STIX 2.0 Specification - Pre-Draft

TLO - Non-Cyber Concepts - Version 0.1

Document Table of Contents

1. Document Development Status

Object / Concept	Status	MVP	Description
`package`	Development	Yes	A grouping of related TLOs.
`report`	Development	Yes	Context describing a set of related cyber threat intelligence content.
`relationship`	Development	Yes	< add text >
`marking-definition`	Review	Yes	< add text >

2. Top Level Objects

2.1. STIX Package

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

A collection of TLOs used specifically for transport.
< to do, please add descriptions >

2.1.1. Properties

Inherits From	**Inherited Properties**	
`stix-core`	**`type, id, spec_version, created_time, created_by_ref, object_markings_refs, granular_markings`**	
Property Name	**Type**	**Description**
`type` (required)	`string`	Indicates that this object is a STIX Package. The value of this field **MUST** be `package`
`attack_patterns` (optional)	`array` of type `attack-pattern`	Specifies a set of one or more Attack_Pattern TTPs.
`campaigns` (optional)	`array` of type `campaign`	Specifies a set of one or more Campaigns.
`configurations` (optional)	`array` of type `configuration`	Specifies a set of one or more Configuration exploit targets.
`courses_of_action` (optional)	`array` 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.
`exploits` (optional)	`array` of type `exploit`	Specifies a set of one or more Exploit TTPs.
`identities` (optional)	`array` of type `identity`	Specifies a set of one or more identities of individuals or

		organizations.
incidents (optional)	`array` of type `incident`	Specifies a set of one or more cyber threat Incidents.
indicators (optional)	`array` of type `indicator`	Specifies a set of one or more cyber threat Indicators.
kill_chains (optional)	`array` of type `kill-chain`	Specifies a set of one or more Kill Chains.
kill_chain_phases (optional)	`array` of type `kill-chain-phase`	Specifies a set of one or more Kill Chain Phases.
malicious_ infrastructures (optional)	`array` of type `malicious-infrastructure`	Specifies a set of one or more Infrastructure TTPs.
malicious_tools (optional)	`array` of type `malicious-tool`	Specifies a set of one or more Malicious Tool TTPs.
malware (optional)	`array` of type `malware`	Specifies a set of one or more Malware TTPs.
marking_definitions (optional)	`array` of type `marking-definition`	Specifies a set of one or more Marking Definitions.
observations (optional)	`array` of type `observation`	Specifies a set of one or more cyber observations.
personas (optional)	`array` of type `persona`	Specifies a set of one or more Personas.
external-references (optional)	`array` of type `external-reference`	Specifies a set of one or more references to a non-STIX object
relationships (optional)	`array` of type `relationship`	Specifies a set of one or more relationships between top-level objects (TLOs).
reports (optional)	`array` of type `report`	Specifies a set of one or more reports.
sightings (optional)	`array` of type `sighting`	Specifies a set of one or more sightings.
threat_actors (optional)	`array` of type `threat-actor`	Specifies a set of one or more Threat Actors.

tools (optional)	array of type tool	<add text>
victim_targetings (optional)	array of type victim-targeting	Specifies a set of one or more Victim Targeting TTPs.
vulnerabilities (optional)	array of type vulnerability	Specifies a set of one or more Vulnerability exploit targets.
weaknesses (optional)	array of type weakness	Specifies a set of one or more Weakness exploit targets.

2.1.2. Relationships

NONE

2.2. Report

Type Name: report	**Status:** Development **MVP**: Yes

A grouping of asserted related TLOs for purposes of reporting.

2.2.1. Properties

Inherits From	Inherited Properties	
stix-core	**type, id, spec_version, created_time, created_by_ref, object_markings_refs, granular_markings**	
descriptive-properties	**title, description**	
Property Name	**Type**	**Description**
type (required)	string	(Overrides cti-core) The value of this field **MUST** be report
title (required)	string	(Overrides descriptive-properties) A human readable title for the construct.
intents (required)	array of type report-intent-cv	Specifies the intended purposes or uses of this Report.
intents_ext (optional)	array of type	Specifies alternate intended purposes

	`vocab-ext`	or uses of this Report.
`report_contains_refs` (required)	`array` of type `identifier`	Specifies the objects that are in this Report.
`confidence` (optional)	`< TO DO >`	The confidence that the objects contained in this report are related as asserted by the title, description, and intents using *TODO*.

2.2.2. Relationships

There are no uninherited default relationships defined between the Report Object and other objects.

Inherited From	Inherited Kinds of Relationships
`stix-core`	`derived-from`, `duplicate-of`, `suggested-update`, `related-to`

2.2.3. Examples

```
// Just a report, where the consumer may or may not already have access to the TLOs
{
  "type": "report",
  "id": "report--84e4d88f-44ea-4bcd-bbf3-b2c1c320bcb3",
  "spec_version": "2.0",
  "created_time": "2015-12-21T19:59:11Z",
  "created_by_ref": "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283",
  "title": "The Black Vine Cyberespionage Group",
  "descriptions": ["A simple report with an indicator and campaign"],
  "intents": ["Threat Report"],
  "report_contains_refs": [
  "indicator--26ffb872-1dd9-446e-b6f5-d58527e5b5d2",
  "campaign--83422c77-904c-4dc1-aff5-5c38f3a2c55c"
}


// A full package with a report and the TLOs / Relationships that are part of the report
{
  "type": "package",
  "id": "package--44af6c39-c09b-49c5-9de2-394224b04982",

  "identities": [
    {
```

```
      "type": "identity",
      "id": "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283",
      "name": "Symantec",
    }
  ],

   "reports": [
    {
      "type": "report",
      "id": "report--84e4d88f-44ea-4bcd-bbf3-b2c1c320bcbd",
      "spec_version": "2.0",
      "created_time": "2015-12-21T19:59:11Z",
      "created_by_ref": "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283",
      "title": "The Black Vine Cyberespionage Group",
      "descriptions": ["A simple report with an indicator and campaign"],
      "intents": ["Threat 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_time": "2015-12-21T19:59:17Z",
      "spec_version": "2.0",
      "title": "Some indicator",
      "indicator_types": ["IP Watchlist"],
      "created_by_ref": "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283"
    }
  ],

  "campaigns": [
    {
      "type": "campaign",
      "id": "campaign--83422c77-904c-4dc1-aff5-5c38f3a2c55c",
      "spec_version": "2.0",
      "created_time": "2015-12-21T19:59:17Z",
      "title": "Some Campaign",
      "created_by_ref": "identity--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",
        "from": "indicator--26ffb872-1dd9-446e-b6f5-d58527e5b5d2",
        "to": "campaign--26ffb872-1dd9-446e-b6f5-d58527e5b5d2",
        "kind_of_": "Related Campaign",
        "created_by_ref": "identity--a463ffb3-1bd9-4d94-b02d-74e4f1658283"
    },
  ]
}
```

2.3. Relationship

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

The Relationship object is used to link together other top-level objects, such as Indicator, Observation, Threat Actor and the like. If other top-level objects are considered “nodes” in the graph, the relationship object represents “edges”.

Open Questions:

1. Need to discuss the values of the kind_of_relationship vocab
2. Need to discuss confidence and its controlled vocabulary
3. From Allan, confidence is something that could be applied to multiple object types and data. Should this not be moved to a more general data structure inherited by other objects?

2.3.1. Properties

Inherits From	**Inherited Properties**	
`stix-core`	**`type, id, spec_version, created_time, created_by_ref, object_markings_refs, granular_markings`**	
`descriptive-properties`	**`title, description`**	
Property Name	**Type**	**Description**
`type` (required)	`string`	(Overrides `cti-core`) The value of this field **MUST** be `relationship`

kind_of_relationship (required)	string	The descriptor for this relationship.
kind_of_relationship_ext (optional)	vocab-ext	The descriptor for this relationship, using a non-standard vocabulary.
source_ref (required)	string	The ID of the source (from) object.
target_ref (required)	string	The ID of the target (to) object.
is_directional (required)	boolean	Indicates whether the relationship is directional. For values in the standard vocabulary, this attribute may be hardcoded to a particular value.
confidence	TODO	The confidence in this relationship, using TODO
confidence_ext	vocab-ext	The confidence in this relationship, using a non-standard vocabulary.

2.4. Marking Definition

Type Name: marking-definition	**Status:** Review **MVP**: Yes

<enter description>

Inherits From	Inherited Properties	
stix-core	**type, id, spec_version, created_time, created_by_ref, object_markings_refs, granular_markings**	
Property Name	**Type**	**Description**
type (required)	string	(Overrides cti-core) The value of this field **MUST** be marking-definition
definition_type (required)	string	

`definition` (required)	`object`	The type of marking this represents.
(other fields)	Various	Used to represent the marking itself. This contains other fields as needed to represent the marking data.

2.4.1. Examples

```
{
  "type": "marking-definition",
  "id": "marking-definition--089a6ecb-cc15-43cc-9494-767639779123",
  "spec_version": "2.0",
  "created_time": "2016-02-19T09:11:01Z",
  "definition_type": "tlp",
  "definition": {
    "tlp": "GREEN"
  }
}

{
  "type": "marking-definition",
  "id": "marking-definition--089a6ecb-cc15-43cc-9494-767639779124",
  "spec_version": "2.0",
  "created_time": "2016-02-19T09:11:01Z",
  "defintion_type": "isa",
  "definition": {
    "classification": "UNCLASSIFIED",
    "caveats": []
  }
}
```