STIX 2.0 Specification

Objects

Version 2.0-draft-3

Document Table of Contents

[​1.​ STIX Domain Objects](#h.se145spjcwnt)

[​1.1.​ Attack Pattern](#h.axjijf603msy)

[​1.1.1.​ Properties](#h.4ohsa4pay4h4)

[​1.1.2.​ Relationships](#h.e33ahkddw0q1)

[​1.1.3.​ Examples](#h.eifqps95z4u2)

[​1.2.​ Campaign](#h.pcpvfz4ik6d6)

[​1.2.1.​ Properties](#h.vvysvm8mt434)

[​1.2.2.​ Relationships](#h.q63x7a5uhc8e)

[​1.2.3.​ Examples](#h.7wqmohs96hf3)

[​1.3.​ Course of Action](#h.uilqxp59env4)

[​1.3.1.​ Properties](#h.d5yf99f0a230)

[​1.3.2.​ Relationships](#h.bokr6guil91f)

[​1.3.3.​ Examples](#h.aebevw4ns9hb)

[​1.4.​ Incident](#h.6cgc3vm9y3gp)

[​1.4.1.​ Properties](#h.8etbi9afk5u9)

[​1.4.2.​ Relationships](#h.dtmaowxsidg2)

[​1.4.3.​ Examples](#h.d7pawar6vnds)

[​1.5.​ Indicator](#h.muftrcpnf89v)

[​1.5.1.​ Properties](#h.wfiae74706sw)

[​1.5.2.​ Relationships](#h.oaq5jdro8yfr)

[​1.5.3.​ Examples](#h.9q4qw2gyp6dk)

[​1.6.​ Infrastructure](#h.maky5z1n51ds)

[​1.6.1.​ Properties](#h.a2d23bd095vb)

[​1.6.2.​ Relationships](#h.qemxsqasxof9)

[​1.6.3.​ Examples](#h.mllp3t1b3l79)

[​1.7.​ Intrusion Set](#h.5ol9xlbbnrdn)

[​1.7.1.​ Properties](#h.ticprjb32bc4)

[​1.7.2.​ Relationships](#h.ld519r8v3oie)

[​1.7.3.​ Example](#h.v96kivialg35)

[​1.8.​ Malware](#h.s5l7katgbp09)

[​1.8.1.​ Properties](#h.gc4ooz6oaz7y)

[​1.8.2.​ Basic Malware Analysis Type](#h.lgh3x56z63m6)

[​1.8.3.​ Relationships](#h.wete2ohmtz4y)

[​1.8.4.​ Examples](#h.bnz4nljdxw5b)

[​1.9.​ Observed Data](#h.k5fndj2c7c1k)

[​1.9.1.​ Properties](#h.h1590esrzg5f)

[​1.9.2.​ Relationships](#h.oohyqxufcj2b)

[​1.9.3.​ Examples](#h.606ggomo2933)

[​1.10.​ Report](#h.n8bjzg1ysgdq)

[​1.10.1.​ Properties](#h.ha4fpad0r9pf)

[​1.10.2.​ Relationships](#h.u1alc2ppehw4)

[​1.10.3.​ Examples](#h.sqjujznqckyn)

[​1.11.​ Source](#h.wh296fiwpklp)

[​1.11.1.​ Properties](#h.ru8fmldl2p6w)

[​1.11.2.​ Relationships](#h.l0fpkltzfsa0)

[​1.11.3.​ Examples](#h.9gjfk0cyi2vw)

[​1.12.​ Threat Actor](#h.k017w16zutw)

[​1.12.1.​ Properties](#h.2wowmlcbkqst)

[​1.12.2.​ Relationships](#h.rddgtiv420uc)

[​1.12.3.​ Examples](#h.slv7cz7xqkpd)

[​1.13.​ Tool](#h.z4voa9ndw8v)

[​1.13.1.​ Properties](#h.m21z3a1f3lou)

[​1.13.2.​ Relationships](#h.d8kskhd6k7bd)

[​1.13.3.​ Examples](#h.z4t7b9qvdfz0)

[​1.14.​ Victim Target](#h.15hpblqi5u59)

[​1.14.1.​ Properties](#h.t2la72srl3hl)

[​1.14.2.​ Relationships](#h.cmilsm4qh54x)

[​1.14.3.​ Examples](#h.7ben8xacjnf1)

[​1.15.​ Vulnerability](#h.q5ytzmajn6re)

[​1.15.1.​ Properties](#h.d9f0iay06wtx)

[​1.15.2.​ Relationships](#h.ibz8ltydjosa)

[​1.15.3.​ Examples](#h.qw1ravdvh8p8)

[​2.​ Relationship Objects](#h.x5yinpqwezlv)

[​2.1.​ Relationship](#h.e2e1szrqfoan)

[​2.1.1.​ Named Relationships Summary](#h.sypzg7rvdvc1)

[​2.1.2.​ Properties](#h.2y6ddegzfg0)

[​2.1.3.​ Relationships](#h.pw1glqtz6mh2)

[​2.2.​ Sighting](#h.a795guqsap3r)

[​2.2.1.​ Properties](#h.7p0n81ikux8f)

[​2.2.2.​ Relationships](#h.jwntpfv8ddt4)

[​2.2.3.​ Examples](#h.evh1nihwcokv)

[​3.​ Bundle](#h.anyynaiz47ix)

[​3.0.1.​ Properties](#h.nuwp4rox8c7r)

[​3.0.2.​ Relationships](#h.p23hxnekt294)

[​3.0.3.​ Examples](#h.36vl4li2t9eo)

# ​1.​ STIX Domain Objects

This specification defines a number of SDOs, each of which corresponds to a unique concept commonly represented in cyber threat intelligence. Using the building blocks of SDOs alongside STIX relationships, individuals can create and share broad and comprehensive cyber threat intelligence.

Property information, relationship information, and examples are provided for each SDO defined below. Property information includes common properties as well as properties that are specific to each SDO. Relationship information includes embedded relationships (e.g., **created\_by\_ref**), common relationships (e.g., related-to), and SDO-specific relationships. Forward relationships (i.e., relationships *from* the SDO to other SDOs) are fully defined, while reverse relationships (i.e., relationships *to* the SDO from other SDOs) are duplicated for convenience.

Some SDOs are similar and can be grouped together into categories. Attack Pattern, Malicious Infrastructure, Malware, and Tool can all be considered types of TTPs (tactics, techniques, and procedures): they describe behaviors and resources that attackers use to carry out their attacks. Campaign, Intrusion Set, and Threat Actor, similarly, all describe attacker groupings: they represent information about why adversaries carry out attacks and how they organize themselves.

## ​1.1.​ Attack Pattern

**Type Name:** attack-pattern

Attack Patterns are a type of TTP that describe ways that adversaries attempt to compromise targets. Attack Patterns are used to help categorize attacks, generalize specific attacks to the patterns that they follow, and provide detailed information about how attacks are performed. An example of an 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: spear phishing as practiced by a particular threat actor (i.e. they might generally say that the target won a contest) can also be an Attack Pattern.

The Attack Pattern SDO contains textual descriptions of the pattern along with references to externally-defined taxonomies of attacks such as CAPEC <TODO: need reference>. Relationships from Attack Pattern can be used to relate it to what it targets (Vulnerabilities and Victim Targets) and which tools and malware use it (Tool and Malware).

### ​1.1.1.​ Properties

|  |  |  |
| --- | --- | --- |
| **Common Properties** | | |
| **type, id, created\_by\_ref, created, modified, version, revoked, labels, external\_references, object\_markings\_refs, granular\_markings** | | |
| **Attack Pattern Specific Properties** | | |
| **name, description, kill\_chain\_phases** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this field **MUST** be attack-pattern |
| **external\_references**  (optional) | list of type external-reference | A list of external references which refer to non-STIX information. This field **MAY** be used to provide one or more Attack Pattern identifiers, such as a CAPEC ID. When specifying a CAPEC ID, the **source** field of the external reference **MUST** be set to capec and the **external\_id** field **MUST** be formatted as CAPEC-[id]. |
| **name** (required) | string | A name used to identify the Attack Pattern. |
| **description** (optional) | string | A description that provides more details and context about the Attack Pattern, potentially including its purpose and its key characteristics. |
| **kill\_chain\_phases** (optional) | list of type kill-chain-phase | The list of Kill Chain phases for which this Attack Pattern is used. |

### ​1.1.2.​ Relationships

These are the relationships explicitly defined between the Attack Pattern object and other objects. The first section lists the embedded relationships by property name along with their corresponding target. The rest of the table identifies the relationships that can be made from this object by way of the Relationship Object. The reverse relationships (relationships "to" this object) are included as a convenience. For their definitions, please see the objects for which they represent a "from" relationship.

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship name or, as with open vocabularies, user-defined names.

|  |  |  |  |
| --- | --- | --- | --- |
| **Embedded Relationships** | | | |
| **created\_by\_ref** | | source | |
| **object\_markings\_refs** | | marking-definition | |
| **Common Relationships** | | | |
| duplicate-of, derived-from, related-to | | | |
| **Source** | **Name** | **Target** | **Description** |
| attack-pattern | targets | victim-target, vulnerability | This Relationship describes that this Attack Pattern typically targets the type of victims or vulnerability represented by the related Victim Target or Vulnerability object.  For example, a targets Relationship linking an Attack Pattern for SQL injection to a Victim Target representing domain administrators means that the form of SQL Injection characterized by the Attack Pattern targets domain administrators in order to achieve its objectives.  Another example is a Relationship linking an Attack Pattern for SQL injection to a Vulnerability in blogging software means that the particular SQL injection attack exploits that vulnerability. |
| attack-pattern | uses | malware, tool | This Relationship describes that the related Malware or Tool is used to perform the behavior identified in the Attack Pattern.  For example, a uses Relationship linking an Attack Pattern for DDoS to a Tool for LOIC indicates that the tool can be used to perform those DDoS attacks. |
| **Reverse Relationships** | | | |
| indicator | indicates | attack-pattern | See forward relationship for definition. |
| course-of-action | mitigates | attack-pattern | See forward relationship for definition. |
| campaign, intrusion-set, threat-actor | uses | attack-pattern | See forward relationship for definition. |

### ​1.1.3.​ Examples

**A generic attack pattern for spear phishing, referencing CAPEC**

{

"type": "attack-pattern",

"id": "attack-pattern--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",

"created": "2016-05-12T08:17:27.000000Z",

"modified": "2016-05-12T08:17:27.000000Z",

"version": 1,

"name": "Spear Phishing",

"description": "...",

"external\_references": [

{

"source": "capec",

"id": "CAPEC-49"

}

]

}

**A specific attack pattern for a particular form of spear phishing, referencing CAPEC**

[

{

"type": "attack-pattern",

"id": "attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5",

"created": "2016-05-12T08:17:27.000000Z",

"modified": "2016-05-12T08:17:27.000000Z",

"version": 1,

"name": "Spear Phishing as Practiced by Adversary X",

"description": "A particular form of spear phishing where the attacker claims that the target had won a contest, including personal details, to get them to click on a link.",

"external\_references": [

{

"source": "capec",

"id": "CAPEC-49"

}

]

},

{

"type": "relationship",

"id": "relationship--57b56a43-b8b0-4cba-9deb-34e3e1faed9e",

"created": "2016-05-12T08:17:27.000000Z",

"modified": "2016-05-12T08:17:27.000000Z",

"version": 1,

"name": "uses",

"source\_ref": "intrusion-set--0c7e22ad-b099-4dc3-b0df-2ea3f49ae2e6",

"target\_ref": "attack-pattern--7e33a43e-e34b-40ec-89da-36c9bb2cacd5"

},

{

"type": "intrusion-set",

"id": "intrusion-set--0c7e22ad-b099-4dc3-b0df-2ea3f49ae2e6",

"created": "2016-05-12T08:17:27.000000Z",

"modified": "2016-05-12T08:17:27.000000Z",

"version": 1,

"name": "Adversary X"

}

]

## ​1.2.​ Campaign

**Type Name:** campaign

A Campaign is a grouping of adversary behavior that describes a set of malicious activities or attacks (sometimes called waves) 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.

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.

### ​1.2.1.​ Properties

|  |  |  |
| --- | --- | --- |
| **Common Properties** | | |
| **type, id, created\_by\_ref, created, modified, version, revoked, labels, external\_references, object\_markings\_refs, granular\_markings** | | |
| **Campaign Specific Properties** | | |
| **name, description, aliases, first\_seen, first\_seen\_precision, objective** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this field **MUST** be campaign |
| **name** (required) | string | A name used to identify the Campaign. |
| **description** (optional) | string | A description that provides more details and context about the Campaign, potentially including its purpose and its key characteristics. |
| **aliases** (optional) | list of type string | Alternative names used to identify this Campaign |
| **first\_seen** (optional) | timestamp | The time that his Campaign was first seen. |
| **first\_seen\_precision** (optional) | timestamp-precision | The precision of the **first\_seen** timestamp. |
| **objective** (optional) | string | This field defines the Campaign’s primary goal, objective, desired outcome, or intended effect — what the Threat Actor hopes to accomplish with this Campaign. |

### ​1.2.2.​ Relationships

These are the relationships explicitly defined between the Campaign object and other objects. The first section lists the embedded relationships by property name along with their corresponding target. The rest of the table identifies the relationships that can be made from this object by way of the Relationship Object. The reverse relationships (relationships "to" this object) are included as a convenience. For their definitions, please see the objects for which they represent a "from" relationship.

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship name or, as with open vocabularies, user-defined names.

|  |  |  |  |
| --- | --- | --- | --- |
| **Embedded Relationships** | | | |
| **created\_by\_ref** | | source | |
| **object\_markings\_refs** | | marking-definition | |
| **Common Relationships** | | | |
| duplicate-of, derived-from, related-to | | | |
| **Source** | **Name** | **Target** | **Description** |
| campaign | attributed-to | intrusion-set, threat-actor | This Relationship describes that the Intrusion Set or Threat Actor is involved in carrying out the Campaign.  For example, an attributed-to Relationship from the Glass Gazelle Campaign to the Urban Fowl threat actor means that the actor carried out or was involved in some of the activity described by the campaign. |
| campaign | targets | victim-target, vulnerability | This Relationship describes that the Campaign uses exploits of the related Vulnerability or targets the type of victims described by the related Victim Target.  For example, a targets Relationship from the Glass Gazelle Campaign to a Vulnerability in a blogging platform indicates that attacks performed as part of Glass Gazelle often exploit that Vulnerability.  Similarly, a targets Relationship from the Glass Gazelle Campaign to a Victim Target describing the energy sector in the United States means that the Campaign typically carries out attacks against targets in that sector. |
| campaign | uses | attack-pattern, infrastructure, malware, tool | This Relationship describes that attacks carried out as part of the campaign typically use the related Attack Pattern, Malware, or Tool.  For example, a uses Relationship from the Glass Gazelle Campaign to the xInject Malware indicate that xInject is often used during attacks attributed to that Campaign. |
| **Reverse Relationships** | | | |
| incident | attributed-to | campaign | See forward relationship for definition. |
| indicator | indicates | campaign | See forward relationship for definition. |

### ​1.2.3.​ Examples

{

"type": "campaign",

"id": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",

"created\_by\_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",

"created": "2016-04-06T20:03:48Z",

"modified": "2016-04-06T20:03:48Z",

"version": 1,

"name": "Green Group Attacks Against Finance",

"description": "Campaign by Green Group against a series of targets in the financial services sector."

}

​

## ​1.3.​ Course of Action

**Type Name:** course-of-action

A Course of Action is an action taken either to prevent an attack or to respond to an attack that is in progress. They may describe technical, automatable responses (applying patches, reconfiguring firewalls) but can also describe higher level actions like employee training or policy changes. For example, a course of action to mitigate a vulnerability could describe applying the patch that fixes it.

The Course of Action SDO contains a textual description of the action; a reserved **action** field also serves as placeholder for future inclusion of machine automatable courses of action. Relationships from the Course of Action can be used to link it to the Vulnerabilities or behaviors (Tool, Malware, Attack Pattern) that it mitigates.

### ​1.3.1.​ Properties

|  |  |  |
| --- | --- | --- |
| **Common Properties** | | |
| **type, id, created\_by\_ref, created, modified, version, revoked, labels, external\_references, object\_markings\_refs, granular\_markings** | | |
| **Course of Action Specific Properties** | | |
| **name, description, action** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this field **MUST** be course-of-action |
| **labels** (required) | list of type open-vocab | This property is a list of classifications for the Course of Action.  This is an open vocabulary and values **SHOULD** come from the course-of-action-label-ov vocabulary. |
| **name** (required) | string | A name used to identify the Course of Action |
| **description** (optional) | string | A description that provides more details and context about the Course of Action, potentially including its purpose and its key characteristics. |
| **action** (reserved) | RESERVED | RESERVED - To capture structured/automated courses of action. |

### ​1.3.2.​ Relationships

These are the relationships explicitly defined between the Course of Action object and other objects. The first section lists the embedded relationships by property name along with their corresponding target. The rest of the table identifies the relationships that can be made from this object by way of the Relationship Object. The reverse relationships (relationships "to" this object) are included as a convenience. For their definitions, please see the objects for which they represent a "from" relationship.

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship name or, as with open vocabularies, user-defined names.

|  |  |  |  |
| --- | --- | --- | --- |
| **Embedded Relationships** | | | |
| **created\_by\_ref** | | source | |
| **object\_markings\_refs** | | marking-definition | |
| **Common Relationships** | | | |
| duplicate-of, derived-from, related-to | | | |
| **Source** | **Name** | **Target** | **Description** |
| course-of-action | mitigates | attack-pattern,  infrastructure, malware,  vulnerability,  tool, incident | This Relationship describes that the Course of Action can mitigate the related Attack Pattern, Malware, Vulnerability, Tool, or Incident. For the purposes of this relationship, mitigate means both complete fixes (e.g. a patch for a Vulnerability) as well as temporary fixes (blocking a Malware C2 address).  For example, a mitigates Relationship from a Course of Action to block an IP address to the xInject Malware indicate that the Course of Action mitigates the impact of the xInject. |
| **Reverse Relationships** | | | |
|  |  |  |  |

### ​1.3.3.​ Examples

[

{

"type": "course-of-action",

"id": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",

"created\_by\_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",

"created": "2016-04-06T20:03:48Z",

"modified": "2016-04-06T20:03:48Z",

"version": 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 the existing UDP 1434 filter ..."

},

{

"type": "relationship",

"id": "relationship--44298a74-ba52-4f0c-87a3-1824e67d7fad",

"created\_by\_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",

"created": "2016-04-06T20:06:37Z",

"modified": "2016-04-06T20:06:37Z",

"version": 1,

"source\_ref": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",

"target\_ref": "malware--31b940d4-6f7f-459a-80ea-9c1f17b5891b",

"name": "mitigates"

},

{

"type": "malware",

"id": "malware--31b940d4-6f7f-459a-80ea-9c1f17b5891b",

"created\_by\_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",

"created": "2016-04-06T20:07:09Z",

"modified": "2016-04-06T20:07:09Z",

"version": 1,

"name": "Poison Ivy"

}

]

## ​1.4.​ Incident

**Type Name:** incident

An incident is a violation of an explicit or implied security policy [TODO add ref to NIST]. Incidents can include, but are not limited to:

* attempts (either failed or successful) to gain unauthorized access to a system or its data
* unwanted disruption or denial of service
* the unauthorized use of a system for the processing or storage of data
* changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

For example, an Incident could describe a malware infestation on one of a company's laptops.

The Incident SDO is a stub in STIX 2.0. Later versions of this specification will expand on these properties and relationships to more fully capture information related to incidents. The current version simply contains a name and description. Relationships from the Incident can describe the intended and actual victims (Victim Target), the perpetrators (Campaign, Intrusion Set, and Threat Actor), and what actions were taken in response (Course of Action).

### ​1.4.1.​ Properties

|  |  |  |
| --- | --- | --- |
| **Common Properties** | | |
| **type, id, created\_by\_ref, created, modified, version, revoked, labels, external\_references, object\_markings\_refs, granular\_markings** | | |
| **Indicator Specific Properties** | | |
| **name, description** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this field **MUST** be incident |
| **labels** (required) | list of type open-vocab | This property is a list of classifications for the Incident.  This is an open vocabulary and values **SHOULD** come from the incident-label-ov vocabulary. |
| **name** (required) | string | A name used to identify the Incident. |
| **description** (optional) | string | A description that provides more details and context about the Incident, potentially including its purpose and its key characteristics. |

### ​1.4.2.​ Relationships

These are the relationships explicitly defined between the Incident object and other objects. The first section lists the embedded relationships by property name along with their corresponding target. The rest of the table identifies the relationships that can be made from this object by way of the Relationship Object. The reverse relationships (relationships "to" this object) are included as a convenience. For their definitions, please see the objects for which they represent a "from" relationship.

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship name or, as with open vocabularies, user-defined names.

|  |  |  |  |
| --- | --- | --- | --- |
| **Embedded Relationships** | | | |
| **created\_by\_ref** | | source | |
| **object\_markings\_refs** | | marking-definition | |
| **Common Relationships** | | | |
| duplicate-of, derived-from, related-to | | | |
| **Source** | **Name** | **Target** | **Description** |
| incident | attributed-to | campaign, intrusion-set, threat-actor | This Relationship describes that the the related Campaign, Intrusion Set,, or Threat Actor is responsible for the Incident.  For example, an attributed-to Relationship from an Incident to a Campaign means that the Campaign was used to carry out the incident. |
| **Reverse Relationships** | | | |
| observed-data, victim-target | part-of | incident | See forward relationship for definition. |
| course-of-action | mitigates | incident | See forward relationship for definition. |

### ​1.4.3.​ Examples

{

"type": "incident",

"id": "incident--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",

"created\_by\_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",

"created": "2016-04-06T20:03:48Z",

"modified": "2016-04-06T20:03:48Z",

"version": 1,

"name": "Green Group Infiltration of Web Servers",

"description": "Green group was able to infiltrate the web server infrastructure and caused sporadic and unpredictable content defacement issues."

}

## ​1.5.​ Indicator

**Type Name:** indicator

Indicators describe evidence of suspicious or malicious cyber activity. In addition to textual information interpreted by analysts, indicators may also contain structured patterns intended to enable automated detection of the malicious activity. For example, an Indicator could be used to represent a domain watchlist and use the CybOX Patterning Language (TODO add reference) to specify the domains of concern.

The Indicator SDO contains a simple textual description, the kill chain phases that it detects behavior in, a time window for when the indicator is valid or useful, and a required **pattern** property to capture a structured detection pattern. The **pattern** property can contain detection patterns specified in either the CybOX Patterning Language (the default) or other patterning languages, such as Snort and YARA (TODO add reference). Conforming STIX implementations **MUST** support the CybOX Patterning Language <TODO: add reference> and **MAY** additionally support other pattern languages. While each structured pattern language has different syntax and potentially different semantics, in general an indicator is considered to have “matched” (or been “sighted”) when the conditions specified in the structured pattern are satisfied in whatever context they are evaluated in.

Relationships from the Indicator can describe the malicious or suspicious behavior that it directly detects (Malware, Tool, and Attack Pattern) as well as the Campaigns, Intrusion Sets, and Threat Actors that it might indicate the presence of.

### ​1.5.1.​ Properties

|  |  |  |
| --- | --- | --- |
| **Common Properties** | | |
| **type, id, created\_by\_ref, created, modified, version, revoked, labels, external\_references, object\_markings\_refs, granular\_markings** | | |
| **Indicator Specific Properties** | | |
| **name, description, pattern, pattern\_lang, valid\_from, valid\_from\_precision, valid\_until, valid\_until\_precision, kill\_chain\_phases** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this field **MUST** be indicator |
| **labels** (required) | list of type open-vocab | This field is an Open Vocabulary that specifies the type of indicator.  This is an open vocabulary and values **SHOULD** come from the indicator-label-ov vocabulary. |
| **name** (optional) | string | A name used to identify the Indicator. |
| **description** (optional) | string | A description that provides more details and context about the Indicator, potentially including its purpose and its key characteristics. |
| **pattern** (required) | string | The detection pattern for this indicator. The default language is CybOX Patterning; implementations **MUST** support processing of CybOX patterns and **MAY** support others, such as Snort and YARA. |
| **pattern\_lang** (optional) | open-vocab | The language used to define the pattern (in the **pattern** field). The default is cybox if the field is omitted.  This is an open vocabulary and values **SHOULD** come from the pattern-lang-ov vocabulary. |
| **valid\_from** (required) | timestamp | The time from which this indicator should be considered valuable intelligence. |
| **valid\_from\_precision** (optional) | timestamp-precision | The precision of the start timestamp. |
| **valid\_until** (optional) | timestamp | The time at which this indicator should no longer be considered valuable intelligence.  If the **valid\_until** property is omitted, then there is no constraint on the latest time for which the Indicator should be used. |
| **valid\_until\_precision** (optional) | timestamp-precision | The precision of the valid until timestamp. |
| **kill\_chain\_phases** (optional) | list of type kill-chain-phase | The phases of the kill chain that this indicator detects. <todo: Fix this definition.> |

### ​1.5.2.​ Relationships

These are the relationships explicitly defined between the Indicator object and other objects. The first section lists the embedded relationships by property name along with their corresponding target. The rest of the table identifies the relationships that can be made from this object by way of the Relationship Object. The reverse relationships (relationships "to" this object) are included as a convenience. For their definitions, please see the objects for which they represent a "from" relationship.

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship name or, as with open vocabularies, user-defined names.

|  |  |  |  |
| --- | --- | --- | --- |
| **Embedded Relationships** | | | |
| **created\_by\_ref** | | source | |
| **object\_markings\_refs** | | marking-definition | |
| **Common Relationships** | | | |
| duplicate-of, derived-from, related-to | | | |
| **Source** | **Name** | **Target** | **Description** |
| indicator | indicates | attack-pattern, campaign,  infrastructure, intrusion-set,  malware,  threat-actor, tool | This Relationship describes that the Indicator can detect evidence of the related Campaign, Intrusion, or Threat Actor. This evidence may not be direct: for example, the Indicator may detect secondary evidence of the Campaign, such as malware or behavior commonly used by that Campaign.  For example, an indicates Relationship from an Indicator to a Campaign object representing Glass Gazelle means that the Indicator is capable of detecting evidence of Glass Gazelle, such as command and control IPs commonly used by that Campaign. |
| **Reverse Relationships** | | | |
|  |  |  |  |

### ​1.5.3.​ Examples

*Indicator Itself, with Context*

[

{

"type": "indicator",

"id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",

"created\_by\_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",

"created": "2016-04-06T20:03:48Z",

"modified": "2016-04-06T20:03:48Z",

"version": 1,

"name": "Poison Ivy Malware",

"description": "This file is part of Poison Ivy",

"pattern": "file-object.hashes.md5 = '3773a88f65a5e780c8dff9cdc3a056f3'",

"pattern\_lang": "cybox",

"valid\_from": "2016-01-01T00:00:00Z"

},

{

"type": "relationship",

"id": "relationship--44298a74-ba52-4f0c-87a3-1824e67d7fad",

"created\_by\_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",

"created": "2016-04-06T20:06:37Z",

"modified": "2016-04-06T20:06:37Z",

"version": 1,

"source\_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",

"target\_ref": "malware--31b940d4-6f7f-459a-80ea-9c1f17b5891b",

"name": "detects"

},

{

"type": "malware",

"id": "malware--31b940d4-6f7f-459a-80ea-9c1f17b5891b",

"created": "2016-04-06T20:07:09Z",

"modified": "2016-04-06T20:07:09Z",

"created\_by\_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",

"version": 1,

"name": "Poison Ivy"

}

]

## ​1.6.​ Infrastructure

**Type Name:** infrastructure

Malicious infrastructures are a type of TTP that describes the backend services and resources used by attackers to carry out attacks. Command and control servers, malware delivery sites, and phishing sites are examples of malicious infrastructure.

The Infrastructure SDO contains basic descriptive information and a characterization of the technical details of the infrastructure using CybOX. Relationships to and from Malicious Infrastructure can relate it to the attackers (Threat Actors, Intrusion Sets, and Campaigns) and incidents that use it and Indicators that can detect it.

The Infrastructure SDO **MUST NOT** be used to capture information about defender infrastructures or assets.

### ​1.6.1.​ Properties

|  |  |  |
| --- | --- | --- |
| **Common Properties** | | |
| **type, id, created\_by\_ref, created, modified, version, revoked, labels, external\_references, object\_markings\_refs, granular\_markings** | | |
| **Infrastructure Specific Properties** | | |
| **name**, **description**, **first\_observed, first\_observed\_precision, kill\_chain\_phases** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this field **MUST** be infrastructure |
| **name** (optional) | string | The name used to identify the Infrastructure. |
| **description** (optional) | string | A description that provides more details and context about the malicious Infrastructure, potentially including its purpose and its key characteristics. |
| **first\_seen** (required) | timestamp | The time that this malicious Infrastructure was first seen. |
| **first\_seen\_precision** (optional) | timestamp-precision | The precision of the **first\_seen** timestamp. |
| **kill\_chain\_phases** (optional) | list of type kill-chain-phase | The list of Kill Chain phases for which this Infrastructure is used. |

### ​1.6.2.​ Relationships

These are the relationships explicitly defined between the Infrastructure object and other objects. The first section lists the embedded relationships by property name along with their corresponding target. The rest of the table identifies the relationships that can be made from this object by way of the Relationship Object. The reverse relationships (relationships "to" this object) are included as a convenience. For their definitions, please see the objects for which they represent a "from" relationship.

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship name or, as with open vocabularies, user-defined names.

|  |  |  |  |
| --- | --- | --- | --- |
| **Embedded Relationships** | | | |
| **created\_by\_ref** | | source | |
| **object\_markings\_refs** | | marking-definition | |
| **Common Relationships** | | | |
| duplicate-of, derived-from, related-to | | | |
| **Source** | **Name** | **Target** | **Description** |
| infrastructure | targets | victim-target, vulnerability | This Relationship documents that this malicious Infrastructure is being used to target this Victim Target or Vulnerability.  For example, a targets Relationship linking an Infrastructure for a phishing hosting site to a Victim Target representing the retail sector indicates that the phishing hosting site is targeted at the retail sector. |
| **Reverse Relationships** | | | |
| indicator | indicates | infrastructure | See forward relationship for definition. |
| course-of-action | mitigates | infrastructure | See forward relationship for definition. |
| campaign, intrusion-set,  malware,  threat-actor,  tool | uses | infrastructure | See forward relationship for definition. |

​

### ​1.6.3.​ Examples

TODO

## ​1.7.​ Intrusion Set

**Type Name:** intrusion-set

An Intrusion Set is a grouped set of adversary behavior and resources with common properties that is believed to be orchestrated by a single organization. An Intrusion Set may capture multiple Campaigns, Incidents or other activity that are all tied together by shared attributes indicating a common 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.

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 goes silent, or changes focus, it is usually difficult to know if it has truly disappeared or ended. Analysts may have varying level 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.

### ​1.7.1.​ Properties

|  |  |  |
| --- | --- | --- |
| **Common Properties** | | |
| **type, id, created\_by\_ref, created, modified, version, revoked, labels, external\_references, object\_markings\_refs, granular\_markings** | | |
| **Campaign Specific Properties** | | |
| **name, description, aliases, first\_seen, first\_seen\_precision, goals, resource\_level, primary\_motivation, secondary\_motivations, region, country** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this field **MUST** be intrusion-set |
| **name** (required) | string | A name used to identify this Intrusion Set. |
| **description** (optional) | string | A description that provides more details and context about the Intrusion Set, potentially including its purpose and its key characteristics. |
| **aliases** (optional) | list of type string | Alternative names used to identify this Intrusion Set. |
| **first\_seen** (optional) | timestamp | The time that this Intrusion Set was first seen. |
| **first\_seen\_precision** (optional) | timestamp-precision | The precision value for the **first\_seen** field |
| **goals** (optional) | list of type string | The high level goals of this Intrusion Set, namely, what are they trying to do. For example, they may be motivated by personal gain, but their goal is to steal credit card numbers. To do this, they may execute specific Campaigns that have detailed objectives like compromising point of sale systems at a large retailer.  Another example: Gain information about latest merger and IPO information from ACME Bank. |
| **resource\_level** (optional) | open-vocab | This defines 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.  This is an open vocabulary and values **SHOULD** come from the attack-resource-level-ov vocabulary. |
| **primary\_motivation** (optional) | open-vocab | The primary reason, motivation, or purpose behind this Intrusion Set. The motivation is why the Intrusion Set wishes to achieve the objective (what they are trying to achieve).  For example, an Intrusion Set with an objective to disrupt the finance sector in a country might be motivated by ideological hatred of capitalism.  This is an open vocabulary and values **SHOULD** come from the attack-motivation-ov vocabulary. |
| **secondary\_motivations** (optional) | list of type open-vocab | The secondary reasons, motivations, or purposes behind this Intrusion Set. These motivations can exist as an equal or near-equal cause to the primary motivation. However, it does not replace or necessarily magnify the primary motivation, but it might indicate additional context.  This is an open vocabulary and values **SHOULD** come from the attack-motivation-ov vocabulary. |
| **region** (optional) | string | The primary region of origin for this Intrusion Set, if the actual country is not yet known. |
| **country** (optional) | string | The primary country of origin for this Intrusion Set. The value **MUST** be from the ISO 3166-1 Alpha-2 codes and represented in lower-case <TODO ISO Ref>. |

### ​1.7.2.​ Relationships

These are the relationships explicitly defined between the Intrusion Set object and other objects. The first section lists the embedded relationships by property name along with their corresponding target. The rest of the table identifies the relationships that can be made from this object by way of the Relationship Object. The reverse relationships (relationships "to" this object) are included as a convenience. For their definitions, please see the objects for which they represent a "from" relationship.

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship name or, as with open vocabularies, user-defined names.

|  |  |  |  |
| --- | --- | --- | --- |
| **Embedded Relationships** | | | |
| **created\_by\_ref** | | source | |
| **object\_markings\_refs** | | marking-definition | |
| **Common Relationships** | | | |
| duplicate-of, derived-from, related-to | | | |
| **Source** | **Name** | **Target** | **Description** |
| intrusion-set | attributed-to | threat-actor | This Relationship describes that the related Threat Actor is involved in carrying out the Intrusion Set.  For example, an attributed-to Relationship from the Red Orca Intrusion Set to the Urban Fowl Threat Actor means that the actor carried out or was involved in some of the activity described by the Intrusion Set. |
| intrusion-set | targets | victim-target, vulnerability | This Relationship describes that the Intrusion Set uses exploits of the related Vulnerability or targets the type of victims described by the related Victim Target.  For example, a targets Relationship from the Red Orca Intrusion Set to a Vulnerability in a blogging platform indicates that attacks performed as part of Red Orca often exploit that Vulnerability.  Similarly, a targets Relationship from the Red Orca Intrusion Set to a Victim Target describing the energy sector in the United States means that the Intrusion Set typically carries out attacks against targets in that sector. |
| intrusion-set | uses | attack-pattern, infrastructure, malware, tool | This Relationship describes that attacks carried out as part of the Intrusion Set typically use the related Attack Pattern, Malware, or Tool.  For example, a uses Relationship from the Red Orca Intrusion Set to the xInject Malware indicate that xInject is often used during attacks attributed to that Intrusion Set. |
| **Reverse Relationships** | | | |
| campaign, incident | attributed-to | intrusion-set | See forward relationship for definition. |
| indicator | indicates | intrusion-set | See forward relationship for definition. |

### ​1.7.3.​ Example

{

"type": "intrusion-set",

"id": "intrusion-set--4e78f46f-a023-4e5f-bc24-71b3ca22ec29",

"created\_by\_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",

"created": "2016-04-06T20:03:48Z",

"modified": "2016-04-06T20:03:48Z",

"version": 1,

"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.",

"aliases": ["Zookeeper"],

"objectives": ["acquisition-theft", "harassment", "damage"]

}

## ​1.8.​ Malware

**Type Name:** malware

Malware is a type of TTP that is also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or of otherwise annoying or disrupting the victim. Malware such as viruses and worms is usually designed to perform these nefarious functions in such a way that users are unaware of them, at least initially.[[1]](#footnote-0)

The Malware SDO characterizes, identifies, and categorizes malware samples via a text description field and may be associated with MAEC[[2]](#footnote-1) content. This provides detailed information about how the malware works and what it does. Relationships from Malware can capture what the malware targets (Vulnerability and Victim Target) and link it to another Malware SDO that is a variant.

### ​1.8.1.​ Properties

|  |  |  |
| --- | --- | --- |
| **Common Properties** | | |
| **type, id, created\_by\_ref, created, modified, version, revoked, labels, external\_references, object\_markings\_refs, granular\_markings** | | |
| **Malware Specific Properties** | | |
| **name, description, kill\_chain\_phases, maec** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this field **MUST** be malware |
| **labels** (required) | list of type open-vocab | The type of malware being described.  This is an open vocabulary and values **SHOULD** come from the malware-labels-ov vocabulary. |
| **external\_references** (optional) | list of type external-reference | A list of external references which refer to non-STIX information.  This field **MAY** be used to capture names for the malware across anti-virus or anti-malware tools.  When doing so, the **source** property **SHOULD** be used to capture the vendor or tool name and the **external\_id** property **SHOULD** be used to capture the exact name it's known by. For example, to capture that an AV tool called "acme-antivirus" detects the malware as "very-bad-malware", an external reference could be added with a **source** of acme-antivirus and an **external\_id** of very-bad-malware. |
| **name** (required) | string | A name used to identify the Malware. |
| **description** (optional) | string | A description that provides more details and context about the Malware, potentially including its purpose and its key characteristics. |
| **kill\_chain\_phases** (optional) | list of type kill-chain-phase | The list of Kill Chain Phases for which this Malware instance can be used. |
| **analysis** (optional) | <malware analysis object> | The **analysis** property contains detailed malware analysis data. If MAEC is used then this property just contains the MAEC content. |
| **analysis\_lang** | string | The **analysis\_lang** property identifies the type of malware analysis found in the **analysis** property. The value of the **analysis\_lang** property **SHOULD** be one of the types defined in the subsections below: basic or maec (see Section TODO). |

### ​1.8.2.​ Basic Malware Analysis Type

<todo description>

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **file\_properties** (required) | cybox/file-object | The CybOX content that describe the file properties of this malware sample. For example, filenames, file sizes, etc..  The file-object **MUST NOT** include any CybOX relationships (i.e., must not include the **contains\_ref**, **signed\_with\_ref** fields and any others that are CybOX relationships). |
| **sample** | cybox/artifact-object |  |

### ​1.8.3.​ Relationships

These are the relationships explicitly defined between the Malware object and other objects. The first section lists the embedded relationships by property name along with their corresponding target. The rest of the table identifies the relationships that can be made from this object by way of the Relationship Object. The reverse relationships (relationships "to" this object) are included as a convenience. For their definitions, please see the objects for which they represent a "from" relationship.

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship name or, as with open vocabularies, user-defined names.

|  |  |  |  |
| --- | --- | --- | --- |
| **Embedded Relationships** | | | |
| **created\_by\_ref** | | source | |
| **object\_markings\_refs** | | marking-definition | |
| **Common Relationships** | | | |
| duplicate-of, derived-from, related-to | | | |
| **Source** | **Name** | **Target** | **Description** |
| malware | targets | victim-target, vulnerability | This Relationship documents that this Malware is being used to target this Victim Target or exploit the Vulnerability.  For example, a targets Relationship linking a Malware representing a downloader to a Vulnerability for CVE-2016-0001 means that the malware exploits that vulnerability.  Similarly, a targets Relationship linking a Malware representing a downloader to a Victim Target representing the energy sector means that downloader is typically used against targets in the energy sector. |
| malware | uses | infrastructure, tool | This Relationship documents that this Malware uses the related infrastructure or tool to perform its functions.  For example, a uses Relationship linking a Malware representing a trojan to an Infrastructure representing a command and control botnet means that the trojan uses the botnet for C2. |
| malware | variant-of | malware | This Relationship is used to document that one piece of Malware is a variant of another piece of Malware.  For example, TorrentLocker is a variant of Cryptolocker. |
| **Reverse Relationships** | | | |
| indicator | indicates | malware | See forward relationship for definition. |
| course-of-action | mitigates | malware | See forward relationship for definition. |
| attack-pattern, campaign, intrusion-set, threat-actor | uses | malware | See forward relationship for definition. |

​

### ​1.8.4.​ Examples

{

"type": "malware",

"id": "malware--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",

"created": "2016-05-12T08:17:27.000000Z",

"modified": "2016-05-12T08:17:27.000000Z",

"version": "1",

"name": "Cryptowall",

"description": "...",

"labels": ["ransomware"]

}

## ​1.9.​ Observed Data

**Type Name:** observed-data

Observed data conveys information that was observed on systems and networks, such as log data or network traffic, using the CybOX specification. For example, observed data can capture the observation of an IP address, of a network connection, of a file, or of a registry key. Observed data is not an intelligence assertion, it is simply information: this file was seen, without any context for what it means. In STIX, observed data is represented as the Observed Data SDO.

Observed Data captures both a single observation of a single entity (file, network connection) as well as the aggregation of multiple observations of an entity. When the **count** property is one the observed data is of a single entity. When the **count** property is more than one, the observed data consists of several instances collected over the time window specified by the **first\_observed** and **last\_observed** properties. When used to collect aggregate data, it's likely that some fields in the CybOX object (e.g. timestamp fields) will be omitted because they would differ for each of the individual observations.

Observed Data can be used by itself (without relationships) to convey raw data collected from network and host-based detection tools. A firewall could emit a single Observed Data instance with a network connection for every connection it sees. That firewall could also aggregate data and instead send out an Observed Data instance every ten minutes with an appropriate count value.

Observed Data can also be related to other STIX Objects to represent raw data that is relevant to those objects. The Sighting object, which captures the sighting of an Indicator, Malware, or other SDO, uses Observed Data to represent the raw information that led to the creation of the Sighting (i.e., what was actually seen to make you think you had that Malware instance). Observed Data can also be related to Incident to provide data that was discovered during the response process or that is otherwise part of the incident.

### ​1.9.1.​ Properties

|  |  |  |
| --- | --- | --- |
| **Common Properties** | | |
| **type, id, created\_by\_ref, created, modified, version, revoked, labels, external\_references, object\_markings\_refs, granular\_markings** | | |
| **Observed Data Specific Properties** | | |
| **first\_observed, last\_observed, number\_observed, cybox** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this field **MUST** be observed-data |
| **first\_observed** (required) | timestamp | The beginning of the time window that the data was observed during. |
| **last\_observed** (required) | timestamp | The end of the time window that the data was observed during. |
| **number\_observed** (required) | number | The number of times the data represented in the **cybox** property was observed. This **MUST** be an integer between 1 and 999,999,999 inclusive.  If the **number\_observed** property is greater than one, the data contained in the **cybox** field was observed multiple times. In these cases, object creators **MAY** omit fields (such as timestamps and IDs) that are specific to a single instance of that observed data. |
| **cybox** (required) | cybox-container | The CybOX content that describes a single "fact" that was observed.  The CybOX content may include multiple objects if those objects are part of a single observation. Multiple objects **MUST NOT** be used within the same Observed Data instance to describe multiple observations. |

​

### ​1.9.2.​ Relationships

These are the relationships explicitly defined between the Observed Data object and other objects. The first section lists the embedded relationships by property name along with their corresponding target. The rest of the table identifies the relationships that can be made from this object by way of the Relationship Object. The reverse relationships (relationships "to" this object) are included as a convenience. For their definitions, please see the objects for which they represent a "from" relationship.

In addition to the relationships created using the generic Relationship object, Observed Data is also a direct target of the Sighting SRO. Sightings represent a relationship between some intelligence entity that was seen (e.g. an Indicator or Malware instance), where it was seen, and what evidence was actually seen. The evidence (or raw data) in that relationship is captured as Observed Data.

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship name or, as with open vocabularies, user-defined names.

|  |  |  |  |
| --- | --- | --- | --- |
| **Embedded Relationships** | | | |
| **created\_by\_ref** | | source | |
| **object\_markings\_refs** | | marking-definition | |
| **Common Relationships** | | | |
| duplicate-of, derived-from, related-to | | | |
| **Source** | **Name** | **Target** | **Description** |
| observed-data | part-of | incident | This Relationship documents that this Observed Data is a part of the related Incident.  For example, a part-of Relationship linking a set of Observed Data containing network connection information to an Incident could capture network traffic that originated from a compromised host and was determined to be command and control traffic. |

​

### ​1.9.3.​ Examples

*Observed Data of a file object*

{

"type": "observed-data",

"id": "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf",

"created\_by\_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",

"created": "2016-04-06T19:58:16Z",

"modified": "2016-04-06T19:58:16Z",

"version": 1,

"first\_observed": "2015-12-21T19:00:00Z",

"last\_observed": "2015-12-21T19:00:00Z",

"number\_observed": 50,

"cybox": {

"spec\_version": "3.0",

"objects": {

"0": {

"type": "file-object",

"file\_name": "malware.exe",

"hashes": {

"md5": "3773a88f65a5e780c8dff9cdc3a056f3",

"sha1": "cac35ec206d868b7d7cb0b55f31d9425b075082b"

}

}

}

}

}

## ​1.10.​ Report

**Type Name:** report

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. They are used to group similar threat intelligence together so that it can be published as a comprehensive cyber threat story.

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

For example, a threat report by ACME Defense Corp. discussing the Glass Gazelle campaign could be represented using Report. The Report itself would contain the narrative of the report while the Campaign SDO and any related SDOs (e.g. Indicators for the Campaign, Malware it uses, and the associated Relationships) would be referenced in the report contents.

### ​1.10.1.​ Properties

|  |  |  |
| --- | --- | --- |
| **Common Properties** | | |
| **type, id, created\_by\_ref, created, modified, version, revoked, labels, external\_references, object\_markings\_refs, granular\_markings** | | |
| **Report Specific Properties** | | |
| **name, description, published, published\_precision, report\_refs** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this field **MUST** be report |
| **labels** (required) | list of type open-vocab | This field is an Open Vocabulary that specifies the primary subject of this report.  This is an open vocabulary and values **SHOULD** come from the report-label-ov vocabulary. |
| **name** (required) | string | A name used to identify the Report. |
| **description** (optional) | string | A description that provides more details and context about the Report, potentially including its purpose and its key characteristics. |
| **published** (required) | timestamp | The date that this report object was officially published by the creator of this report.  The publication data (public release, legal release, etc.) may be different than date the report was created or shared internally (the STIX creation date). |
| **report\_refs** (required) | list of type identifier | Specifies other STIX Objects that are referred to by this Report. |

### ​1.10.2.​ Relationships

There are no relationships explicitly defined between the Report object and other objects, other than those defined as common relationships. The first section lists the embedded relationships by property name along with their corresponding target.

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship name or, as with open vocabularies, user-defined names.

|  |  |  |  |
| --- | --- | --- | --- |
| **Embedded Relationships** | | | |
| **created\_by\_ref** | | source | |
| **object\_markings\_refs** | | marking-definition | |
| **report\_refs** | | list of type identifier | |
| **Common Relationships** | | | |
| duplicate-of, derived-from, related-to | | | |

​

### ​1.10.3.​ Examples

// Just a report, where the consumer may or may not already have access to the SDOs

{

"type": "report",

"id": "report--84e4d88f-44ea-4bcd-bbf3-b2c1c320bcb3",

"created\_by\_ref": "source--a463ffb3-1bd9-4d94-b02d-74e4f1658283",

"created": "2015-12-21T19:59:11Z",

"modified": "2016-05-21T19:59:11Z",

"version": 1,

"name": "The Black Vine Cyberespionage Group",

"description": "A simple report with an indicator and campaign",

"labels": ["campaign-report"],

"report\_contains\_refs": [

"indicator--26ffb872-1dd9-446e-b6f5-d58527e5b5d2",

"campaign--83422c77-904c-4dc1-aff5-5c38f3a2c55c",

"relationship--f82356ae-fe6c-437c-9c24-6b64314ae68a"

]

}

// A full bundle with a report and the SDOs / Relationships that are part of the report

{

"type": "bundle",

"id": "bundle--44af6c39-c09b-49c5-9de2-394224b04982",

"sources": [

{

"type": "source",

"id": "source--a463ffb3-1bd9-4d94-b02d-74e4f1658283",

"name": "Acme Cybersecurity Solutions",

}

],

"reports": [

{

"type": "report",

"id": "report--84e4d88f-44ea-4bcd-bbf3-b2c1c320bcbd",

"created\_by\_ref": "source--a463ffb3-1bd9-4d94-b02d-74e4f1658283",

"created": "2015-12-21T19:59:11Z",

"modified": "2016-05-21T19:59:11Z",

"version": 1,

"name": "The Black Vine Cyberespionage Group",

"description": "A simple report with an indicator and campaign",

"labels": ["campaign-report"],

"report\_contains\_refs": [

"indicator--26ffb872-1dd9-446e-b6f5-d58527e5b5d2",

"campaign--83422c77-904c-4dc1-aff5-5c38f3a2c55c"

]

}

],

"indicators": [

{

"type": "indicator",

"id": "indicator--26ffb872-1dd9-446e-b6f5-d58527e5b5d2",

"created": "2015-12-21T19:59:17Z",

"modified": "2016-05-21T19:59:11Z",

"version": 1,

"name": "Some indicator",

"indicator\_types": ["anonymization"],

"created\_by\_ref": "source--a463ffb3-1bd9-4d94-b02d-74e4f1658283"

}

],

"campaigns": [

{

"type": "campaign",

"id": "campaign--83422c77-904c-4dc1-aff5-5c38f3a2c55c",

"created": "2015-12-21T19:59:17Z",

"modified": "2016-05-21T19:59:11Z",

"version": 1,

"name": "Some Campaign",

"created\_by\_ref": "source--a463ffb3-1bd9-4d94-b02d-74e4f1658283"

}

],

“relationships”: [

{

"id": "relationship--f82356ae-fe6c-437c-9c24-6b64314ae68a",

"type": "relationship",

"created\_at": "2015-12-21T19:59:17.000000+00:00",

"created\_by\_ref": "source--a463ffb3-1bd9-4d94-b02d-74e4f1658283",

"source\_ref": "indicator--26ffb872-1dd9-446e-b6f5-d58527e5b5d2",

"target\_ref": "campaign--26ffb872-1dd9-446e-b6f5-d58527e5b5d2",

"name": "indicates"

},

]

}

## ​1.11.​ Source

**Type Name:** source

Sources represent individuals and organizations that provide information in STIX. They are used to represent the identity of content creators.

The Source SDO can capture basic identifying information, contact information, and the sectors and regions that they belong to. Sources are linked to STIX Objects via the **created\_by\_ref** field on the related SDO to indicate that they are the provider of that intelligence.

### ​1.11.1.​ Properties

|  |  |  |
| --- | --- | --- |
| **Common Properties** | | |
| **type, id, created\_by\_ref, created, modified, version, revoked, labels, external\_references, object\_markings\_refs, granular\_markings** | | |
| **Source Specific Properties** | | |
| **name, description, entity\_class, sector, contact\_information** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this field **MUST** be source |
| **name** (required) | string | The name of this Source. |
| **description** (optional) | string | A description that provides more details and context about the Source, potentially including its purpose and its key characteristics. |
| **entity\_class** (required) | open-vocab | The type of entity that this Source describes, e.g. an individual or organization.  This is an open vocabulary and the values **SHOULD** come from the entity-class-ov vocabulary. |
| **sector** (optional) | open-vocab | The industry sector of this Source.  This is an open vocabulary and values **SHOULD** come from the industry-sector-ov vocabulary. |
| **contact\_information** (optional) | string | The contact information (e-mail, phone number, etc.) for this Source. No format for this information is defined by the STIX specification. |

### ​1.11.2.​ Relationships

There is a direct embedded reference to Source in all STIX Objects called **created\_by\_ref** that is inherited from the Common Properties. This property links each object with the Source of the organization or individual that created the object.

There are no relationships explicitly defined between the Source object and other objects, other than those defined as common relationships. The first section lists the embedded relationships by property name along with their corresponding target.

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship name or, as with open vocabularies, user-defined names.

|  |  |  |  |
| --- | --- | --- | --- |
| **Embedded Relationships** | | | |
| **created\_by\_ref** | | source | |
| **object\_markings\_refs** | | marking-definition | |
| **Common Relationships** | | | |
| duplicate-of, derived-from, related-to | | | |

### ​1.11.3.​ Examples

A Source for an individual named John Smith

{

"type": "source",

...,

"name": "John Smith",

"classification": "individual",

...

}

A Source for a company named ACME Widget, Inc.

{

"type": "source",

...,

"name": "ACME Widget, Inc.",

"classification": "organization",

...

}

## ​1.12.​ Threat Actor

**Type Name:** threat-actor

Threat actors are actual individuals, groups, or organizations believed to be operating with malicious intent. A Threat Actor is not an Intrusion Set or attack package but may support or be affiliated with various Intrusion Sets (attack packages), groups, or organizations over time.

Threat Actors leverage their resources and the resources of an Intrusion Set to conduct attacks and run Campaigns against targets.

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

### ​1.12.1.​ Properties

|  |  |  |
| --- | --- | --- |
| **Common Properties** | | |
| **type, id, created\_by\_ref, created, modified, version, revoked, labels, external\_references, object\_markings\_refs, granular\_markings** | | |
| **Threat Actor Specific Properties** | | |
| **name, description, aliases, entity\_class, roles, goals, sophistication, resource\_level, primary\_motivation, secondary\_motivations, personal\_motivations, regions, nationality** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this field **MUST** be  threat-actor |
| **labels** (required) | list of type open-vocab | This field specifies the type of threat actor, if known or suspected.  This is an open vocabulary and values **SHOULD** come from the threat-actor-label-ov vocabulary. |
| **name** (required) | string | A name used to identify this Threat Actor or Threat Actor group. |
| **description** (optional) | string | A description that provides more details and context about the Threat Actor, potentially including its purpose and its key characteristics. |
| **aliases** (optional) | list of type string | A list of other names that this Threat Actor is believed to use. |
| **entity\_class** (required) | open\_vocab | The type of entity that this Threat Actor describes, e.g. an individual, organization.  This is an open vocabulary and the values **SHOULD** come from the entity-class-ov vocabulary. |
| **roles** (optional) | list of type open-vocab | This is a list of roles the Threat Actor plays.  This is an open vocabulary and the values **SHOULD** come from the threat-actor-roles-ov vocabulary. |
| **goals** (optional) | list of type string | The high level goals of this Threat Actor, namely, what are they trying to do. For example, they may be motivated by personal gain, but their goal is to steal credit card numbers. To do this, they may execute specific Campaigns that have detailed objectives like compromising point of sale systems at a large retailer. |
| **sophistication** (optional) | open-vocab | The skill, specific knowledge, special training, or expertise a Threat Actor must have to perform the attack.  This is an open vocabulary and values **SHOULD** come from the attack-sophistication-level-ov vocabulary. |
| **resource\_level** (optional) | open-vocab | This defines 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 Level attribute — a specific resource level implies that the Threat Actor has access to at least a specific sophistication level.  This is an open vocabulary and values **SHOULD** come from the attack-resource-level-ov vocabulary. |
| **primary\_motivation** (optional) | open-vocab | The primary reason, motivation, or purpose behind this Threat Actor.  For example, a Threat Actor with an objective to disrupt the finance sector in a country might be motivated by ideological hatred of capitalism.  This is an open vocabulary and values **SHOULD** come from the attack-motivation-ov vocabulary. |
| **secondary\_motivations** (optional) | list of type open-vocab | The secondary reasons, motivations, or purposes behind this Threat Actor.  The secondary reasons, motivations, or purposes behind this Threat Actor. These motivations can exist as an equal or near-equal cause to the primary motivation. However, it does not replace or necessarily magnify the primary motivation, but it might indicate additional context.  This is an open vocabulary and values **SHOULD** come from the attack-motivation-ov vocabulary. |
| **personal\_motivations** (optional) | list of type open-vocab | The personal reasons, motivations, or purposes of the Threat Actor regardless of organizational goals.  Personal motivation, which is independent of the organization’s goals, describes what impels an individual to carry out an attack. Personal Motivation may align with the organization’s motivation—as is common with activists—but more often it supports personal objectives. For example, an individual analyst may join a Data Miner corporation because his or her values and skills align with the corporation’s objectives. But the analyst most likely performs his or her daily work toward those objectives for personal reward in the form of a paycheck. The motivation of personal reward may be even stronger for Threat Actors who commit illegal acts, as it is more difficult for someone to cross that line purely for altruistic reasons.  This is an open vocabulary and values **SHOULD** come from the attack-motivation-ov vocabulary. |
| **regions** (optional) | list of type string | The regions or geographic locations they are known to operate in. |
| **nationalities** (optional) | list of type string | The nationalities of this Threat Actor. The value **MUST** be from the ISO 3166-1 Alpha-2 codes and represented in lower-case <TODO ISO Ref>. |

### ​1.12.2.​ Relationships

These are the relationships explicitly defined between the Threat Actor object and other objects. The first section lists the embedded relationships by property name along with their corresponding target. The rest of the table identifies the relationships that can be made from this object by way of the Relationship Object. The reverse relationships (relationships "to" this object) are included as a convenience. For their definitions, please see the objects for which they represent a "from" relationship.

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship name or, as with open vocabularies, user-defined names.

|  |  |  |  |
| --- | --- | --- | --- |
| **Embedded Relationships** | | | |
| **created\_by\_ref** | | source | |
| **object\_markings\_refs** | | marking-definition | |
| **Common Relationships** | | | |
| duplicate-of, derived-from, related-to | | | |
| **Source** | **Name** | **Target** | **Description** |
| threat-actor | targets | victim-target, vulnerability | This Relationship describes that the Threat Actor uses exploits of the related Vulnerability or targets the type of victims described by the related Victim Target.  For example, a targets Relationship from the John Smith Threat Actor to a Vulnerability in a blogging platform indicates that attacks performed by John Smith often exploit that Vulnerability.  Similarly, a targets Relationship from the John Smith Threat Actor to a Victim Target describing the energy sector in the United States means that John Smith often carries out attacks against targets in that sector. |
| threat-actor | uses | attack-pattern, infrastructure, malware, tool | This Relationship describes that attacks carried out as part of the Threat Actor typically use the related Attack Pattern, Malware, or Tool.  For example, a uses Relationship from the John Smith Threat Actor to the xInject Malware indicate that xInject is often used by John Smith. |
| **Reverse Relationships** | | | |
| campaign, incident, intrusion-set, | attributed-to | threat-actor | See forward relationship for definition. |
| indicator | indicates | threat-actor | See forward relationship for definition. |

### ​1.12.3.​ Examples

{

"type": "threat-actor",

"id": "threat-actor--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",

"created\_by\_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",

"created": "2016-04-06T20:03:48Z",

"modified": "2016-04-06T20:03:48Z",

"version": 1,

"name": "Evil Org",

"description": "The Evil Org threat actor group"

}

## ​1.13.​ Tool

**Type Name:** tool

In STIX, tools are a type of TTP that are legitimate software that are used by threat actors to perform attacks. Knowing how and when threat 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.

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 document malware. Further, Tool **MUST NOT** be used to document tools used as part of a course of action in response to an attack. Tools used during response activities can be included directly as part of a Course of Action SDO.

### ​1.13.1.​ Properties

|  |  |  |
| --- | --- | --- |
| **Common Properties** | | |
| **type, id, created\_by\_ref, created, modified, version, revoked, labels, external\_references, object\_markings\_refs, granular\_markings** | | |
| **Tool Specific Properties** | | |
| **name, description, tool\_version, kill\_chain\_phases** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this field **MUST** be tool |
| **labels** (required) | list of type open-vocab | The kind(s) of tool(s) being described.  This is an open vocabulary and values **SHOULD** come from the tool-label-ov vocabulary. |
| **name** (required) | string | The name used to identify the Tool. |
| **description** (optional) | string | A description that provides more details and context about the Tool, potentially including its purpose and its key characteristics. |
| **tool\_version** (optional) | string | The version identifier associated with the tool. |
| **kill\_chain\_phases** (optional) | list of type kill-chain-phase | The list of Kill Chain Phases for which this tool instance can be used. |

### ​1.13.2.​ Relationships

These are the relationships explicitly defined between the Tool object and other objects. The first section lists the embedded relationships by property name along with their corresponding target. The rest of the table identifies the relationships that can be made from this object by way of the Relationship Object. None are defined for this Tool object. The reverse relationships (relationships "to" this object) are included as a convenience. For their definitions, please see the objects for which they represent a "from" relationship.

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship name or, as with open vocabularies, user-defined names.

|  |  |  |  |
| --- | --- | --- | --- |
| **Embedded Relationships** | | | |
| **created\_by\_ref** | | source | |
| **object\_markings\_refs** | | marking-definition | |
| **Common Relationships** | | | |
| duplicate-of, derived-from, related-to | | | |
| **Source** | **Name** | **Target** | **Description** |
| tool | targets | victim-target, vulnerability | This Relationship documents that this Malware is being used to target this Victim Target or exploit the Vulnerability.  For example, a targets Relationship linking an exploit Tool to a Vulnerability for CVE-2016-0001 means that the tool exploits that vulnerability.  Similarly, a targets Relationship linking a DDoS Tool to a Victim Target representing the energy sector means that Tool is typically used against targets in the energy sector. |
| tool | uses | infrastructure | This Relationship documents that this Tool uses the related infrastructure to perform its functions.  For example, a uses Relationship linking a remote access Tool to an Infrastructure representing a proxy indicates that Tool is or can be used through that proxy. |
| **Reverse Relationships** | | | |
| indicator | indicates | tool | See forward relationship for definition |
| course-of-action | mitigates | tool | See forward relationship for definition |
| attack-pattern, campaign, intrusion-set, malware,  threat-actor | uses | tool | See forward relationship for definition |

​

### ​1.13.3.​ Examples

{

"type": "tool",

"id": "tool--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",

"created\_by\_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",

"created": "2016-04-06T20:03:48Z",

"modified": "2016-04-06T20:03:48Z",

"version": 1,

"name": "VNC"

}

​

## ​1.14.​ Victim Target

**Type Name:** victim-target

Victim Targets refer to the targets of potential or actual attacks. They are characterized generally when describing the types of victims a campaign or threat actor targets (e.g. employees in the healthcare sector) or more specifically when describing the actual victims of an incident.

The Victim Target SDO can capture basic identifying information, the sectors and regions that the target belongs to, and the roles the victim has (e.g. domain administrator).

### ​1.14.1.​ Properties

|  |  |  |
| --- | --- | --- |
| **Common Properties** | | |
| **type, id, created\_by\_ref, created, modified, version, revoked, labels, external\_references, object\_markings\_refs, granular\_markings** | | |
| **Target Specific Properties** | | |
| **name, description, entity\_class, roles, sectors, regions** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this field **MUST** be victim-target |
| **name** (required) | string | The name of this Victim Target. When referring to a specific entity (e.g., an individual or organization), this field **SHOULD** contain the canonical name of the specific entity. |
| **description** (optional) | string | A description that provides more details and context about the Victim Target, potentially including its purpose and its key characteristics. |
| **entity\_class** (required) | open-vocab | The type of entity that this Victim Target describes, e.g. an individual, organization.  This is an open vocabulary and the values **SHOULD** come from the entity-class-ov vocabulary. |
| **roles** (optional) | list of type string | The list of roles that this Victim Target performs (eg. CEO, Domain Administrators, Doctors, Hospital, or Retailer). No open vocabulary is yet defined for this property. |
| **sectors** (optional) | list of type open-vocab | The list of sectors that the Victim Target of the attack belongs to.  This is an open vocabulary and values **SHOULD** come from the industry-sector-ov vocabulary. |
| **regions** (optional) | list of type string | The list of regions (localities, nationalities) for this Victim Target.  When representing nationalities, the value **MUST** be from [ISO Ref]. |

### ​1.14.2.​ Relationships

These are the relationships explicitly defined between the Victim Target object and other objects. The first section lists the embedded relationships by property name along with their corresponding target. The rest of the table identifies the relationships that can be made from this object by way of the Relationship Object. None are defined for this Victim Target object. The reverse relationships (relationships "to" this object) are included as a convenience. For their definitions, please see the objects for which they represent a "from" relationship.

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship name or, as with open vocabularies, user-defined names.

|  |  |  |  |
| --- | --- | --- | --- |
| **Embedded Relationships** | | | |
| **created\_by\_ref** | | source | |
| **object\_markings\_refs** | | marking-definition | |
| **Common Relationships** | | | |
| duplicate-of, derived-from, related-to | | | |
| **Source** | **Name** | **Target** | **Description** |
| victim-target | part-of | incident | This Relationship describes that the the related Victim Target was a victim of this incident.  For example, an part-of Relationship from an Incident to a Victim Target representing ACME Corporation means that ACME Corporation was an actual victim of that Incident. |
| **Reverse Relationships** | | | |
| attack-pattern, campaign,  infrastructure,  intrusion-set,  malware,  threat-actor,  tool | targets | victim-target | See forward relationship for definition. |

### ​1.14.3.​ Examples

Targeting of domain administrators:

{

"type": "victim-target",

"id": "victim-target--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",

"created": "2016-05-12T08:17:27.000000Z",

"modified": "2016-05-12T08:17:27.000000Z",

"version": 1,

"name": "Domain Administrators",

"classification": "class",

"roles": ["domain-administrators"]

}

Targeting of hospitals in the United States:

{

"type": "victim-target",

"id": "victim-target--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",

"created": "2016-05-12T08:17:27.000000Z",

"modified": "2016-05-12T08:17:27.000000Z",

"version": 1,

"name": "Hospitals in the United States",

"classification": "class",

"roles": ["hospitals"],

"sectors": ["healthcare"],

"regions": ["us"]

}

Targeting of the British military:

{

"type": "victim-target",

"id": "victim-target--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",

"created": "2016-05-12T08:17:27.000000Z",

"modified": "2016-05-12T08:17:27.000000Z",

"version": 1,

"name": "British Military",

"classification": "organization",

"roles": ["military"],

"regions": ["gb"]

}

## ​1.15.​ Vulnerability

**Type Name:** vulnerability

A Vulnerability is a mistake in software that can be directly used by a hacker to gain access to a system or network [TODO add NIST ref]. For example, if a piece of malware exploits CVE-2015-12345, a Malware Object could be linked to a Vulnerability Object that references CVE-2015-12345.

The Vulnerability SDO is primarily used to link to external definitions of vulnerabilities or to describe 0-day vulnerabilities that do not yet have an external definition. Typically, other SDOs assert relationships to STIX Vulnerability objects when a specific vulnerability is exploited as part of malicious cyber activity. As such, Vulnerability Objects can be used as a linkage to the asset management and compliance process.

### ​1.15.1.​ Properties

|  |  |  |
| --- | --- | --- |
| **Common Properties** | | |
| **type, id, created\_by\_ref, created, modified, version, revoked, labels, external\_references, object\_markings\_refs, granular\_markings** | | |
| **Vulnerability Specific Properties** | | |
| **name, description** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this field MUST be vulnerability |
| **external\_references**  (optional) | list of type external-reference | A list of external references which refer to non-STIX information. This field **MAY** be used to provide one or more Vulnerability identifiers, such as a CVE ID [TODO: add reference]. When specifying a CVE ID, the **source** field of the external reference **MUST** be set to cve and the **external\_id** field **MUST** be the exact CVE identifier. |
| **name** (required) | string | A name used to identify the Vulnerability. |
| **description** (optional) | string | A description that provides more details and context about the Vulnerability, potentially including its purpose and its key characteristics. |

### ​1.15.2.​ Relationships

These are the relationships explicitly defined between the Vulnerability object and other objects. The first section lists the embedded relationships by property name along with their corresponding target. The rest of the table identifies the relationships that can be made from this object by way of the Relationship Object. None are defined for this Vulnerability object.The reverse relationships (relationships "to" this object) are included as a convenience. For their definitions, please see the objects for which they represent a "from" relationship.

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship name or, as with open vocabularies, user-defined names.

|  |  |  |  |
| --- | --- | --- | --- |
| **Embedded Relationships** | | | |
| **created\_by\_ref** | | source | |
| **object\_markings\_refs** | | marking-definition | |
| **Common Relationships** | | | |
| duplicate-of, derived-from, related-to | | | |
| **Source** | **Name** | **Target** | **Description** |
|  |  |  |  |
| **Reverse Relationships** | | | |
| attack-pattern, campaign, infrastructure, intrusion-set, malware, threat-actor, tool | targets | vulnerability | See forward relationship for definition. |
| course-of-action | mitigates | vulnerability | See forward relationship for definition. |

### ​1.15.3.​ Examples

{

"type": "vulnerability",

"id": "vulnerability--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",

"created": "2016-05-12T08:17:27.000000Z",

"modified": "2016-05-12T08:17:27.000000Z",

"version": 1,

"name": "CVE-2016-1234"

"external\_references": [

{

"source": "cve",

"id": "CVE-2016-1234"

}

]

}

# ​2.​ Relationship Objects

STIX Relationship Objects (SROs) represent types of relationships used to describe cyber threat intelligence. The generic Relationship SRO is used to describe many varied types of relationships, while the specific Sighting SRO contains additional properties to represent sighting relationships.

Property information, relationship information, and examples are provided for each SRO defined below. Property information includes common properties as well as properties that are specific to each SRO. Relationship information includes embedded relationships (e.g., **created\_by\_ref**), common relationships (e.g., related-to), and SRO-specific relationships. Forward relationships (i.e., relationships *from* the SRO to other SROs) are fully defined, while reverse relationships (i.e., relationships *to* the SRO from other SROs) are duplicated for convenience.

## ​2.1.​ Relationship

**Type Name:** relationship

Relationship is used to link together other SDOs, such as Indicator, Observed Data, and Threat Actor in order to describe how those SDOs are related to each other. If SDOs are considered “nodes” or “vertices” in the graph, the relationship object represents “edges”.

STIX defines many named relationships to link together SDOs. These named relationships are contained in the "Relationships" table under each SDO definition. Named relationships **SHOULD** be used whenever possible to ensure consistency. An example of a named relationship is that an indicator indicates a campaign.

STIX also allows relationships from any SDO to any SDO that have not been defined in this specification. These relationships **MAY** use the related-to relationship name or **MAY** use a custom relationship name. Custom relationship names **SHOULD** be all lowercase and **SHOULD** use dashes instead of spaces or underscores. As an example, a user might want to link malware directly to a tool. They can do so using related-to to say that the Malware is related to the Tool but not describe how, or they could use delivered-by (a custom name they determined) to indicate more detail.

Note that some relationships in STIX may seem like "shortcuts". For example, an Indicator doesn't really detect a Campaign: it detects activity (Attack Patterns, Malware, etc.) that are often used by that campaign. While some analysts might want all of the source data and think that shortcuts are "wrong", in many cases it's helpful to provide just the key points (shortcuts) and leave out the low-level details. In other cases, the low-level analysis may not be known or sharable, while the high-level analysis is. For these reasons, relationships that might appear to be "shortcuts" are not excluded from STIX.

### ​2.1.1.​ Named Relationships Summary

This relationship summary table is provided as a convenience. If there is a discrepancy between this table and the relationships defined with each of the SDOs, then the relationships defined with the SDOs **MUST** be viewed as authoritative.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Source** | **Name** | **Target** | **Source** | **Name** | **Target** |
| attack-pattern | targets | vulnerability | infrastructure | targets | victim-target |
| attack-pattern | targets | victim-target | infrastructure | targets | vulnerability |
| attack-pattern | uses | malware | intrusion-set | attributed-to | threat-actor |
| attack-pattern | uses | tool | intrusion-set | targets | victim-target |
| campaign | attributed-to | intrusion-set | intrusion-set | targets | vulnerability |
| campaign | attributed-to | threat-actor | intrusion-set | uses | attack-pattern |
| campaign | targets | victim-target | intrusion-set | uses | infrastructure |
| campaign | targets | vulnerability | intrusion-set | uses | malware |
| campaign | uses | attack-pattern | intrusion-set | uses | tool |
| campaign | uses | infrastructure | malware | targets | victim-target |
| campaign | uses | malware | malware | targets | vulnerability |
| campaign | uses | tool | malware | uses | infrastructure |
| course-of-action | mitigates | attack-pattern | malware | uses | tool |
| course-of-action | mitigates | incident | malware | variant-of | malware |
| course-of-action | mitigates | infrastructure | observed-data | part-of | incident |
| course-of-action | mitigates | malware | threat-actor | targets | victim-target |
| course-of-action | mitigates | tool | threat-actor | targets | vulnerability |
| course-of-action | mitigates | vulnerability | threat-actor | uses | infrastructure |
| incident | attributed-to | campaign | threat-actor | uses | malware |
| incident | attributed-to | intrusion-set | threat-actor | uses | tool |
| incident | attributed-to | threat-actor | tool | targets | victim-target |
| indicator | indicates | attack-pattern | tool | targets | vulnerability |
| indicator | indicates | campaign | tool | uses | infrastructure |
| indicator | indicates | infrastructure | victim-target | part-of | incident |
| indicator | indicates | intrusion-set |  |  |  |
| indicator | indicates | malware |  |  |  |
| indicator | indicates | threat-actor |  |  |  |
| indicator | indicates | tool |  |  |  |

### ​2.1.2.​ Properties

|  |  |  |
| --- | --- | --- |
| **Common Properties** | | |
| **type, id, created\_by\_ref, created, modified, version, revoked, labels, external\_references, object\_markings\_refs, granular\_markings** | | |
| **Relationship Specific Properties** | | |
| **name, description, source\_ref, target\_ref** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this field **MUST** be relationship |
| **name** (required) | string | The name used to identify the Relationship. This value **SHOULD** be an exact value listed in the relationships for the source and target SDO, but **MAY** be any string. The value of this field **MUST** be in ASCII and is limited to characters a-z (lowercase ASCII), 0-9, and dash (-). |
| **description** (optional) | string | A description that provides more details and context about the Relationship, potentially including its purpose and its key characteristics. |
| **source\_ref** (required) | identifier | The **id** of the source (from) object. |
| **target\_ref** (required) | identifier | The **id** of the target (to) object. |

### ​2.1.3.​ Relationships

There are no relationships explicitly defined between the Relationship object and other objects, other than those defined as common relationships. The first section lists the embedded relationships by property name along with their corresponding target.

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship name or, as with open vocabularies, user-defined names.

|  |  |  |  |
| --- | --- | --- | --- |
| **Embedded Relationships** | | | |
| **created\_by\_ref** | | source | |
| **object\_markings\_refs** | | marking-definition | |
| **Common Relationships** | | | |
| duplicate-of, derived-from, related-to | | | |

## ​2.2.​ Sighting

**Type Name:** sighting

A sighting denotes the fact that some entity in cyber threat intelligence (e.g., an indicator, malware, tool, threat actor, etc.) was seen. Sightings are used to track who and what are being targeted, how attacks are carried out, and to track trends in attack behavior.

Sighting is a special type of SRO: it's a relationship that contains extra fields not present on the generic Relationship object. These extra fields are included to represent data specific to sighting relationships (e.g., count, representing how many times something was seen), but for other purposes the Sighting can be treated as a Relationship with a name of "sighting-of". Sighting is captured as a relationship because you can't have a sighting unless you have something that has been sighted. Sighting does not make sense without the relationship to what was sighted.

Sighting relationships relate three aspects of the sighting:

* What was sighted, such as the Indicator, Malware, Campaign, or other object (**sighting\_of\_ref**)
* Who sighted it and/or where it was sighted, represented as a Victim Target (**where\_sighted\_refs**)
* What was actually seen on systems and networks, represented as Observed Data (**observed\_data\_refs**).

What was sighted is required: a sighting doesn't make sense unless you say what you saw. Who sighted it, where it was sighted, and what was actually seen are optional: in many cases it isn't necessary to provide that level of detail in order to provide value.

Sightings are used whenever any intelligence entity (STIX Domain Object) has been "seen". In some cases, the object creator wishes to convey very little information about the sighting: the details might be sensitive, but the fact that they saw a malware instance or threat actor could still be very useful. In other cases, providing the details may be helpful or even necessary: saying exactly which of 1000 IP addresses in an indicator were sighted is helpful to track which of those IPs remain malicious.

Sighting is distinct from Observed Data in that Sighting is an intelligence assertion ("I saw this threat actor") while Observed Data is simply information ("I saw this file"). When you combine them by included the linked Observed Data (**observed\_data\_refs**) from a Sighting, you can say "I saw this file, and that makes me think I saw this threat actor". Although **confidence** is currently reserved, notionally confidence would be added to Sighting (the intelligence relationship) but not to Observed Data (the raw information).

### ​2.2.1.​ Properties

|  |  |  |
| --- | --- | --- |
| **Common Properties** | | |
| **type, id, created\_by\_ref, created, modified, version, revoked, labels, external\_references, object\_markings\_refs, granular\_markings** | | |
| **Sighting Specific Properties** | | |
| **first\_seen, first\_seen\_precision, last\_seen, last\_seen\_precision, count, sighting\_of\_ref, observed\_data\_refs, where\_sighted\_refs, summary** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this field **MUST** be sighting |
| **first\_seen** (optional) | timestamp | The beginning of the time window during which the SDO referenced by the sighting\_of\_ref property was sighted. |
| **first\_seen\_precision** (optional) | timestamp-precision | The precision of the **first\_seen** timestamp. |
| **last\_seen** (optional) | timestamp | The end of the time window during which the SDO referenced by the sighting\_of\_ref property was sighted. |
| **last\_seen\_precision** (optional) | timestamp-precision | The precision of the **last\_seen** timestamp. |
| **count** (optional) | number | This **MUST** be 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.  observed-data has a similar property called **number\_observed**, which refers to the number of times the data was observed. These counts refer to different concepts and are distinct. |
| **sighting\_of\_ref** (required) | identifier | An ID reference to the object that has been sighted (i.e. Indicator or Malware).  For example, if this is a sighting of an Indicator, that indicator’s ID would be the value of this property. |
| **observed\_data\_refs** (optional) | list of type identifier | A list of ID references to the Observed Data objects that contain the raw cyber data for this Sighting.  For example, a Sighting of an Indicator with an IP address could include the Observed Data for the network connection that the Indicator was used to detect. |
| **where\_sighted\_refs** (optional) | list of type identifier | The ID of the Victim Target objects of the entities that saw the sighting.  Omitting the **where\_sighted\_refs** field does not imply that the sighting was seen by the object creator. To indicate that the sighting was seen by the object creator, a Victim Target representing the object creator **MUST** be listed in **where\_sighted\_refs**. |
| **summary** (optional) | boolean | The **summary** property indicates whether the Sighting should be considered summary data. Summary data is an aggregation of previous Sightings reports and should not be considered primary source data. Default value is false. |

### ​2.2.2.​ Relationships

There are no relationships explicitly defined between the Sighting object and other objects, other than those defined as common relationships. The first section lists the embedded relationships by property name along with their corresponding target.

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship name or, as with open vocabularies, user-defined names.

|  |  |  |  |
| --- | --- | --- | --- |
| **Embedded Relationships** | | | |
| **created\_by\_ref** | | source | |
| **object\_markings\_refs** | | marking-definition | |
| **sighting\_of\_ref** | | identifier | |
| **observed\_data\_refs** | | identifier | |
| **where\_sighted\_refs** | | identifier | |
| **Common Relationships** | | | |
| duplicate-of, derived-from, related-to | | | |

​

### ​2.2.3.​ Examples

*Sighting of Indicator, without Observed Data*

{

"type": "sighting",

"id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c75",

"created\_by\_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",

"created": "2016-04-06T20:08:31Z",

"modified": "2016-04-06T20:08:31Z",

"version": 1,

"sighting\_of\_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f"

}

*Sighting of Indicator, with Observed Data (what exactly was seen) and where it was seen*

[

{

"type": "sighting",

"id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c75",

"created\_by\_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",

"created": "2016-04-06T20:08:31Z",

"modified": "2016-04-06T20:08:31Z",

"version": 1,

"sighting\_of\_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",

"observed\_data\_refs": [ "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf" ],

"where\_sighted\_refs": [ "source--b67d30ff-02ac-498a-92f9-32f845f448ff" ],

"first\_sighted": "2015-12-21T19:00:00Z",

"last\_sighted": "2015-12-21T19:00:00Z",

"count": 50

},

{

"type": "observed-data",

"id": "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf",

"created\_by\_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",

"created": "2016-04-06T19:58:16Z",

"modified": "2016-04-06T19:58:16Z",

"version": 1,

"start": "2015-12-21T19:00:00Z",

"stop": "2016-04-06T19:58:16Z",

"count": 50,

"cybox": {

"objects": {

"1": {

"type": "file-object",

"file\_name": "malware.exe",

"hashes": {

"md5": "3773a88f65a5e780c8dff9cdc3a056f3",

"sha1": "cac35ec206d868b7d7cb0b55f31d9425b075082b"

}

}

}

]

}

]

# ​3.​ Bundle

**Type Name:** bundle

A Bundle is a collection of arbitrary STIX Objects grouped together in a single container. A Bundle does not have any semantic meaning and objects in the same Bundle are not necessary related. Objects **MUST NOT** be considered related by virtue of being in the same Bundle.

A bundle used to group STIX Objects. It can be thought of as an envelope, enabling the delivery or representation of multiple STIX Objects in a single document. It does not have any of the Common Properties other than the **type** and **id** fields. Bundle is transient and implementations should not assume that other implementations will treat it as a persistent object.

### ​3.0.1.​ Properties

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this field **MUST** be bundle |
| **id** (required) | identifier | An identifier for this bundle. The **id** field for the bundle is designed to help tools that may need it for processing, but tools are not required to store or track it. Consuming tools should not rely on the presence of this field. |
| **spec\_version** (required) | spec-version-enum | The version of the STIX specification used to represent the content in this bundle. This enables non-TAXII transports or other transports without their own content identification mechanisms to know the version of STIX content. |
| **attack\_patterns** (optional) | list of type attack-pattern | Specifies a set of one or more Attack Patterns. |
| **campaigns** (optional) | list of type campaign | Specifies a set of one or more Campaigns. |
| **courses\_of\_action** (optional) | list of type course-of-action | Specifies a set of one or more Courses of Action that could be taken in regard to one of more cyber threats. |
| **incidents** (optional) | list of type incidents | Specifies a set of one or more cyber threat Incidents. |
| **indicators** (optional) | list of type indicator | Specifies a set of one or more cyber threat Indicators. |
| **infrastructures** (optional) | list of type infrastructure | Specifies a set of one or more Infrastructure. |
| **intrusion\_sets** (optional) | list of type intrusion-set | Specifies a set of one or more cyber threat Intrusion Sets. |
| **malware** (optional) | list of type malware | Specifies a set of one or more Malware. |
| **marking\_definitions** (optional) | list of type marking-definition | Specifies a set of one or more Marking Definitions. |
| **observed\_data** (optional) | list of type observed-data | Specifies a set of one or more piece of Observed Data. |
| **relationships** (optional) | list of type relationship | Specifies a set of one or more relationships between SDOs. |
| **reports** (optional) | list of type report | Specifies a set of one or more reports. |
| **sightings** (optional) | list of type sighting | Specifies a set of one or more sightings. |
| **sources** (optional) | list of type source | Specifies a set of one or more individual or organizational sources |
| **threat\_actors** (optional) | list of type threat-actor | Specifies a set of one or more Threat Actors. |
| **tools** (optional) | list of type tool | Specifies a set of one or more Tools. |
| **victim\_targets** (optional) | list of type victim-target | Specifies a set of one or more Victim Targets. |
| **vulnerabilities** (optional) | list of type vulnerability | Specifies a set of one or more Vulnerability. |
| **custom\_objects** (optional) | list of type custom-object | Specifies a list of one or more custom objects. |

### ​3.0.2.​ Relationships

Bundle is not a STIX Object and **MUST NOT** have any relationships to it or from it.

### ​3.0.3.​ Examples

{

"type": "bundle",

"id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",

"spec\_version": "2.0”,

"indicators": [

{

"type": "indicator",

"id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",

"created\_by\_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",

"created": "2016-04-29T14:09:00.123456Z",

"modified": "2016-04-29T14:09:00.123456Z",

"version": 1,

"object\_marking\_refs": ["marking-definition--089a6ecb-cc15-43cc-9494-767639779123"],

"name": "Poison Ivy Malware",

"description": "This file is part of Poison Ivy",

"pattern": "file-object.hashes.md5 = '3773a88f65a5e780c8dff9cdc3a056f3'"

}

],

"marking\_definitions": [

{

"type": "marking-definition",

"id": "marking-definition--089a6ecb-cc15-43cc-9494-767639779123",

"created": "2016-02-19T09:11:01Z",

"modified": "2016-02-19T09:11:01Z",

"version": 1",

"definition": {

"type": "tlp",

"tlp": "green"

}

}

]

}

1. NIST SP 800-83. http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf. [↑](#footnote-ref-0)
2. Malware Attribute Enumeration and Characterization. http://maecproject.github.io. [↑](#footnote-ref-1)