STIX 2.0 Specification - Pre-Draft

TLO - Standard TLOs - Version 0.2

Document Table of Contents

Document Development Status

TODO - This section should be removed from the document prior to completion. It is included here to help visually track where things are at in the process.

Each physical documents contains a table that defines 4 levels of development for each TLO and CTI concept. The first level is called Concept. Content coming in to one of the documents starts as a Concept. Once the community starts to work on it it will move to Development. During this phase, the group will flesh out the design and come up with normative text. As the group comes to general consensus the TLO will move to a Review phase. During this phase the community can comment and offer suggestions on the normative text and design. After a period of time of no comments or feedback, the TLO will move to its final stage of Draft.

Object / Concept	Status	MVP
`asset`	Concept	Undecided
`campaign`	Concept	Yes
`course-of-action`	Concept	Yes
`cybox-container`	Concept	Yes
`external-reference`	Concept	Yes
`identity`	Concept	Yes
`incident`	Concept	Yes
`indicator`	Development	Yes
`observation`	Development	Yes
`sighting`	Development	Yes
`threat-actor`	Concept	Yes
`tool`	Concept	Undecided

1. Top Level Objects

1.1. Asset

Type Name: `asset`	**Status:** Concept **MVP**: Undecided

The Asset object is used to describe something that belongs to an organization (either friendly or hostile). In many cases this is computing infrastructure (hosts, networks, applications), but in other cases it could describe non-computing assets like personnel, data, or capital.

Open Questions:

- Is using something like CIM enough, and is asset MVP?
- Definition is vague
- What properties do we include?
    - IP address
    - Hostname
    - URL/FQDN (if external)
    - Asset ID (if internal)
    - Serial # (if internal)
- The state of being compromised and whether the owner is aware is kind of related to the incident, do they really belong on the asset itself?
- Technical characteristics via CybOX are not well defined, need to clarify or remove.

1.1.1. Properties

STIX TLO Common Properties		
`type, id, created_by_ref, created_time, revision, modified_time, revoked, revision_comment, confidence, object_markings_refs, granular_markings`		
Property Name	**Type**	**Description**

type (required)	`string`	(Overrides `stix-core`) The value of this field **MUST** be `asset`
title (optional)	`string`	A human readable title
description (optional)	`string`	A human readable description
kind_of_asset (required)	`asset-kind-cv`	What type of asset this Asset object represents. Field purloined from VERIS Asset classification.
kind_of_asset_ext (optional)	`vocab-ext`	Specifies alternate values for the **kind** property
compromised (optional)	boolean	Is the asset compromised?
owner_aware (optional)	boolean	Is the owner aware the asset is compromised?
technical_characteristics (optional)	*CybOX Characterization*	The technical characteristics of this asset

Use the “compromised-by” relationship from a Threat Actor to describe who compromised the asset. The “owned-by” and “managed-by” relationships (pointing to an Identity) are used to characterize who owns and manages the asset.

1.1.2. Relationships

These are the default relationships defined between the Asset Object and other objects.

Inherited From		**Inherited Kinds of Relationships**
`stix-core`		`duplicate-of`, `other`
Kind of Relationship	**Target**	**Description**
`compromised-by`	`threat-actor`	Relates the Asset to the Threat Actor that compromised the Asset.
`managed-by`	`identity`	Relates the Asset to the Organization or Individual that manages the Asset.
`owned-by`	`identity`	Relates the Asset to the Organization or Individual that owns the Asset.

`evidenced-by`	`observation`	Relates the Asset to an Observation providing evidence that backs up the assertions provided in this Object.
`part-of-malicious-infrastructure`	`malicious-infrastructure`	Relates the Asset as being used as part of Malicious Infrastructure run by a Threat Actor.

1.2. Campaign

Type Name: `campaign`	**Status:** Concept **MVP**: Undecided

Campaign is used to describe a pattern of malicious activity by one or more threat actors with a particular intent over a period of time. For example, a campaign would be used to describe a banking criminal's attack against the customers of ACME Bank in the United States in 2015.

Open Questions:

- Do we use exact timestamps to represent first seen/last seen, or continue with the status CV.
- We need to have a general conversation about impact, see: https://docs.google.com/document/d/1HJqhvzO35h62gQGPvghVRIAtQrZn3_J__0UcDAj-NXY/edit#heading=h.vby6r0avsvz5

1.2.1. Properties

STIX TLO Common Properties		
`type, id, created_by_ref, created_time, revision, modified_time, revoked, revision_comment, confidence, object_markings_refs, granular_markings`		
Property Name	**Type**	**Description**
`type` (required)	`string`	(Overrides `stix-core`) The value of this field **MUST** be `campaign`.

title (optional)	string	A human readable title
description (optional)	string	A human readable description
severity (reserved)	RESERVED	RESERVED FOR FUTURE USE
status (optional)	campaign-status-cv	The current status of this campaign (historic, current, future).
status_ext	vocab-ext	Specifies alternate values for the **status** property

1.2.2. Relationships

These are the default relationships defined between the Campaign Object and other objects.

Inherited From		Inherited Kinds of Relationships
stix-core		duplicate-of, other
Kind of Relationship	**Target Type**	**Description**
attributed-to	threat-actor	Relates the Campaign to a Threat Actor that is associated with this Campaign.
activity	course-of-action	Relates examples of what you can do to protect yourself when you see this Campaign.
evidenced-by	observation	Relates the Campaign to the an Observation providing evidence that backs up the assertions provided in this Object.

1.3. Course of Action

Type Name: course-of-action	**Status:** Concept **MVP**: Undecided

Course of Action describes a response action to a cyber threat. Courses of Action may be pre-emptive, and intended to prevent a future attack; or responsive, and intended to remediate a successful attack. Courses of Action may be machine readable or human readable.

Open Questions:

- Need to define how extensions work generally, as structured COA is an extension
- Need to review business impact and make sure it is consistent with other uses of impact (understanding that it's slightly different because COAs are applied to yourself)
- Mark has a question on structured_coas: IMHO this should be a list of MIME entities perhaps with some metadata. PDFs are one type of course of action (and are structured/non-structured intended to be captured in the same list?)

1.3.1. Properties

STIX TLO Common Properties		
`type`, `id`, `created_by_ref`, `created_time`, `revision`, `modified_time`, `revoked`, `revision_comment`, `confidence`, `object_markings_refs`, `granular_markings`		
Property Name	**Type**	**Description**
`type` (required)	`string`	(Overrides `stix-core`) The value of this field **MUST** be `course-of-action`
`title` (optional)	`string`	A human readable title
`description` (optional)	`string`	A human readable description
`stage` (optional)	`coa-stage-cv`	Whether this is a preemptive remedy or a response action.
`stage_ext` (optional)	`vocab-ext`	Specifies alternate values for the **`stage`** property
`kind_of_coa` (optional)	`coa-kind-cv`	The type of response action.
`kind_of_coa_ext` (optional)	`vocab-ext`	Specifies alternate values for the **`kind`** property

structured_coa (optional)	`object`	A structured representation of the COA actions meant for automation.
business_impact (optional)	`statement (high-medium-low-cv)`	The impact on operations as a result of carrying out this COA.
cost (optional)	`statement (high-medium-low-cv)`	The cost to the business as a result of carrying out this COA.

1.3.2. Relationships

These are the default relationships between the Course-of-action Object and other objects.

Inherited From		Inherited Kinds of Relationships
`stix-core`		`duplicate-of`, `other`
Kind of Relationship	**Target**	**Description**
`evidenced-by`	`observation`	Relates the Course-of-action to an Observation providing evidence that backs up the assertions provided in this Object.

1.4. CybOX Container

CybOX containers are used to capture cyber objects, actions, and relationships as defined by CybOX. This can be treated as a generic CybOX container but adds STIX TLO semantics on top of it.

Type Name: `cybox-container`	**Status:** Concept **MVP**: Yes

1.4.1. 2.4.1.Properties

STIX TLO Common Properties

type, id, created_by_ref, created_time, revision, modified_time, revoked, revision_comment, confidence, object_markings_refs, granular_markings		
Property Name	**Type**	**Description**
type (required)	`string`	(Overrides `stix-core`) The value of this field **MUST** be `reference`
objects (optional)	`array` of type `cybox-object`	(Inherits from CybOX) The list of CybOX objects in this container.
actions (optional)	`array` of type `cybox-action`	(Inherits from CybOX) The list of CybOX actions in this container.
relationships (optional)	`array` of type `cybox-relationship`	(Inherits from CybOX) The list of CybOX relationships in this container.

1.4.2. Relationships

These are the default relationships between the CybOX Container and other objects.

Inherited From		**Inherited Kinds of Relationships**
`stix-core`		`duplicate-of`, `other`
Kind of Relationship	**Target**	**Description**
`evidenced-by`	`observation`	Relates a CybOX Object or group of Objects within a CybOX Container to a TTP.

1.5. External Reference

Type Name: `external-reference`	**Status:** Concept **MVP**: Undecided

External references are used to describe pointers to information represented outside of STIX. For example, an incident could use an external reference to indicate an ID for that incident in an external database or a report could use references to represent source material.

Open Questions:

- Should this stay as a separate TLO or just become a part of CTI core (as an array of references)? This has already been discussed at length, we'll have to make sure not to ignore previous consensus.

1.5.1. Properties

STIX TLO Common Properties		
`type, id, created_by_ref, created_time, revision, modified_time, revoked, revision_comment, confidence, object_markings_refs, granular_markings`		
Property Name	**Type**	**Description**
`type` (required)	`string`	(Overrides `stix-core`) The value of this field **MUST** be `reference`
`title` (optional)	`string`	A human readable title
`description` (optional)	`string`	A human readable description
`reference_url` (optional)	`url`	A URL reference to an external resource.
`external_identifier` (optional)	`string`	An identifier for the external reference content.
`defining_context` (optional)	`string`	The context within which the external_identifier is defined (system, registry, organization, etc.)

1.5.2. Relationships

Status: stub

1.6. Incident

Type Name: `incident`	**Status:** Concept **MVP**: Undecided

Incidents are discrete instances of threats affecting an organization along with information discovered or decided during an incident response investigation. They consist of data such as time-related information, parties involved, assets affected, impact assessment, related Indicators, related observables, leveraged attack techniques, attribution, intended effects, nature of compromise, responses taken or recommended, and logs of actions taken.

1.6.1. Properties

Status: stub

1.6.2. Relationships

These are the default relationships between the Incident Object and other objects.

Inherited From		**Inherited Kinds of Relationships**
`stix-core`		`duplicate-of`, `other`
Kind of Relationship	**Target**	**Description**
`part-of`	`Campaign`	Relates the Incident to a Campaign to enable tagging it as being an instance of an individual attack performed as part of a Campaign.
`evidenced-by`	`Observation`	Relates the Incident to an Observation providing evidence that backs up the assertions provided in this Object.

1.7. Identity

Type Name: `identity`	**Status:** Concept **MVP**: Undecided

Identity represents information about individuals (people), groups, and organizations. This came from the Information Source construct in STIX 1.2. Information Source was broken up into External Reference, Identity, and Tool. This should be reviewed.

- Identity = single company
- Identity = individual person
- Identity = group
- Identity = sector (CIKR)
- Identity = sector (finance)
- Need to represent assets for an identity (ASN, public IP space)

Open Questions:

1. This should be discussed with Incident, Asset, Victim Targeting, etc.
2. We also need to discuss the properties that we include for identities (both MVP and post-MVP)
    a. Allan has suggested:
        i. username
        ii. soc #
        iii. phone number
        iv. first name/last name
        v. userid #

1.7.1. Properties

STIX TLO Common Properties		
`type, id, created_by_ref, created_time, revision, modified_time, revoked, revision_comment, confidence, object_markings_refs, granular_markings`		
Property Name	**Type**	**Description**
`type` (required)	`string`	(Overrides `stix-core`) The value of this field **MUST** be `identity`
`title` (optional)	`string`	A human readable title
`description` (optional)	`string`	A human readable description

ciq-specification (optional)	`string`	A string containing OASIS CIQ-PIL schema 3.0 XML formatted content describing the Identity in more detail.

1.7.2. Relationships

These are the default relationships between the Identity Object and other objects.

Inherited From		**Inherited Kinds of Relationships**
`stix-core`		`duplicate-of`, `other`
Kind of Relationship	**Target**	**Description**
`tracked-as`	`threat-actor`	Relates the Identity to a Threat Actor to enable tracking of their actions.
`persona-of`	`threat-actor`	Relates the Identity as a persona that the Threat Actor uses.
`evidenced-by`	`observation`	Relates the Identity to an Observation providing evidence that backs up the assertions provided in this Object.

Note: There is also a direct reference to identity embedded in all top-level objects (inherited from `stix-core`*),* **`created_by_ref`***, that links each TLO with the Identity of the organization or individual that created the TLO.*

1.8. Indicator

Type Name: `indicator`	**Status:** Development **MVP**: Yes

Indicators are used for detecting malicious activity. The Indicator object is a STIX TLO that uses the CybOX patterning grammar to describe something (as a general expression or exact match) that you might see or should look for and includes an assertion of what it means if you see it.

1.8.1. Properties

STIX TLO Common Properties		
type, id, created_by_ref, created_time, revision, modified_time, revoked, revision_comment, confidence, object_markings_refs, granular_markings		
Property Name	**Type**	**Description**
type (required)	`string`	(Overrides `stix-core`) The value of this field **MUST** be `indicator`
title (optional)	`string`	A human readable title
description (optional)	`string`	A human readable description
pattern (required)	`pattern-expression`	TODO: definition of pattern-expression in the playground document (worked by CybOX patterning mini-group)
labels (required)	`array` of type `string`	Specifies the type for this Indicator.
start_time (optional)	`timestamp`	The start time for which this indicator is valid.
end_time (optional)	`timestamp`	The end time for which this indicator is valid.
severity (reserved)	`RESERVED`	RESERVED FOR FUTURE USE
decay_rate (optional)	`< to do >`	A hint to help people understand what the decay rate is. < to do fix this description >

1.8.2. Relationships

These are the default relationships defined between the Indicator Object and other objects.

Inherited From	Inherited Kinds of Relationships
`stix-core`	`duplicate-of`, `other`

Kind of Relationship	Target	Description
`indicates`	`threat-actor`, `attack-pattern`, `exploit`, `malicious-infrastructure`, `malicious-tool`, `malware`, `persona`, `victim-targeting`, `configuration`, `vulnerability`, `weakness`, `campaign`, `kill-chain-phase`	Relates the indicator to the threat that it indicates. For example, you can send a relationships that points from an Indicator to some Malware with a value of "indicates". What that means is if you see that indicator it indicates that you have that piece of malware running on your computer / in your network to the level of confidence expressed in the relationship.
`suggested-coa-of`	`course-of-action`	Relates the Indicator to a Course of Action to allow Organizations to protect themselves against the threat indicated when this Indicator alerts.
`uses`	`exploit`	Relates the Indicator to an exploit that can exploit the vulnerability/misconfiguration or weakness.
`evidenced-by`	`observation`	Relates the Indicator to an Observation providing evidence that backs up the assertions provided in this Object. The evidenced-by relationship allows producers to a link to the Observations that they used to determine what the Indicator needed to match to trigger. The same Observation can be related with both an evidenced-by relationship AND a sighting-of relationship.

1.8.3. Examples

Indicator Itself, with Context

```
[
```

```
  {
    "type": "indicator",
    "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "created_time": "2016-04-06T20:03:48Z",
    "created_by_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "title": "Poison Ivy Malware",
    "description": "This file is part of Poison Ivy",
    "pattern": "file-object.hashes.md5 = '3773a88f65a5e780c8dff9cdc3a056f3'"
  },
  {
    "type": "relationship",
    "id": "relationship--44298a74-ba52-4f0c-87a3-1824e67d7fad",
    "created_time": "2016-04-06T20:06:37Z",
    "created_by_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "source_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "target_ref": "malware--31b940d4-6f7f-459a-80ea-9c1f17b5891b",
    "kind_of_relationship": "indicates"
  },
  {
    "type": "malware",
    "id": "malware--31b940d4-6f7f-459a-80ea-9c1f17b5891b",
    "created_time": "2016-04-06T20:07:09Z",
    "created_by_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "title": "Poison Ivy"
  }
]
```

1.9. Observation

Type Name: `observation`	**Status:** Development **MVP**: Yes

Observations document actions and objects that were observed at a certain time. The Observation object uses CybOX objects to describe something that was seen and is a container or wrapper (entry point) for CybOX data in STIX.

1.9.1. Properties

STIX TLO Common Properties		
type, id, created_by_ref, created_time, revision, modified_time, revoked, revision_comment, confidence, object_markings_refs, granular_markings		
Property Name	**Type**	**Description**

type (required)	`string`	(Overrides `stix-core`) The value of this field **MUST** be `observation`
start (required)	`timestamp`	The time of the start of this observation.
end (required)	`timestamp`	The time of the end of this observation. For single point in time observations, this should match the **start** time. If the count equals 1, then the `first_seen` and `last_seen` **MUST** be equal.
count (required)	`integer`	This is an integer between 0 and 999,999,999 inclusive.
cybox (required)	`array` of type `cybox`	The CybOX content that describes what was seen. If you can not share the CybOX data you must use NULL

1.9.2. Relationships

NONE

1.9.3. Examples

Observation of a file object

```
{
  "type": "observation",
  "id": "observation--b67d30ff-02ac-498a-92f9-32f845f448cf",
  "created_time": "2016-04-06T19:58:16Z",
  "created_by_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",
  "start": "2015-12-21T19:00:00Z",
  "end": "2015-12-21T19:00:00Z",
  "count": 50,
  "cybox": [
      {
      "type": "file-object",
      "file_name": "malware.exe",
      "hashes": {
      "md5": "3773a88f65a5e780c8dff9cdc3a056f3",
      "sha1": "cac35ec206d868b7d7cb0b55f31d9425b075082b"
```

```
    }
  ]
}
```

1.10. Sighting

Type Name: `sighting`	**Status:** Development **MVP**: Yes

Sightings represent events of security interest, often detected via indicators or analytics, and are used to communicate that the indicator or analytic was "sighted" and/or to request further analysis. The Sighting object describes something (an event) that the producer would like to provide or request additional context about. It can be tied to how it was discovered (indicator, analytic, or even a description of human analysis) and to what was actually seen (set of observations). It could also be tied to other objects to indicate that, for example, a campaign was spotted. Sighting also has count to help with scale issues. Sightings differ from Observations in that you can tie a Sighting to something that triggered it, whereas the Observation is simply the CybOX wrapper in STIX.

1.10.1. Properties

STIX TLO Common Properties		
`type, id, created_by_ref, created_time, revision, modified_time, revoked, revision_comment, confidence, object_markings_refs, granular_markings`		
Property Name	**Type**	**Description**
`type` (required)	`string`	(Overrides `stix-core`) The value of this field **MUST** be `sighting`
`sighting_of_ref` (required)	`identifier`	The ID of the object (TLO) that was sighted, but not this exact TLO.
`observation_refs` (required)	`array` of type `identifier`	The IDs of the Observations that were seen. This is used when for example you have an indicator watch list with hundreds of IPs and you need to sight a single IP address. There **MUST** be at least one ID present.

where_sighted_refs (optional)	array of type identifier	The ID of the identity object of the entity that saw the sighting.

1.10.2. Relationships

NONE

1.10.3. Examples

Sighting of Indicator, without Observations

```
{
  "type": "sighting",
  "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c75",
  "created_time": "2016-04-06T20:08:31Z",
  "created_by_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",
  "sighting_of_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f"
}
```

Sighting of Indicator, with Observation (what exactly was seen)

```
[
  {
    "type": "sighting",
    "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c75",
    "created_time": "2016-04-06T20:08:31Z",
    "created_by_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "sighting_of_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "observation_refs": [ "observation--b67d30ff-02ac-498a-92f9-32f845f448cf" ],
    "where_sighted_refs": [ "source--b67d30ff-02ac-498a-92f9-32f845f448ff" ]
  },
  {
    "type": "observation",
    "id": "observation--b67d30ff-02ac-498a-92f9-32f845f448cf",
    "created_time": "2016-04-06T19:58:16Z",
    "created_by_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "start": "2015-12-21T19:00:00Z",
    "stop": "2015-12-21T19:00:00Z",
    "count": 50,
    "cybox": [
      {
        "type": "file-object",
        "file_name": "malware.exe",
        "hashes": {
          "md5": "3773a88f65a5e780c8dff9cdc3a056f3",
          "sha1": "cac35ec206d868b7d7cb0b55f31d9425b075082b"
        }
```

```
      }
    ]
  }
]
```

Sighting of Analytic, with Observation (what exactly was seen)

```
[
  {
    "type": "sighting",
    "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c75",
    "created_time": "2016-04-06T20:08:31Z",
    "created_by_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "sighting_of_refs": "reference--9623a193-6a3a-4bed-aede-d9fb8471ea0d",
    "observation_refs": [ "observation--b67d30ff-02ac-498a-92f9-32f845f448cf" ]
  },
  {
    "type": "external-reference",
    "id": "external-reference--9623a193-6a3a-4bed-aede-d9fb8471ea0d",
    "created_time": "2016-04-06T20:15:00+00:00",
    "created_by_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "reference_url": "http://uba_system/the/ml/algo/details/1234",
    "description": "Potentially some human readable description of the analytic or why it
triggered until we can represent it in STIX"
  },
  {
    "type": "observation",
    "id": "observation--b67d30ff-02ac-498a-92f9-32f845f448cf",
    "created_time": "2016-04-06T19:58:16Z",
    "created_by_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "start": "2015-12-21T19:00:00Z",
    "stop": "2015-12-21T19:00:00Z",
    "count": 75,
    "cybox": [
      {
        "type": "file-object",
        "file_name": "malware.exe",
        "hashes": {
          "md5": "3773a88f65a5e780c8dff9cdc3a056f3",
          "sha1": "cac35ec206d868b7d7cb0b55f31d9425b075082b"
        }
      }
    ]
  }
]
```

1.11. Threat Actor

Type Name: `threat-actor`	**Status:** Concept **MVP**: Undecided

A threat actor describes an individual or group with malicious intent.

Open Questions:

- How does threat actor relate to identity (how do you characterize the identity of a threat actor)? Do we use the identity TLO, include identity information inside Threat Actor, etc.?

1.11.1. Properties

STIX TLO Common Properties		
`type, id, created_by_ref, created_time, revision, modified_time, revoked, revision_comment, confidence, object_markings_refs, granular_markings`		
`descriptive-properties`	**`title, description`**	
Property Name	**Type**	**Description**
`type` (required)	`string`	(Overrides `stix-core`) The value of this field **MUST** be `threat-actor`
`title` (optional)	`string`	A human readable title
`description` (optional)	`string`	A human readable description
`severity` (reserved)	`RESERVED`	RESERVED FOR FUTURE USE
`kind_of_threat_actor` (optional)	`statement (threat-actor-kind-cv)`	The kind (type) of this threat actor.
`motivation` (optional)	`statement (threat-actor-motivation-cv)`	The motivation of this threat actor.

sophistication (optional)	`statement (threat-actor-sophistication-cv)`	The sophistication of this threat actor
planning_and_ operational_support (optional)	`statement (planning-and-operations-cv)`	The planning and operational support available to this threat actor.

The real identity of the Threat Actor is related to the Threat Actor via a relationship of value ‘identity-of’. If the Threat Actor has a persona that they use then that is constructed using a relationship between the Identity the persona uses and the the Threat Actor with a value of ‘persona-of’.

1.11.2. Threat Actor Relationships

These are the default relationships between a Threat Actor Object and other objects.

Inherited From		**Inherited Kinds of Relationships**
`stix-core`		`duplicate-of`, `other`
Kind of Relationship	**Target**	**Description**
`identity-of`	`identity`	Relates the Threat Actor to a real Identity that describes who they really are.
`persona-of`	`identity`	Relates the Threat Actor to a fake persona they use to obscure their real identity.
`targeted`	`identity`	Relates the Threat Actor to a Organization or Individual who was targeted by this Threat Actor
`breached`	`identity`	Relates the Threat Actor to a Organization or Individual who was compromised by this Threat Actor
`member-of`	`identity`	The Threat actor is a member of an Organization

`administers`	`campaign`	Relates the Threat Actor to a Campaign as the administrator of a Campaign.
`operates`	`campaign`	Relates the Threat Actor to a Campaign as the operator of a Campaign.
`plans`	`campaign`	Relates the Threat Actor to a Campaign as the planner of a Campaign.
`uses`	`malware, exploit`	Relates the Malware or Exploit as one being used by the Threat Actor to perform attacks. This will enable Organizations to quickly find similar Threat Actors that uses the same exploits.
`evidenced-by`	`observation`	Relates the Threat Actor to an Observation that demonstrates involvement from the threat actors described in this Object.
`compromises`	`asset`	Relates the Threat Actor to an Asset that is delivered by or communicates with this Asset.
`controls-malicious-infrastructure`	`malicious-infrastructure`	Relates the Threat Actor to Malicious Infrastructure that is delivers or communicates with Malware.
`administers-malicious-infrastructure`	`malicious-infrastructure`	Relates the Threat Actor to Malicious Infrastructure that is delivers or communicates with Malware as an administrator.
`uses-attack-pattern`	`attack-pattern`	Relates the Threat Actor to an Attack Pattern that describes what it does.
`target-selection-of`	`victim-targeting`	Relates the Threat Actor to a type of Victim Targeting
`member-of`	`threat-actor`	Allows recording that a Threat Actor is a member of another Threat Actor.

1.12. Tool

Type Name: `tool`	**Status:** Concept **MVP**: Undecided

Tool (STIX 1.2) is intended to characterize the properties of a hardware or software tool, including those related to instances of its use. It is meant to be used to describe a tool that was used to perform a threat analysis (source of analysis) or create STIX content (source of the STIX content).

Open Questions:

1. Is this necessary? Do people need to represent which tools they used to perform analysis or create STIX content?
2. How does it relate to malicious tool? Is malicious-tool a totally separate object or does it go away (merged into this) and we use relationships to indicate whether tools are malicious?
3. Allan: Could this just be a hash of the tool?

1.12.1. Properties

<STUB>

1.12.2. Relationships

Status: stub