "type": "relationship",
    "id": "relationship--a502bd26-42d1-4020-b652-70ec37797cb6",
    "created": "2019-07-22T12:34:02.602Z",
    "modified": "2019-07-22T12:34:02.602Z",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "relationship_type": "drops",
    "source_ref": "tool--44322d2b-ffd4-b1bf-123f-008e46b3cd12",
    "target_ref": "malware--bbb757e7-9bf9-3364-bf88-29dc0644d1e9"
}
```


3.19.5 Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Tool object. Additional required Consumer support for Tools is listed in the table below.

Table 39 - Required Consumer Support for Tools

Personas	Behavior
All Tool Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more Tool objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each Tool object, the Consumer can process the information about the Tool fields to the user 4. For each Tool object, the Consumer can process any related SDOs/SROs and associated fields

3.19.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the Tool Producer Test Case Data, as per the requirements in section 3.19.5.

3.20 Versioning

As additional information is discovered about a SDO or SRO, the Producer of that object may version the original object using the versioning approach outlined in section 3.6 of the STIX 2.1 OASIS Standard. Consumers of the STIX object will also be updated through their various personas as the original object is versioned. This feature of the STIX 2.1 OASIS Standard allows for STIX objects to be updated as the context changes and the information becomes more complete, based on enrichments and further intelligence discovery.

As a rule of thumb, for the purpose of interoperability, if a value is changed for a property that is required of the Object as per the relevant section of the STIX 2.1 OASIS Standard, then the Producer **SHOULD** create a new object instead of simply versioning the initial object. This is because a change in value for an object's STIX 2.1 OASIS Standard-required property is considered a material change. Further, the Producer **SHOULD** then revoke the initial object.

If a value is changed or added for a property that is optional of the Object as per the relevant section of the STIX 2.1 OASIS Standard, the Producer **SHOULD** version the initial object as this is seen as a minor change.

3.20.1 Description

A STIX 2.1 Producer or Consumer must support versioning of SDOs and SROs to support interoperability within STIX.

3.20.2 Creation Required Producer Persona Support

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

The Producer persona can identify a STIX object that they wish to share with Consumers. For example, a Producer may wish to create a Threat Actor object and share it.

Table 40 - Required Producer Support for Versioning-Creation

Persona	Behavior
All Versioning Producer personas	1. Producer allows a user to select or specify the STIX content to create and send to a Consumer persona 2. The following data must be provided by the persona: a. The Identity object must comply with the Identity object referenced in section 2.3.4 b. The STIX Object being created must abide by the Producer requirements within the relevant use case of this document, except for Extensions which must abide by section 7.3 of the STIX 2.1 spec

3.20.3 Creation Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.20.2.

3.20.3.1 Creation of an Indicator

```
{
    "type": "identity",
    "id": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "id": "indicator--6cd5cd4f-ff42-4d67-8402-02aad22f8b63",
    "spec_version": "2.1",
    "name": "Bad IP1",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[ipv4-addr:value = '198.51.100.1']",
    "pattern_type": "stix"
}
```

3.20.3.2 Creation of a Sighting

```
{
    "type": "identity",
    "id": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "sighting",
    "id": "sighting--f185c0e8-f187-4880-be0b-1f10df2d356f",
    "spec_version": "2.1",
    "created_by_ref": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "first_seen": "2017-12-21T19:00:00.000Z",
    "last_seen": "2018-01-06T19:00:00.000Z",
    "count": 50,
    "sighting_of_ref": "indicator--12fd1bad-8306-4ed4-8c9b-7dfdd8ad5eb8"
},
{
    "type": "indicator",
    "id": "indicator--12fd1bad-8306-4ed4-8c9b-7dfdd8ad5eb8",
    "spec_version": "2.1",
```



```
    "name": "Bad IP1",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2017-12-17T11:11:13.000Z",
    "modified": "2017-12-17T11:11:13.000Z",
    "valid_from": "2017-12-22T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[ipv4-addr:value = '127.198.96.42']",
    "pattern_type": "stix"
}
```

3.20.4 Creation Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Creation Support. Additional required Consumer support for Versioning-Creation is listed in the table below.

Table 41 - Required Consumer Support for Versioning-Creation

Persona	Behavior
All Versioning Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more STIX Objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each STIX Object, the Consumer can process the information about the Object's fields to the user 4. For each STIX Object, the Consumer can process any related SDOs/SROs and associated fields

3.20.5 Creation Consumer Test Case Data

The Consumer **MUST** be able to handle the test cases within the Versioning-Creation Producer Test Case Data, as per the requirements in section 3.20.4.

3.20.6 Modification Required Producer Persona Support

The Producer persona must be able to create one or more SDOs/SROs with the appropriate date timestamp representing when the object was updated. Keep in mind the rule of thumb provided in section 3.3 for determining when to version an object.

The Producer persona can identify a STIX object that they wish to update and re-share to Consumers.

Table 42 - Required Producer Support for Versioning-Modification

Persona	Behavior
All Versioning Producer personas	1. Producer allows a user to select a previously shared STIX Object 2. The following data must be provided by the persona: a. The Identity object must comply with the Identity object referenced in section 2.3.4 b. The STIX Object being versioned must abide by the Producer

	requirements within the relevant use case of this document, except for Extensions which must abide by section 7.3 of the STIX 2.1 spec. Additionally: i. **created** must match, to millisecond granularity, when the object was originally created ii. **modified** must match, to millisecond granularity, when the object was selected to be re-shared after being updated. This timestamp **MUST** be later than the **created** timestamp

3.20.7 Modification Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.20.6.

3.20.7.1 Modification of an Indicator

```
{
    "type": "identity",
    "id": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "id": "indicator--6cd5cd4f-ff42-4d67-8402-02aad22f8b63",
    "spec_version": "2.1",
    "name": "Bad IP1",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-18T13:04:22.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["anomalous-activity"],
    "pattern": "[ ipv4-addr:value = '198.51.100.1' ]",
    "pattern_type": "stix"
}
```

3.20.7.2 Modification of a Sighting

```
{
    "type": "identity",
    "id": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
```



```
    "type": "sighting",
    "id": "sighting--f185c0e8-f187-4880-be0b-1f10df2d356f",
    "spec_version": "2.1",
    "created_by_ref": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-18T11:11:13.000Z",
    "first_seen": "2017-12-21T19:00:00.000Z",
    "last_seen": "2018-01-16T19:00:00.000Z",
    "count": 50,
    "sighting_of_ref": "indicator--12fd1bad-8306-4ed4-8c9b-7dfdd8ad5eb8"
},
{
    "type": "indicator",
    "id": "indicator--12fd1bad-8306-4ed4-8c9b-7dfdd8ad5eb8",
    "spec_version": "2.1",
    "name": "Bad IP1",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2017-12-17T11:11:13.000Z",
    "modified": "2017-12-17T11:11:13.000Z",
    "valid_from": "2017-12-22T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[ipv4-addr:value = '127.198.96.42']",
    "pattern_type": "stix"
}
```

3.20.8 Modification Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Versioning-Modification use case. Additional required Consumer support for Versioning-Modification is listed in the table below.

Table 43 - Required Consumer Support for Versioning-Modification

Persona	Behavior
All Versioning Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more STIX Objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each STIX Object, the Consumer can process the information about the Object's fields to the user 4. For each STIX Object, the Consumer can process any related SDOs/SROs and associated fields

3.20.9 Modification Consumer Test Case Data

The Consumer **MUST** be able to handle the test cases within the Versioning-Modification Producer Test Case Data, as per the requirements in section 3.20.8.

3.20.10 Revocation Required Producer Persona Support

The Producer persona must be able to create STIX content with one or more objects with the appropriate date representing when the object was revoked for sharing, along with **revoked** being set to True. Revoked objects are no longer considered valid by the Producer, and thus future versions of objects with a revoked **id MUST NOT** be created.

A Producer persona can identify a STIX object that they wish to update as revoked and re-share to Consumers.

Table 44 - Required Producer Support for Versioning-Revocation

Persona	Behavior
All Versioning Producer personas	1. Producer allows a user to select a previously shared STIX Object that is no longer valid and wishes to revoke that object 2. The following data must be provided by the persona: a. The Identity object must comply with the Identity object referenced in section 2.3.4 b. The STIX Object being revoked must abide by the Producer requirements within the relevant use case of this document, except for Extensions which must abide by section 7.3 of the STIX 2.1 spec. Additionally: i. **created** must match, to millisecond granularity, when the object was originally created ii. **modified** must match, to millisecond granularity, when the object was revoked. This timestamp **MUST** be later than the **created** timestamp iii. **revoked** must be set to true

3.20.11 Revocation Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.20.10.

3.20.11.1 Revocation of an Indicator

```
{
    "type": "identity",
    "id": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "indicator",
    "id": "indicator--6cd5cd4f-ff42-4d67-8402-02aad22f8b63",
    "spec_version": "2.1",
    "name": "Bad IP1",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2018-01-17T11:11:13.000Z",
```



```
    "modified": "2018-01-19T13:04:22.000Z",
    "valid_from": "2018-01-01T00:00:00.000Z",
    "indicator_types": ["anomalous-activity"],
    "pattern": "[ ipv4-addr:value = '198.51.100.1' ]",
    "pattern_type": "stix",
    "revoked": true
}
```

3.20.11.2 Revocation of a Sighting

```
{
    "type": "identity",
    "id": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "ACME Corp Sighting, Inc.",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-17T11:11:13.000Z",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff"
},
{
    "type": "sighting",
    "id": "sighting--f185c0e8-f187-4880-be0b-1f10df2d356f",
    "spec_version": "2.1",
    "created_by_ref": "identity--f6e43aa5-76cc-45ca-9b06-be2d65f26bfb",
    "created": "2018-01-17T11:11:13.000Z",
    "modified": "2018-01-19T11:11:13.000Z",
    "first_seen": "2017-12-21T19:00:00.000Z",
    "last_seen": "2018-01-16T19:00:00.000Z",
    "count": 50,
    "sighting_of_ref": "indicator--12fd1bad-8306-4ed4-8c9b-7dfdd8ad5eb8",
    "revoked": true
},
{
    "type": "indicator",
    "id": "indicator--12fd1bad-8306-4ed4-8c9b-7dfdd8ad5eb8",
    "spec_version": "2.1",
    "name": "Bad IP1",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2017-12-17T11:11:13.000Z",
    "modified": "2017-12-17T11:11:13.000Z",
    "valid_from": "2017-12-22T00:00:00.000Z",
    "indicator_types": ["malicious-activity"],
    "pattern": "[ipv4-addr:value = '127.198.96.42']",
    "pattern_type": "stix"
}
```

3.20.12 Revocation Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Revocation Support. Additional required Consumer support for Versioning-Revocation is listed in the table below.

Table 45 - Required Consumer Support for Versioning-Revocation

Persona	Behavior
All Versioning Consumer Personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more STIX Objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer **MUST** be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each STIX Object, the Consumer is able to verify that the **created_by_ref** value maps to a received Identity 4. For each STIX Object**,** the Consumer may show the **created** and **modified** dates for them and that the object has been revoked

3.20.13 Consumer Test Case Revocation Data

The Consumer **MUST** be able to handle the test cases within the Versioning-Revocation Producer Test Case Data, as per the requirements in section 3.20.12.

3.21 Vulnerability Sharing

A vulnerability is "a weakness or defect in the requirements, designs, or implementations of the computational logic (e.g., code) found in software and some hardware components (e.g., firmware) that can be directly exploited to negatively impact the confidentiality, integrity, or availability of that system.". Organizations share information about existing or 0-day vulnerabilities to inform asset management and compliance processes. Typically, STIX SDOs (e.g. Attack Pattern, Malware, etc.) reference a Vulnerability when it is targeted and exploited as part of malicious cyber activity.

3.21.1 Description

Vulnerability objects can be used as a linkage to the asset management and compliance process.

3.21.2 Required Producer Persona Support

Table 46 - Required Producer Support for Vulnerability

Personas	Behavior

All Vulnerability Producer personas	1. Producer allows a user to select or specify the STIX content to send to a Consumer persona 2. The following data must be provided by the persona: a. The Identity object must comply with the Identity object referenced in section 2.3.4 b. The Vulnerability object must conform to the Vulnerability specification as per section 4.19 of the STIX 2.1 OASIS Standard; specifically, these properties must be provided: i. **type** must be 'vulnerability' ii. **spec_version** must be '2.1' iii. **id** must uniquely identify the Vulnerability, and must be a UUID prepended with 'vulnerability--' iv. **created_by_ref** must point to the Identity of the Producer v. **created** is the time at which the Vulnerability was originally created vi. **modified** is the time at which this particular version of the Vulnerability was last modified vii. **name** identifies the vulnerability viii. **external_references** should be a list of external references which refer to non-STIX information

3.21.3 Producer Test Case Data

The Producer must be able to create the content within the following test cases in this section, as per the requirements in section 3.21.2.

3.21.3.1 Create Vulnerability Object

A Producer must be able to create a Vulnerability object, generating content such as the following content.

```
{
    "type": "identity",
    "id": "identity--d88cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "XYZA Corp, Inc.",
    "created": "2014-01-17T11:11:13.000Z",
    "modified": "2014-01-17T11:11:13.000Z",
    “created_by_ref”: “identity--d88cb6e5-0c4b-4611-8297-d1b8b55e40b5"
},
{
    "type": "vulnerability",
    "spec_version": "2.1",
    "id": "vulnerability--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
    "created": "2016-05-12T08:17:27.000Z",
    "modified": "2016-05-12T08:17:27.000Z",
    "created_by_ref": "identity--d88cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "name": "CVE-2016-1234",
```



```
    "external_references": [
        {
            "source_name": "cve",
            "external_id": "CVE-2016-1234"
        }
    ]
}
```

3.21.4 Producer Example Data

3.21.4.1 Malware Targets a Vulnerability

```
{
    "type": "identity",
    "id": "identity--d88cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "spec_version": "2.1",
    "identity_class": "organization",
    "name": "XYZA Corp, Inc.",
    "created": "2014-01-17T11:11:13.000Z",
    "modified": "2014-01-17T11:11:13.000Z"
},
{
    "type": "malware",
    "id": "malware--61a62a6a-9a18-4758-8e52-622431c4b8ae",
    "spec_version": "2.1",
    "created": "2015-05-15T09:00:00.000Z",
    "modified": "2015-05-15T09:00:00.000Z",
    "created_by_ref": "identity--d88cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "name": "Malicious Malware #5",
    "description": "Malicious malware #5 targets ABC software from Vendor XYZ",
    "malware_types": [
        "remote-access-trojan"
    ]
},
{
    "type": "vulnerability",
    "id": "vulnerability--c7cab3fb-0822-43a5-b1ba-c9bab34361a2",
    "spec_version": "2.1",
    "created": "2015-05-15T09:00:00.000Z",
    "modified": "2015-05-15T09:00:00.000Z",
    "created_by_ref": "identity--d88cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "name": "CVE-2012-1234",
    "description": "Vulnerability in ABC software from Vendor XYZ",
    "external_references": [
        {
            "source_name": "cve",
            "external_id": "CVE-2012-1234"
        }
    ]
},
{
    "type": "relationship",
    "id": "relationship--56b1023c-9e28-4449-8b4f-bc2adde45e1a",
```



```
    "spec_version": "2.1",
    "created": "2015-05-15T09:00:00.000Z",
    "modified": "2015-05-15T09:00:00.000Z",
    "created_by_ref": "identity--d88cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "relationship_type": "targets",
    "source_ref": "malware--61a62a6a-9a18-4758-8e52-622431c4b8ae",
    "target_ref": "vulnerability--717cb1c9-eab3-4330-8340-e4858055aa80"
}
```

3.21.4.2 Threat Actor Targets a Vulnerability

```
{
    "type": "identity",
    "id": "identity—1621d4d4-b67d-41e3-9670-f01faf20d111",
    "spec_version": "2.1",
    "created": "2015-05-10T16:27:17.760Z",
    "modified": "2015-05-15T16:27:17.760Z",
    "name": "Bravo Researchers",
    "identity_class": "organization"
},
{
    "type": "threat-actor",
    "id": "threat-actor—9a8a0d25-7636-429b-a99e-b2a73cd0f11f",
    "spec_version": "2.1",
    "created": "2015-05-07T14:22:14.760Z",
    "modified": "2015-05-07T14:22:14.760Z",
    "name": "Adversary Bravo",
    "description": "Adversary Bravo is known to use phishing attacks to deliver remote access
malware to the targets.",
    "threat_actor_types": ["spy", "criminal"],
    "created_by_ref": "identity—1621d4d4-b67d-41e3-9670-f01faf20d111"
},
{
    "type": "vulnerability",
    "id": "vulnerability--c7cab3fb-0822-43a5-b1ba-c9bab34361a2",
    "spec_version": "2.1",
    "created": "2015-05-15T09:00:00.000Z",
    "modified": "2015-05-15T09:00:00.000Z",
    "name": "CVE-2012-1234",
    "description": "Vulnerability in ABC software from Vendor XYZ",
    "created_by_ref": "identity—1621d4d4-b67d-41e3-9670-f01faf20d111",
    "external_references": [
        {
            "source_name": "cve",
            "external_id": "CVE-2012-1234"
        }
    ]
},
{
    "type": "relationship",
    "id": "relationship--6ce78886-1027-4800-9301-40c274fd472f",
    "spec_version": "2.1",
    "created": "2015-05-15T09:00:00.000Z",
```



```
    "modified": "2015-05-15T09:00:00.000Z",
    "relationship_type": "targets",
    "source_ref": "threat-actor–9a8a0d25-7636-429b-a99e-b2a73cd0f11f",
    "target_ref": "vulnerability--717cb1c9-eab3-4330-8340-e4858055aa80",
    "created_by_ref": "identity–1621d4d4-b67d-41e3-9670-f01faf20d111"
}
```

3.21.5 Required Consumer Persona Support

Adhere to section 2.3.2 based on the Required Producer Persona Support of the Vulnerability object. Additional required Consumer support for Vulnerability is listed in the table below.

Table 47 - Required Consumer Support for Vulnerability

Persona	Behavior
All Vulnerability Consumer personas	1. Consumer allows a user to receive STIX content with: a. An Identity of the Producer b. One or more Vulnerability objects c. One or more SROs or embedded relationships 2. For each STIX Object, the Consumer must be able to process the fields within the Identity object referenced by the **created_by_ref**, as enumerated in section 2.3.4 3. For each Vulnerability object, the Consumer can process the information about the Vulnerability fields to the user 4. For each Vulnerability object, the Consumer can process any related SDOs/SROs and associated fields

3.21.6 Consumer Test Case Data

The Consumer must be able to handle the test cases within the Vulnerability Producer Test Case Data, as per the requirements in section 3.21.5.

4 Persona Checklist

The following checklists summarize all tests that a persona (Producer or Consumer) must conform to within that persona.

4.1 Defined Persona Checklists

The use case requirements, as represented in Table 1, for the personas defined in section 1.2.1.1 are contained in this section.

4.1.1 Adversary Infrastructure Mapping (AIM)

For the purpose of this document, an AIM is a software or system, that consumes and produces STIX content, that is used to map out adversarial networks.

Any instance being qualified as an AIM must confirm test results for the following use cases.

Table 48 - Adversary Infrastructure Mapping (AIM) Test Verification List

Use Case	Section	Interoperability	Results
Attack Pattern Sharing | Consumer	3.1.6	Level 1	<fill in>
Campaign Sharing | Consumer	3.2.6	Level 1	<fill in>
Campaign Sharing | Producer	3.2.3	Level 1	<fill in>
Infrastructure Sharing | Producer	3.8.3	Level 1	<fill in>
Intrusion Set Sharing | Producer	3.9.3	Level 1	<fill in>
Intrusion Set Sharing | Consumer	3.9.6	Level 1	<fill in>
Location Sharing | Producer	3.10.3	Level 1	<fill in>
Note Sharing | Producer	3.13.3	Level 1	<fill in>
Threat Actor Sharing | Producer	3.18.3	Level 1	<fill in>
Threat Actor Sharing | Consumer	3.18.6	Level 1	<fill in>
Tool Sharing | Producer	3.19.3	Level 1	<fill in>
Attack Pattern Sharing | Producer	3.1.3	Level 2	<fill in>
Infrastructure Sharing | Consumer	3.8.6	Level 2	<fill in>
Location Sharing | Consumer	3.10.6	Level 2	<fill in>
Note Sharing | Consumer	3.13.6	Level 2	<fill in>

Tool Sharing | Consumer	3.19.6	Level 2	<fill in>

4.1.2 Local Infrastructure Mapping (LIM)

For the purpose of this document, a LIM is defined as a Software that scans local networks and provides STIX representations of these finds.

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

Table 49 - Local Infrastructure Mapping (LIM) Test Verification List

Use Case	Section	Interoperability	Results
Infrastructure Sharing | Producer	3.8.3	Level 1	<fill in>
Location Sharing | Producer	3.10.3	Level 1	<fill in>
Note Sharing | Producer	3.13.3	Level 1	<fill in>
Observed Data Sharing | Producer	3.14.3	Level 1	<fill in>
Vulnerability Sharing | Producer	3.21.3	Level 1	<fill in>
Infrastructure Sharing | Consumer	3.8.6	Level 2	<fill in>
Vulnerability Sharing | Consumer	3.21.6	Level 2	<fill in>

4.1.3 Malware Analysis System (MAS)

For the purpose of this document, a MAS is defined as a software instance, system, or set of systems that performs static and/or dynamic analysis of binary files and produces STIX content with this analysis information.

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

Table 50 - Malware Analysis System (MAS) Test Verification List

Use Case	Section	Interoperability	Results
Malware Analysis Sharing | Producer	3.11.3	Level 1	<fill in>
Malware Sharing | Producer	3.12.3	Level 1	<fill in>
Indicator Sharing | Producer	3.7.3	Level 2	<fill in>

4.1.4 Security Incident and Event Management (SIEM)

For the purpose of this document a SIEM is a software instance that acts as a Producer and/or Consumer of STIX 2.1 content. A SIEM that produces STIX content will typically create Indicators and other information about incidents. A SIEM that consumes STIX content will typically consume Sightings, Indicators.

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

Table 51 - Security Incident and Event Management (SIEM) Test Verification List

Use Case	Section	Interoperability	Results
Indicator Sharing | Consumer	3.7.6	Level 1	<fill in>
Observed Data Sharing | Producer	3.14.3	Level 1	<fill in>
Observed Data Sharing | Consumer	3.14.6	Level 1	<fill in>
Sighting Sharing | Producer	3.17.3	Level 1	<fill in>
Versioning-Creation | Producer	3.20.3	Level 1	<fill in>
Versioning-Modification | Producer	3.20.7	Level 1	<fill in>
Versioning-Revocation | Producer	3.20.11	Level 1	<fill in>
Note Sharing | Producer	3.13.3	Level 2	<fill in>
Note Sharing | Consumer	3.13.6	Level 2	<fill in>
Sighting Sharing | Consumer	3.17.6	Level 2	<fill in>
Versioning-Creation | Consumer	3.20.5	Level 2	<fill in>
Versioning-Modification | Consumer	3.20.9	Level 2	<fill in>
Versioning-Revocation | Consumer	3.20.13	Level 2	<fill in>

4.1.5 Threat Detection System (TDS)

For the purpose of this document a TDS is a software instance of any network product that monitors, detects and alerts such as Intrusion Detection Software (IDS), Endpoint Detection and Response (EDR) software, web proxy, etc. This is applicable for both Producers and Consumers.

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

Table 52 - Threat Detection System (TDS) Test Verification List

Use Case	Section	Interoperability	Results

Indicator Sharing | Consumer	3.7.6	Level 1	<fill in>
Sighting Sharing | Producer	3.17.3	Level 1	<fill in>
Sighting Sharing | Consumer	3.17.6	Level 1	<fill in>
Versioning-Creation | Producer	3.20.3	Level 1	<fill in>
Versioning-Modification | Producer	3.20.7	Level 1	<fill in>
Versioning-Revocation | Producer	3.20.11	Level 1	<fill in>
Course of Action Sharing | Consumer	3.4.6	Level 2	<fill in>
Observed Data Sharing | Consumer	3.14.6	Level 2	<fill in>
Versioning-Creation | Consumer	3.20.5	Level 2	<fill in>
Versioning-Modification | Consumer	3.20.9	Level 2	<fill in>
Versioning-Revocation | Consumer	3.20.13	Level 2	<fill in>

4.1.6 Threat Intelligence Platform (TIP)

For the purpose of this document, a TIP is defined as a software instance that acts as a Producer and/or Consumer of STIX 2.1 content primarily used to aggregate, refine and share intelligence with other machines or security personnel operating other security infrastructure.

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

Table 53 - Threat Intelligence Platform (TIP) Test Verification List

Use Case	Section	Interoperability	Results
Attack Pattern Sharing | Producer	3.1.3	Level 1	<fill in>
Attack Pattern Sharing | Consumer	3.1.6	Level 1	<fill in>
Campaign Sharing | Producer	3.2.3	Level 1	<fill in>
Campaign Sharing | Consumer	3.2.6	Level 1	<fill in>
Confidence Sharing | Producer	3.3.3	Level 1	<fill in>
Confidence Sharing | Consumer	3.3.6	Level 1	<fill in>
Course of Action Sharing | Producer	3.4.3	Level 1	<fill in>

Course of Action Sharing | Consumer	3.4.6	Level 1	<fill in>
Data Markings Sharing | Producer	3.5.3	Level 1	<fill in>
Data Markings Sharing | Consumer	3.5.6	Level 1	<fill in>
Indicator Sharing | Producer	3.7.3	Level 1	<fill in>
Indicator Sharing | Consumer	3.7.6	Level 1	<fill in>
Intrusion Set Sharing | Producer	3.9.3	Level 1	<fill in>
Intrusion Set Sharing | Consumer	3.9.6	Level 1	<fill in>
Malware Analysis Sharing | Consumer	3.11.6	Level 1	<fill in>
Malware Sharing | Producer	3.12.3	Level 1	<fill in>
Malware Sharing | Consumer	3.12.6	Level 1	<fill in>
Note Sharing | Producer	3.13.3	Level 1	<fill in>
Note Sharing | Consumer	3.13.6	Level 1	<fill in>
Observed Data Sharing | Consumer	3.14.6	Level 1	<fill in>
Opinion Sharing | Producer	3.15.3	Level 1	<fill in>
Opinion Sharing | Consumer	3.15.6	Level 1	<fill in>
Report Sharing | Producer	3.16.3	Level 1	<fill in>
Report Sharing | Consumer	3.16.6	Level 1	<fill in>
Threat Actor Sharing | Producer	3.18.3	Level 1	<fill in>
Threat Actor Sharing | Consumer	3.18.6	Level 1	<fill in>
Versioning-Creation | Producer	3.20.3	Level 1	<fill in>
Versioning-Creation | Consumer	3.20.5	Level 1	<fill in>
Versioning-Modification | Producer	3.20.7	Level 1	<fill in>
Versioning-Modification | Consumer	3.20.9	Level 1	<fill in>
Versioning-Revocation | Producer	3.20.11	Level 1	<fill in>
Versioning-Revocation | Consumer	3.20.13	Level 1	<fill in>

Vulnerability Sharing | Producer	3.21.3	Level 1	<fill in>
Vulnerability Sharing | Consumer	3.21.6	Level 1	<fill in>
Location Sharing | Producer	3.10.3	Level 2	<fill in>
Location Sharing | Consumer	3.10.6	Level 2	<fill in>
Observed Data Sharing | Producer	3.14.3	Level 2	<fill in>
Sighting Sharing | Producer	3.17.3	Level 2	<fill in>
Sighting Sharing | Consumer	3.17.6	Level 2	<fill in>

4.1.7 Threat Mitigation System (TMS)

A TMS is a software instance that acts on Course of Action and data from other threat mitigations such as a firewall, IPS, Endpoint Detection and Response (EDR) software, etc. This is applicable for both Producers and Consumers.

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

Table 54 - Threat Mitigation System (TMS) Test Verification List

Use Case	Section	Interoperability	Results
Course of Action Sharing | Consumer	3.4.6	Level 1	<fill in>
Indicator Sharing | Consumer	3.7.6	Level 1	<fill in>
Sighting Sharing | Consumer	3.17.6	Level 1	<fill in>
Versioning-Creation | Producer	3.20.3	Level 1	<fill in>
Versioning-Modification | Producer	3.20.7	Level 1	<fill in>
Versioning-Revocation | Producer	3.20.11	Level 1	<fill in>
Observed Data Sharing | Consumer	3.14.6	Level 2	<fill in>
Versioning-Creation | Consumer	3.20.5	Level 2	<fill in>
Versioning-Modification | Consumer	3.20.9	Level 2	<fill in>
Versioning-Revocation | Consumer	3.20.13	Level 2	<fill in>

4.2 Generic Persona Checklists

The use case requirements, as specified in section 2.2, for the generic personas in section 1.2.1.2 are contained in this section.

4.2.1 STIX Consumer (SXC)

For the purpose of this document, a SXC is a software instance that consumes STIX 2.1 content in order to perform translations to domain-specific formats consumable by enforcement and/or detection systems that do not natively support STIX 2.1. A SXC will typically consume STIX content but may not produce any STIX content itself.

Any software instance being qualified as a SXC must confirm test results for the following use cases. Note, in addition to those tests designated as “Mandatory” in the below table, to qualify as a SXC, a software instance will have to confirm test results for all of the Consumer tests of at least one additional use case. And as explained in section 2.2, a software instance will be considered a SXC only for the use cases it supports.

Table 55 - STIX Consumer (SXC) Test Verification List

Use Case	Section	Verification	Results
Attack Pattern Sharing | Consumer	3.1.6	Optional	<fill in>
Campaign Sharing | Consumer	3.2.6	Optional	<fill in>
Confidence Sharing | Consumer	3.3.6	Mandatory	<fill in>
Course of Action Sharing | Consumer	3.4.6	Optional	<fill in>
Data Markings Sharing | Consumer	3.5.6	Mandatory	<fill in>
Grouping Sharing | Consumer	3.6.6	Optional	<fill in>
Indicator Sharing | Consumer	3.7.6	Optional	<fill in>
Infrastructure Sharing | Consumer	3.8.6	Optional	<fill in>
Intrusion Set Sharing | Consumer	3.9.6	Optional	<fill in>
Location Sharing | Consumer	3.10.6	Optional	<fill in>
Malware Analysis Sharing | Consumer	3.11.6	Optional	<fill in>
Malware Sharing | Consumer	3.12.6	Optional	<fill in>
Note Sharing | Consumer	3.13.6	Optional	<fill in>
Observed Data Sharing | Consumer	3.14.6	Optional	<fill in>

Opinion Sharing | Consumer	3.15.6	Optional	<fill in>
Report Sharing | Consumer	3.16.6	Optional	<fill in>
Sighting Sharing | Consumer	3.17.6	Optional	<fill in>
Threat Actor Sharing | Consumer	3.18.6	Optional	<fill in>
Tool Sharing | Consumer	3.19.6	Optional	<fill in>
Versioning-Creation | Consumer	3.20.5	Mandatory	<fill in>
Versioning-Modification | Consumer	3.20.9	Mandatory	<fill in>
Versioning-Revocation | Consumer	3.20.13	Mandatory	<fill in>
Vulnerability Sharing | Consumer	3.21.6	Optional	<fill in>

4.2.2 STIX Producer (SXP)

For the purpose of this document, a SXP is a software instance that acts as a Producer of STIX 2.1 content.

Any software instance being qualified as a SXP must confirm test results for the following use cases. Note, in addition to those tests designated as “Mandatory” in the below table, to qualify as a SXP, a software instance will have to confirm test results for all of the Producer tests of at least one additional use case. And as explained in section 2.2, a software instance will be considered a SXP only for the use cases it supports.

Table 56 - STIX Producer (SXP) Test Verification List

Use Case	Section	Verification	Results
Attack Pattern Sharing | Producer	3.1.3	Optional	<fill in>
Campaign Sharing | Producer	3.2.3	Optional	<fill in>
Confidence Sharing | Producer	3.3.3	Mandatory	<fill in>
Course of Action Sharing | Producer	3.4.3	Optional	<fill in>
Data Markings Sharing | Producer	3.5.3	Mandatory	<fill in>
Grouping Sharing | Producer	3.6.3	Optional	<fill in>
Indicator Sharing | Producer	3.7.3	Optional	<fill in>
Infrastructure Sharing | Producer	3.8.3	Optional	<fill in>

Intrusion Set Sharing | Producer	3.9.3	Optional	<fill in>
Location Sharing | Producer	3.10.3	Optional	<fill in>
Malware Analysis Sharing | Producer	3.11.3	Optional	<fill in>
Malware Sharing | Producer	3.12.3	Optional	<fill in>
Note Sharing | Producer	3.13.3	Optional	<fill in>
Observed Data Sharing | Producer	3.14.3	Optional	<fill in>
Opinion Sharing | Producer	3.15.3	Optional	<fill in>
Report Sharing | Producer	3.16.3	Optional	<fill in>
Sighting Sharing | Producer	3.17.3	Optional	<fill in>
Threat Actor Sharing | Producer	3.18.3	Optional	<fill in>
Tool Sharing | Consumer	3.19.3	Optional	<fill in>
Versioning-Creation | Producer	3.20.3	Mandatory	<fill in>
Versioning-Modification | Producer	3.20.7	Mandatory	<fill in>
Versioning-Revocation | Producer	3.20.12	Mandatory	<fill in>
Vulnerability Sharing | Producer	3.21.3	Optional	<fill in>

Appendix A. Acknowledgments

Interoperability Subcommittee Chairs

Stephen Russett, Cyber Threat Intelligence Network, Inc.
Michael Rosa, DHS
Marlon Taylor, DHS
Jason Keirstead, IBM
Allan Thomson, Individual
Rajesh Patil, LookingGlass
Justin Stewart, LookingGlass

Special Thanks

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

Patrick Maroney, AT&T
Mark Davidson, Celerium, Inc.
Christian Hunt, Copado
Andrew Storms, Copado
Jane Ginn, Cyber Threat Intelligence Network, Inc. (CTIN)
Ryusuke Masuoka, Fujitsu Limited
Toshitaka Satomi, Fujitsu Limited
Roseann Guttierrez, IBM
Chris Lenk, MITRE Corporation
Daniel Haynes, MITRE Corporation
Dez Beck, MITRE Corporation
Ivan Kirillov, MITRE Corporation
Rich Piazza, MITRE Corporation
Jeffrey Mates, US Department of Defense (DoD)

Participants

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

First	Last	Organization
Casey	Carr	Accenture
Ray-yu	Chang	Accenture

Robert	Coderre	Accenture
Robert	Keith	Accenture
Curtis	Kostrosky	Accenture
Kyle	Maxwell	Accenture
Ralph	Thomas	Accenture
Florian	Skopik	AIT Austrian Institute of Technology
Greg	Fischer	Anomali
Wei	Huang	Anomali
Russell	Matbouli	Anomali
Hugh	Njemanze	Anomali
Katie	Pelusi	Anomali
Patrick	Maroney	AT&T
Dean	Thompson	Australia and New Zealand Banking Group (ANZ Bank)
Justin	Dobosh	Bank of America
Radu	Marian	Bank of America
Tony	Pham	Bank of America
Charles	Yarbrough	Carnegie Mellon University

Trey	Darley	CCB/CERT.be
Alexandre	Dulaunoy	CIRCL
Andras	Iklody	CIRCL
Christian	Studer	CIRCL
Raphaël	Vinot	CIRCL
Syam	Appala	Cisco Systems
Ted	Bedwell	Cisco Systems
Craig	Brozefsky	Cisco Systems
Caitlin	Huey	Cisco Systems
Henry	Peltokangas	Cisco Systems
Pavan	Reddy	Cisco Systems
Omar	Santos	Cisco Systems
Sam	Taghavi Zargar	Cisco Systems
Jyoti	Verma	Cisco Systems
Andrew	Windsor	Cisco Systems
Kevin	Chan	Copado
Kelly	Cullinane	Copado

John-Mark	Gurney	Copado
Christian	Hunt	Copado
Daniel	Riedel	Copado
Andrew	Storms	Copado
Tim	Hudson	Cryptsoft Pty Ltd.
Arsalan	Iqbal	CTM360
Jane	Ginn	Cyber Threat Intelligence Network, Inc. (CTIN)
Bret	Jordan	Cyber Threat Intelligence Network, Inc. (CTIN)
Ben	Ottoman	Cyber Threat Intelligence Network, Inc. (CTIN)
David	Powell	Cyber Threat Intelligence Network, Inc. (CTIN)
Andreas	Sfakianakis	Cyber Threat Intelligence Network, Inc. (CTIN)
Nick	Sturgeon	Cyber Threat Intelligence Network, Inc. (CTIN)
Michael	Butt	Cyware Labs
Utkarsh	Garg	Cyware Labs
Anuj	Goel	Cyware Labs
Avkash	Kathiriya	Cyware Labs
Andrew	Nau	Cyware Labs

Timothy	Casey	DarkLight, Inc.
Ryan	Hohimer	DarkLight, Inc.
Ryan	Joyce	DarkLight, Inc.
Paul	Patrick	DarkLight, Inc.
Andrew	Byrne	Dell
joe	laugle	Dell
Ravi	Sharda	Dell
Will	Urbanski	Dell
David	Ailshire	DHS Office of Cybersecurity and Communications (CS&C)
Steven	Fox	DHS Office of Cybersecurity and Communications (CS&C)
Taneika	Hill	DHS Office of Cybersecurity and Communications (CS&C)
Evette	Maynard-Noel	DHS Office of Cybersecurity and Communications (CS&C)
Jackie Eun	Park	DHS Office of Cybersecurity and Communications (CS&C)
Sean	Sobieraj	DHS Office of Cybersecurity and Communications (CS&C)
Marlon	Taylor	DHS Office of Cybersecurity and Communications (CS&C)
Preston	Werntz	DHS Office of Cybersecurity and Communications (CS&C)
Joep	Gommers	EclecticIQ

Sergey	Polzunov	EclecticIQ
Alexander	Shamparov	EclecticIQ
Zed	Tan	EclecticIQ
Aukjan	van Belkum	EclecticIQ
Raymon	van der Velde	EclecticIQ
Joseph	Woodruff	EclecticIQ
Ben	Sooter	Electric Power Research Institute (EPRI)
Carolina	Canales-Valenzuela	Ericsson
Chris	Ricard	Financial Services Information Sharing and Analysis Center (FS-ISAC)
Charles	White	Fornetix
Yasutaka	Ebihara	Fujitsu Limited
Ryusuke	Masuoka	Fujitsu Limited
Derek	Northrope	Fujitsu Limited
Toshitaka	Satomi	Fujitsu Limited
Koji	Yamada	Fujitsu Limited
Robert	van Engelen	Genivia
Mark	Risher	Google Inc.

Naoki	Hayashi	Hitachi, Ltd.
Yoshihide	Kawada	Hitachi, Ltd.
Jun	Nakanishi	Hitachi, Ltd.
Kazuo	Noguchi	Hitachi, Ltd.
Akihito	Sawada	Hitachi, Ltd.
Yutaka	Takami	Hitachi, Ltd.
Masato	Terada	Hitachi, Ltd.
Xiaoyu	Ge	Huawei Technologies Co., Ltd.
Ho	Hock, William	Huawei Technologies Co., Ltd.
Dong	Huang	Huawei Technologies Co., Ltd.
David	Webber	Huawei Technologies Co., Ltd.
Mohamed	Badr	IBM
Eldan	Ben-Haim	IBM
Roseann	Guttierrez	IBM
Sandra	Hernandez	IBM
Jason	Keirstead	IBM
Chenta	Lee	IBM

John	Morris	IBM
Devesh	Parekh	IBM
Emily	Ratliff	IBM
Nick	Rossmann	IBM
Laura	Rusu	IBM
frank	schaffa	IBM
garret	taylor	IBM
Ron	Williams	IBM
Ashwini	Jarral	IJIS Institute
Michele	Drgon	Individual
Joerg	Eschweiler	Individual
Elysa	Jones	Individual
Terry	MacDonald	Individual
Anthony	Rutkowski	Individual
Allan	Thomson	Individual
James	Cabral	InfoTrack US
Jorge	Aviles	Johns Hopkins University Applied Physics Laboratory

Cory	Huyssoon	Johns Hopkins University Applied Physics Laboratory
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
Nathan	Reller	Johns Hopkins University Applied Physics Laboratory
Pamela	Smith	Johns Hopkins University Applied Physics Laboratory
Russell	Culpepper	Kaiser Permanente
Beth	Pumo	Kaiser Permanente
Scott	Robertson	Kaiser Permanente
Michael	Slavick	Kaiser Permanente
Javier	Garcia Robles	LookingGlass
Himanshu	Kesar	LookingGlass
Rajesh	Patil	LookingGlass
Vlad	Serban	LookingGlass
Chris	Wood	LookingGlass
Kent	Landfield	McAfee

Desiree	Beck	Mitre Corporation
Jen	Burns	Mitre Corporation
Michael	Chisholm	Mitre Corporation
Mike	Cokus	Mitre Corporation
Sam	Cornwell	Mitre Corporation
Kartikey	Desai	Mitre Corporation
Danny	Haynes	Mitre Corporation
Chris	Lenk	Mitre Corporation
Bob	Natale	Mitre Corporation
Nicole	Parrish	Mitre Corporation
Richard	Piazza	Mitre Corporation
Larry	Rodrigues	Mitre Corporation
Zach	Rush	Mitre Corporation
Jon	Salwen	Mitre Corporation
Matt	Scola	Mitre Corporation
Richard	Struse	Mitre Corporation
Alex	Tweed	Mitre Corporation

Emmanuelle	Vargas-Gonzalez	Mitre Corporation
Bryan	Worrell	Mitre Corporation
John	Wunder	Mitre Corporation
Jackson	Wynn	Mitre Corporation
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
Michael	Rosa	National Security Agency
Daichi	Hasumi	NEC Corporation
Takahiro	Kakumaru	NEC Corporation
Lauri	Korts-Pärn	NEC Corporation
Drew	Varner	NineFX, Inc.
Stephen	Banghart	NIST

Scott	Carlisle	Northrop Grumman
James	Crossland	Northrop Grumman
Ivan	Diaz	Northrop Grumman
Anthony	Lay	Northrop Grumman
Qem	Lumi	Northrop Grumman
Robert	Van Dyk	Northrop Grumman
Cheolho	Lee	NSR
James Bryce	Clark	OASIS
Chet	Ensign	OASIS
Web	Master	OASIS
CTI	Mirror	OASIS
cti-cybox	Mirror	OASIS
cti-stix	Mirror	OASIS
cti-taxii	Mirror	OASIS
Dee	Schur	OASIS
Patrick	Bredenberg	Oracle
Johnny	Gau	Oracle

Sunil	Ravipati	Oracle
Joel	Myhre	Pacific Disaster Center
Ryan	Clough	Palo Alto Networks
Ryan	Olson	Palo Alto Networks
Jason	Liu	Peraton
Stephan	Relitz	Peraton
Altaz	Valani	Security Compass
David	Bizeul	SEKOIA
Georges	Bossert	SEKOIA
Duncan	Sparrell	sFractal Consulting LLC
Marco	Caselli	Siemens AG
Jonas	Plum	Siemens AG
Jeremy	Berthelet	Sopra Steria Group
Alexandre	Cabrol Perales	Sopra Steria Group
Adam	Wyner	Swansea University
Alan	Steer	TELUS
Srujan	Kotikela	Texas A&M University-Commerce

Andrew	Gidwani	ThreatConnect, Inc.
Cole	Iliff	ThreatConnect, Inc.
Andrew	Pendergast	ThreatConnect, Inc.
Jason	Spies	ThreatConnect, Inc.
Alejandro	Valdivia	ThreatConnect, Inc.
Haig	Colter	ThreatQuotient, Inc.
Jason	Avery	Trend Micro
Ed	Cabrera	Trend Micro
Ziv	Chang	Trend Micro
David	Girard	Trend Micro
Robert	McArdle	Trend Micro
Brandon	Niemczyk	Trend Micro
Jessie	Chuang	TWNCERT
Julie	Wang	TWNCERT
Vasileios	Mavroeidis	University of Oslo
Ulrik	Palmstrøm	University of Oslo
Jeffrey	Mates	US Department of Defense (DoD)

Keven	Ates	US Federal Bureau of Investigation

Appendix B. Revision History

Revision	Date	Editor	Changes Made
01	2018-04-13	Justin Stewart	Imported into Google Docs Update format to match the TAXII Interoperability document
02	2021-09-24	Kartikey Desai	Updated use cases to use STIX 2.1. Added new use cases for 2.1. Addressed STIX 2.1 conformance requirements. Updated Terminology and Personas. Provided new personas. Renamed DFP and TIS personas. Removed certification process instructions.
03	2021-10-08	Marlon Taylor	Persona Checklists split between Defined personas and Generic personas. Modified Defined persona checklists to use Interoperability levels instead of Optional/Mandatory. Added clarification about interoperability between personas of different levels. Added Producer examples to some use cases.