stix2-elevator Documentation

Release 1.0.0

OASIS Open

Jun 15, 2018

Contents:

The stix2-elevator is a software tool for converting STIX 1.x XML to STIX 2.0 JSON. Due to the differences between STIX 1.x and STIX 2.0, this conversion is best-effort only, During the conversion, stix2-elevator provides information on the assumptions it needs to make to produce valid STIX 2.0 JSON, and what information was not able to be converted.

To convert STIX 2.0 JSON back to STIX 1.x XML use the stix2-slider.

For more information about STIX 2, see the website of the OASIS Cyber Threat Intelligence Technical Committee.

CHAPTER 1

Introduction

The stix2-elevator is a python script written to automatically convert STIX 1.x content to STIX 2.0. It is available at https://github.com/oasis-open/cti-stix-elevator/.

It important to emphasize that the elevator is not for use in a *production* system without human inspection of the results it produces. It is more a tool to explore the differences between STIX 2.0 and STIX 1.x content previously created.

While much of the conversion is straightforward, several assumptions concerning the meaning of the STIX 1.x needed to be made. These are discussed in **'Conversion Issues'_** section.

The elevator produces many messages during the conversion process, that can be reviewed manually to help enhance the automatically produced content, in order to reflect the original content more accurately. A list of these messages can be found in **'Warning Messages'_** section.

CHAPTER 2

Installing

2.1 Requirements

- Python 2.7, or 3.4+
- python-stix and its dependencies

> **Note:** Make sure to use either the latest version of python-stix 1.1.1.x or 1.2.0.x, depending on whether you want to support STIX 1.1.1 or STIX 1.2.

- python-stix2 >= 0.5.1
- stix2-validator >= 0.4.0 and its dependencies
- pycountry >= 1.20
- stixmarx >= 1.0.3

2.2 Installation Steps

Install with pip:

```
$ pip install stix2-elevator
```

This will install all necessary dependencies, including the latest version of python-stix.

If you need to support older STIX 1.1.1 content, install python-stix 1.1.1.x first:

```
$ pip install 'stix<1.2'
$ pip install stix2-elevator
```

You can also install the stix2-elevator from GitHub to get the latest (unstable) version:

```
$ pip install git+https://github.com/oasis-open/cti-stix-elevator.git
```

CHAPTER 3

Command Line Interface

The elevator comes with a bundled script which you can use to elevate STIX 1.1.1 - 1.2.1 content to STIX 2.0 content:

```
usage: stix2_elevator [-h] [--incidents] [--no-squirrel-gaps]
          [--infrastructure]
          [--package-created-by-id PACKAGE_CREATED_BY_ID]
          [--default-timestamp DEFAULT_TIMESTAMP]
          [--validator-args VALIDATOR_ARGS]
          [-e ENABLE] [-d DISABLE] [-s]
          [--message-log-directory MESSAGE_LOG_DIRECTORY]
          [--log-level {DEBUG,INFO,WARN,ERROR,CRITICAL}]
          [-m MARKINGS_ALLOWED] [-p {no_policy,strict_policy}]
          file
```

stix2-elevator v1.2.0

The stix2-elevator is a work-in-progress. It should be used to explore how existing STIX 1.x would potentially be represented in STIX 2.0. Using the current version of the stix2-elevator will provide insight to issues that might need to be mitigated to convert your STIX 1.x content.

positional arguments:

```
file          The input STIX 1.x document to be elevated.
```

optional arguments:

```
-h, --help
              Show this help message and exit

--no-squirrel-gaps
              Do not include STIX 1.x content that cannot be
              represented directly in STIX 2.0 using the description
              property.

--package-created-by-id PACKAGE_CREATED_BY_ID
              Use provided identifier for "created_by_ref"
```

(continues on next page)

(continued from previous page)

```
              properties.

              Example: --package-created-by-id "identity--1234abcd-1a12-12a3-0ab4-
↪1234abcd5678"

--default-timestamp DEFAULT_TIMESTAMP
              Use provided timestamp for properties that require a
              timestamp.

              Example: --default-timestamp "2016-11-15T13:10:35.053000Z"

--validator-args VALIDATOR_ARGS
              Arguments to pass to stix-validator.

              Default: --strict-types

              Example: --validator-args="-v --strict-types -d 212"

-e ENABLE, --enable ENABLE
              A comma-separated list of the stix2-elevator messages
              to enable. If the --disable option is not used, no
              other messages will be shown.

              Example: --enable 250

-d DISABLE, --disable DISABLE
              A comma-separated list of the stix2-elevator messages
              to disable.

              Example: --disable 212,220

-s, --silent
              If this flag is set, all stix2-elevator messages will
              be disabled.

--message-log-directory MESSAGE_LOG_DIRECTORY
              If this flag is set, all stix2-elevator messages will
              be saved to a file. The name of the file will be the
              input file with extension .log in the specified
              directory.

              Note, make sure the directory already exists.

              Example: --message-log-directory "../logs".

--log-level {DEBUG,INFO,WARN,ERROR,CRITICAL}
              The logging output level.

-m MARKINGS_ALLOWED, --markings-allowed MARKINGS_ALLOWED
              Avoid error exit, if these markings types
              (as specified via their python class names) are in the
              content, but not supported by the elevator. Specify as
              a comma-separated list.

              Example: --markings-allowed "ISAMarkingsAssertion,ISAMarkings"

-p {no_policy,strict_policy}, --policy {no_policy,strict_policy}
```

(continues on next page)

(continued from previous page)

```
                The policy to deal with errors
```

Refer to the *Warning Messages* section for all stix2-elevator messages. Use the associated code number to `--enable` or `--disable` a message. By default, the stix2-elevator displays all messages.

Note: disabling the message does not disable any functionality.

CHAPTER 4

Mappings from STIX 1.x to STIX 2.0

This section outlines the disposition of each property of the top-level objects when converted.

For each STIX 1.x object that was converted the following options are possible:

- **STIX 1.x property mapped directly to a STIX 2.0 property.** This property's value is used unaltered in the conversion to 2.0.
- **STIX 1.x property translated into STIX 2.0 property.** This property's value must undergo some minor processing to determine the corresponding content for 2.0.
- **STIX 1.x property mapped using STIX 2.0 relationships.** This property is used to construct a 2.0 relationship object. The "reverse" notation indicates the the STIX 1.x property is found on target object.
- **STIX 1.x property recorded in the STIX 2.0 description property.** This property has no corresponding property in STIX 2.0, but its value can be (optionally) included in the description property of the 2.0 object as text.
- **STIX 1.x property not mapped.** This property will not be included in the converted 2.0 object.

4.1 Top Level Object Mappings

This table describes the mapping between STIX 1.0 and STIX 2.0 top-level objects. Notice that certain object types in STIX 1.x that were not top-level objects are in STIX 2.0 (e.g., Malware).

STIX 1.x object	STIX 2.0 object
Campaign	campaign
Course_Of_Action	course-of-action
et:Vulnerability	vulnerability
et:Weakness	*not converted*
et:Configuration	*not converted*
Incident	*not converted*
Indicator	indicator
Report	report
Observable	observed-data
Package	bundle
Threat Actor	threat-actor
ttp:Attack_Pattern	attack-pattern
ttp:Infrastructure	*not converted*
ttp:Malware	malware
ttp:Persona	*not converted*
ttp:Tool	tool
ttp:Victim_Targeting	identity

4.2 Common Properties

STIX 1.x Properties Mapped Directly to STIX 2.0 Properties

STIX 1.x property	STIX 2.0 property
Description	description
timestamp	modified
Title	name

In STIX 1.x only one timestamp is recorded, whereas in STIX 2.0, there are two properties: `created` and `modified`. The `created` timestamp is not stored in objects in STIX 1.x. The `timestamp` property in STIX 1.x holds the `modified` timestamp.

STIX 1.x Properties Translated to STIX 2.0 Properties

STIX 1.x property	STIX 2.0 property
id	id
Handling	object_markings_refs, granular_markings
Information_Source	created_by_ref, external_references
Type	labels

In STIX 1.x, an `id` contained a "namespace". This was deemed unnecessary in STIX 2.0, therefore they contain no origin information.

- Handling

  Data Markings, called Handling in STIX 1.x, have been completely redesigned for STIX 2.0. STIX 1.x used *xpath*, which was a reasonable choice given its reliance on XML for implementation. However, the use of xpath was very difficult to implement, and was more expressive than was deemed necessary.

  STIX 2.0 introduces two new concepts, object markings and granular markings, which simplify the marking of data. Object markings apply to a whole object, whereas granular markings are specific

to particular properties of an object. The selection of which properties are to be marked is expressed in a serialization-neutral way. The scope of marking definitions is at the object level. There is no marking that can apply to a whole bundle, or report.

- Information_Source

  In STIX 1.x there were several related concepts that were used to identify the sources of information and various parties of interest. Parties of interest are creators of content, victim targets, and other responsible parties. Sources of information could be an individual, organization or some software application. Additionally, it was possible to make references to source material external to STIX, e.g., a citation, URL, or an ID in an external system or repository.

  In STIX 2.0, we have retained the concept of an `IdentityType` object, but do not rely on the OASIS CIQ standard model as STIX 1.x did. The `Identity` object type in STIX 2.0 contains a very streamlined set of properties: `identity_class` to specify if it is an individual or organization, `sectors` to indicate the industry sector that the identity belongs to, and a free text property, `contact_information` to specify such information. All other STIX 1.x propeties are not mapped in the conversion.

  The `InformationSourceType` object was used in STIX 1.x to associate an object with its creator's identity. In STIX 2.0, the common property `created_by_ref` is used, and it must contain the identifier of an `Identity` object.

  The `InformationSourceType` object was also used in STIX 1.x to specify external information. Other properties like `capec_id` of `AttackPatternType`, or `cwe_id` of `VulnerabilityType` were also used for external information, holding the ids of items in repositories or systems external to STIX. In STIX 2.0, the data type `external-reference` is used for all external information.

- Type

  In STIX 2.0, the type of an object is defined to be a specific literal, and is recorded in the `type` property. The type of an object in STIX 1.x was either implicitly defined by its element name or explicitly using xsi:type.

- Kill Chains

  In STIX 1.x, kill chains, with their phases, were defined using the `KillChainType`, which is found in the `Kill_Chains` property of a `TTP`. These kill chains phases were refered to in the `TTP` and `Indicator Kill_Chain_Phases` properties. In STIX 2.0, kill chains and their phases are not explicitly defined, but are referenced using their common names. If the Lockheed Martin Cyber Kill Chain™ is used the `kill_chain_name` property must be `lockheed-martin-cyber-kill-chain`, according to the specification.

STIX 1.x Properties Mapped Using STIX 2.0 Relationships

none

STIX 1.x Properties Recorded in the STIX 2.0 Description Property

- `Short_Description`
- `Confidence`

  The confidence concept is not present in STIX 2.0. However, the property name confidence has been reserved for future STIX versions.

STIX 1.x Properties Not Mapped

- `idref`

  Relationships in STIX 2.0 make use of id references to indicate the source and target of the relationship. STIX 2.0 objects additionally use `id` references for any property whose suffix is `ref` or‘‘refs‘‘.

The decision available in STIX 1.x to specify related objects by embedding them is not available in STIX 2.0.

- `Related_Packages`

  STIX 1.x packages correspond to STIX 2.0 bundles. However, bundles cannot refer to other bundles, so there is no way to express this property in STIX 2.0.

- `Version`

  Individual STIX objects do not have their own STIX version in STIX 2.0. A bundle has the property `spec_version`, which applies to all objects that are contained in the bundle.

4.2.1 Versioning

STIX 1.x supported the versioning of objects, but it was a feature that was rarely used. STIX 2.0 support of versioning is based on two common properties: `modified` and `revoked`. However, the elevator does not support converting STIX 1.x versioned objects, in the unlikely inclusion of such objects.

All converted objects will be assumed to be the one and only version of an object. If more than one object is found with the same id, it will *not* be flagged as an error.

4.3 Relationships

All STIX 1.x relationships were defined explicitly in the specification and they are all embedded as properties of the object. In STIX 2.0, relationships are top-level objects so they exist independently from their source and target objects. Additionally, although the STIX 2.0 specification suggests certain relationships between object types, a relationship between any two objects is allowed.

Relationships in STIX 1.x could be specified either using the `idref` property, or by embedding the object within the relationship itself. In the former case, the STIX 2.0 object should use the original object's `id` as the `source_ref` property, and the `idref` as the `target_ref` property. In the latter case, the embedded object must first be converted to a top-level STIX 2.0 object. Of course, the embedded object's `id` might not present. In that case, an new id must be created.

An Example

STIX 1.x in XML

```
<stix:Campaign id="example:Campaign-e5268b6e-4931-42f1-b379-87f48eb41b1e"
               timestamp="2014-08-08T15:50:10.983728+00:00"
               xsi:type='campaign:CampaignType' version="1.2">
    <campaign:Attribution>
        <campaign:Attributed_Threat_Actor>
            <stixCommon:Threat_Actor idref="example:threatactor-56f3f0db-b5d5-431c-
↪ae56-c18f02caf500"/>
        </campaign:Attributed_Threat_Actor>
    </campaign:Attribution>
</stix:Campaign>
```

STIX 2.0 in JSON

```
{
        "created": "2014-08-08T15:50:10.983Z",
        "id": "relationship--3dcf59c3-30e3-4aa5-9c05-2cbffcee5922",
        "modified": "2014-08-08T15:50:10.983Z",
```

(continues on next page)

(continued from previous page)

```
        "relationship_type": "attributed-to",
        "source_ref": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
        "target_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500",
        "type": "relationship"
}

{
        "id": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e"

}

{
        "id": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500"

}
```

4.4 Attack Pattern

STIX 1.x Properties Mapped Directly to STIX 2.0 Properties

none

STIX 1.x Properties Translated to STIX 2.0 Properties

STIX 1.x property	STIX 2.0 property
`capec_id`	`external_references`
`ttp:Kill_Chain_Phases`	`kill_chain_phases`

STIX 1.x Properties Mapped Using STIX 2.0 Relationships

STIX 1.x property	STIX 2.0 relationship type
`ttp:Victim_Targeting`	`targets`
`ttp:Exploit_Targets`	`targets` (vulnerability, only)
`ttp:Related_TTPs`	`uses` (malware, tool), `related-to` (when not used for versioning)

STIX 1.x Properties Recorded in the STIX 2.0 Description Property

- `ttp:Intended_Effect`

STIX 1.x Properties Not Mapped

- `ttp:Kill_Chains`

An Example

STIX 1.x in XML

```
<stix:TTP id="example:ttp-8ac90ff3-ecf8-4835-95b8-6aea6a623df5" xsi:type='ttp:TTPType
↪'>
   <ttp:Title>Phishing</ttp:Title>
   <ttp:Behavior>
       <ttp:Attack_Patterns>
           <ttp:Attack_Pattern capec_id="CAPEC-98">
               <ttp:Description>Phishing</ttp:Description>
```

(continues on next page)

(continued from previous page)

```
            </ttp:Attack_Pattern>
        </ttp:Attack_Patterns>
    </ttp:Behavior>
    <ttp:Information_Source>
        <stixCommon:Identity idref="example:identity-f690c992-8e7d-4b9a-9303-
↪3312616c0220"/>
    </ttp:Information_Source>
</stix:TTP>
```

STIX 2.0 in JSON

```
{
    "created": "2017-01-27T13:49:54.326Z",
    "created_by_ref": "identity--f690c992-8e7d-4b9a-9303-3312616c0220"
    "description": "Phishing",
    "external_references": [
        {
            "external_id": "CAPEC-98",
            "source_name": "capec"
        }
    ],
    "id": "attack-pattern--8ac90ff3-ecf8-4835-95b8-6aea6a623df5",
    "modified": "2017-01-27T13:49:54.326Z",
    "name": "Phishing",
    "type": "attack-pattern"
}
```

4.5 Campaigns

STIX 1.x Properties Mapped Directly to STIX 2.0 Properties

STIX 1.x property	STIX 2.0 property
Names	aliases

STIX 1.x Properties Translated to STIX 2.0 Properties

STIX 1.x property	STIX 2.0 property
Intended_Effect	objective

STIX 1.x Properties Mapped Using STIX 2.0 Relationships

STIX 1.x property	STIX 2.0 relationship type
Related_TTPs	uses
Related_Campaign	indicates (reverse)
Attribution	attributed-to
Associated_Campaigns	related-to (when not used for versioning)

STIX 1.x Properties Recorded in the STIX 2.0 Description Property

- Status

STIX 1.x Properties Not Mapped

- Activity
- Related_Incidents

An Example

STIX 1.x in XML

```
<stix:Campaign id="example:Campaign-e5268b6e-4931-42f1-b379-87f48eb41b1e"
               timestamp="2014-08-08T15:50:10.983"
               xsi:type='campaign:CampaignType' version="1.2">
    <campaign:Title>Operation Bran Flakes</campaign:Title>
    <campaign:Description>A concerted effort to insert false information into the BPP
↪'s web pages</campaign:Description>
    <campaign:Names>
        <campaign:Name>OBF</campaign:Name>
    </campaign:Names>
    <campaign:Intended_Effect>Hack www.bpp.bn</campaign:Intended_Effect>
    <campaign:Related_TTPs>
        <campaign:Related_TTP>
            <stixCommon:TTP id="example:ttp-2d1c6ab3-5e4e-48ac-a32b-f0c01c2836a8"
                            timestamp="2014-08-08T15:50:10.983464+00:00"
                            xsi:type='ttp:TTPType' version="1.2">
                <ttp:Victim_Targeting>
                    <ttp:identity id="example:identity-ddfe7140-2ba4-48e4-b19a-
↪df069432103b">
                        <stixCommon:name>Branistan Peoples Party</stixCommon:name>
                    </ttp:identity>
                </ttp:Victim_Targeting>
            </stixCommon:TTP>
        </campaign:Related_TTP>
    </campaign:Related_TTPs>
    <campaign:Attribution>
        <campaign:Attributed_Threat_Actor>
            <stixCommon:Threat_Actor idref="example:threatactor-56f3f0db-b5d5-431c-
↪ae56-c18f02caf500"/>
        </campaign:Attributed_Threat_Actor>
    </campaign:Attribution>
    <campaign:Information_Source>
        <stixCommon:Identity id="example:identity-f690c992-8e7d-4b9a-9303-3312616c0220
↪">
        <stixCommon:name>The MITRE Corporation - DHS Support Team</stixCommon:name>
        <stixCommon:Role xsi:type="stixVocabs:InformationSourceRoleVocab-1.0">Initial␣
↪Author</stixCommon:Role>
    </campaign:Information_Source>
</stix:Campaign>
```

STIX 2.0 in JSON

```
{
    "type": "identity",
    "id": "identity--f690c992-8e7d-4b9a-9303-3312616c0220",
    "created": "2016-08-08T15:50:10.983Z",
    "modified": "2016-08-08T15:50:10.983Z",
    "name": "The MITRE Corporation - DHS Support Team",
    "identity_class": "organization"
}

{
```

(continues on next page)

(continued from previous page)


```
    "type": "identity",
    "id": "identity--ddfe7140-2ba4-48e4-b19a-df069432103b",
    "created_by_ref": "identity--f690c992-8e7d-4b9a-9303-3312616c0220",
    "created": "2016-08-08T15:50:10.983Z",
    "modified": "2016-08-08T15:50:10.983Z",
    "name": "Branistan Peoples Party",
    "identity_class": "organization"
}

{
    "type": "campaign",
    "id": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
    "created_by_ref": "identity--f690c992-8e7d-4b9a-9303-3312616c0220",
    "created": "2016-08-08T15:50:10.983Z",
    "modified": "2016-08-08T15:50:10.983Z",
    "name": "Operation Bran Flakes",
    "description": "A concerted effort to insert false information into the BPP's web␣
↪pages",
    "aliases": ["OBF"],
    "first_seen": "2016-01-08T12:50:40.123Z",
    "objective": "Hack www.bpp.bn"
}
```


See *Threat Actor* for the Threat Actor object.

4.6 Course of Action

In STIX 2.0 the `course-of-action` object is defined as a stub. This means that in STIX 2.0 this object type is pretty "bare-bones", not containing most of the properties that were found in STIX 1.x. The property `action` is reserved, but not defined in STIX 2.0.

STIX 1.x Properties Mapped Directly to STIX 2.0 Properties

none

STIX 1.x Properties Translated to STIX 2.0 Properties

none

STIX 1.x Properties Mapped Using STIX 2.0 Relationships

STIX 1.x property	STIX 2.0 relationship type
`Related_COAs`	`related-to` (when not used for versioning)

STIX 1.x Properties Recorded in the STIX 2.0 Description Property

- `Stage`
- `Objective`
- `Impact`
- `Cost`
- `Efficacy`

STIX 1.x Properties Not Mapped

- Parameter_Observables
- Structured_COA
- Action

An Example

STIX 1.x in XML

```
<stix:Course_Of_Action id="example:coa-495c9b28-b5d8-11e3-b7bb-000c29789db9" xsi:type=
↪'coa:CourseOfActionType' version="1.2">
    <coa:Title>Block traffic to PIVY C2 Server (10.10.10.10)</coa:Title>
    <coa:Stage xsi:type="stixVocabs:COAStageVocab-1.0">Response</coa:Stage>
    <coa:Type xsi:type="stixVocabs:CourseOfActionTypeVocab-1.0">Perimeter Blocking</
↪coa:Type>
    <coa:Objective>
        <coa:Description>Block communication between the PIVY agents and the C2 Server
↪</coa:Description>
        <coa:Applicability_Confidence>
            <stixCommon:Value xsi:type="stixVocabs:HighMediumLowVocab-1.0">High</
↪stixCommon:Value>
        </coa:Applicability_Confidence>
    </coa:Objective>
    <coa:Parameter_Observables cybox_major_version="2" cybox_minor_version="1" cybox_
↪update_version="0">
        <cybox:Observable id="example:Observable-356e3258-0979-48f6-9bcf-6823eecf9a7d
↪">
            <cybox:Object id="example:Address-df3c710c-f05c-4edb-a753-de4862048950">
                <cybox:Properties xsi:type="AddressObj:AddressObjectType" category=
↪"ipv4-addr">
                    <AddressObj:Address_Value>10.10.10.10</AddressObj:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
    </coa:Parameter_Observables>
    <coa:Impact>
        <stixCommon:Value xsi:type="stixVocabs:HighMediumLowVocab-1.0">Low</
↪stixCommon:Value>
        <stixCommon:Description>This IP address is not used for legitimate hosting so␣
↪there should be no operational impact.</stixCommon:Description>
    </coa:Impact>
    <coa:Cost>
        <stixCommon:Value xsi:type="stixVocabs:HighMediumLowVocab-1.0">Low</
↪stixCommon:Value>
    </coa:Cost>
    <coa:Efficacy>
        <stixCommon:Value xsi:type="stixVocabs:HighMediumLowVocab-1.0">High</
↪stixCommon:Value>
    </coa:Efficacy>
</stix:Course_Of_Action>
```

STIX 2.0 in JSON

```
{
    "id": "bundle--495c4c04-b5d8-11e3-b7bb-000c29789db9",
    "objects": [
        {
            "created": "2017-01-27T13:49:41.298Z",
```

(continues on next page)

(continued from previous page)

```
            "description": "\n\nSTAGE:\n\tResponse\n\n
                                OBJECTIVE: Block communication between the PIVY␣
↪agents and the C2 Server\n\n
                                CONFIDENCE: High\n\n
                                IMPACT:Low, This IP address is not used for␣
↪legitimate hosting so there should be no operational impact.\n\n
                                COST:Low\n\n
                                EFFICACY:High",
            "id": "course-of-action--495c9b28-b5d8-11e3-b7bb-000c29789db9",
            "labels": [
                "perimeter-blocking"
            ],
            "modified": "2017-01-27T13:49:41.298Z",
            "name": "Block traffic to PIVY C2 Server (10.10.10.10)",
            "type": "course-of-action"
        }
    ],
    "spec_version": "2.0",
    "type": "bundle"
}
```

4.7 Indicator

STIX 1.x Composite Indicator Expressions and CybOX 2.x Composite Observable Expressions allow a level of flexibility not present in STIX 2.0 patterns. These composite expressions can frequently have ambiguous interpretations, so STIX 2.0 Indicators created by the stix2-elevator from STIX 1.x Indicators containing composite expressions should be inspected to ensure the STIX 2.0 Indicator has the intended meaning.

STIX 1.x Properties Mapped Directly to STIX 2.0 Properties

STIX 1.x property	STIX 2.0 property
Valid_Time_Position	valid_from, valid_until

STIX 1.x Properties Translated to STIX 2.0 Properties

STIX 1.x property	STIX 2.0 property
Alternative_ID	external_references
Kill_Chain_Phases	kill_chain_phases
IndicatorExpression	pattern
Producer	created_by_ref

STIX 1.x Properties Mapped Using STIX 2.0 Relationships

STIX 1.x property	STIX 2.0 relationship type
Indicated_TTP	detects
Suggested_COAs	related-to
Related_Indicators	related-to (when not used for versioning)
Related_Campaigns	indicates

STIX 1.x Properties Recorded in the STIX 2.0 Description Property

none

STIX 1.x Properties Not Mapped

- negate
- Test_Mechanisms
- Likely_Impact

An Example

STIX 1.x in XML

```
<stix:Indicator id="example:Indicator-d81f86b9-975b-bc0b-775e-810c5ad45a4f"
                xsi:type='indicator:IndicatorType'>
    <indicator:Title>Malicious site hosting downloader</indicator:Title>
    <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">URL Watchlist</
↪indicator:Type>
    <indicator:Observable id="example:Observable-ee59c28e-d922-480e-9b7b-a79502696505
↪">
        <cybox:Object id="example:URI-b13ae3fc-80af-49c2-9de9-f713abc070ba">
            <cybox:Properties xsi:type="URIObj:URIObjectType" type="URL">
                <URIObj:Value condition="Equals">http://x4z9arb.cn/4712</URIObj:Value>
            </cybox:Properties>
        </cybox:Object>
    </indicator:Observable>
</stix:Indicator>
```

STIX 2.0 in JSON

```
{
   "created": "2017-01-27T13:49:53.935Z",
   "id": "indicator--d81f86b9-975b-bc0b-775e-810c5ad45a4f",
   "labels": [
       "url-watchlist"
   ],
   "modified": "2017-01-27T13:49:53.935Z",
   "name": "Malicious site hosting downloader",
   "pattern": "[url:value = 'http://x4z9arb.cn/4712']",
   "type": "indicator",
   "valid_from": "2017-01-27T13:49:53.935382Z"
}
```

Sightings

In STIX 1.x sightings were a property of IndicatorType. In STIX 2.0, sightings are a top-level STIX *relationship* object. Because they represent the relationship (match) of an indicator pattern to observed data (or other object), they are more naturally represented as a STIX 2.0 relationship.

For example, suppose the above indicator pattern was matched against an actual cyber observable ("observed-data–b67d30ff-02ac-498a-92f9-32f845f448cf"), because a victim (whose identity is represented by "identity–b67d30ff-02ac-498a-92f9-32f845f448ff") observed that URL.

The STIX 2.0 sighting would be:

```
{
    "type": "sighting",
    "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c75",
    "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
    "created": "2016-04-06T20:08:31.000Z",
```

(continues on next page)

(continued from previous page)

```
    "modified": "2016-04-06T20:08:31.000Z",
    "first_seen": "2015-12-21T19:00:00Z",
    "last_seen": "2015-12-21T19:00:00Z",
    "count": 50,
    "sighting_of_ref": "indicator--d81f86b9-975b-bc0b-775e-810c5ad45a4f",
    "observed_data_refs": ["observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf"],
    "where_sighted_refs": ["identity--b67d30ff-02ac-498a-92f9-32f845f448ff"]
}
```

4.8 Malware

The Malware object in STIX 2.0 is a stub. STIX 2.0 does not support the inclusion of MAEC content. The main properties of malware in STIX 2.0 are not much different than the defined ones in 1.x, however, because of the lack of the ability to include the MAEC content fewer details of malware are representable in STIX 2.0.

Malware is not a top-level object in STIX 1.x, but a property of a `TTP`.

The `name` property of the STIX 1.x Malware object is the preferred property to use to populated the `name` property in the STIX 2.0 object, although if missing, the `title` property can be used.

STIX 1.x Properties Mapped Directly to STIX 2.0 Properties

none

STIX 1.x Properties Translated to STIX 2.0 Properties

STIX 1.x property	STIX 2.0 property
`ttp:Kill_Chain_Phases`	`kill_chain_phases`

STIX 1.x Properties Mapped Using STIX 2.0 Relationships

STIX 1.x property	STIX 2.0 relationship type
`ttp:Related_TTPs`	`variant-of` (malware), `related-to` (when not used for versioning), `uses` (tool)
`ttp:Exploit_Targets`	`targets` (vulnerability, only)
`ttp:Victim_Targeting`	`targets`

STIX 1.x Properties Recorded in the STIX 2.0 Description Property

- `ttp:Intended_Effect`

STIX 1.x Properties Not Mapped

- `ttp:Kill_Chains`
- any MAEC content

An Example

STIX 1.x in XML

```
<stix:TTP id="example:ttp-e610a4f1-9676-eab3-bcc6-b2768d58281a"
          xsi:type='ttp:TTPType'
          timestamp="2014-05-08T09:00:00.000000Z">
   <ttp:Title>Poison Ivy</ttp:Title>
```

(continues on next page)

(continued from previous page)

```
   <ttp:Behavior>
       <ttp:Malware>
           <ttp:Malware_Instance id="example:malware-fdd60b30-b67c-11e3-b0b9-
↪f01faf20d111">
               <ttp:Type xsi:type="stixVocabs:MalwareTypeVocab-1.0">Remote Access␣
↪Trojan</ttp:Type>
               <ttp:Name>Poison Ivy</ttp:Name>
           </ttp:Malware_Instance>
       </ttp:Malware>
   </ttp:Behavior>
</stix:TTP>
```

STIX 2.0 in JSON

```
{
   "created": "2017-01-27T13:49:53.997Z",
   "description": "\n\nTITLE:\n\tPoison Ivy",
   "id": "malware--fdd60b30-b67c-11e3-b0b9-f01faf20d111",
   "labels": [
       "remote-access-trojan"
   ],
   "modified": "2017-01-27T13:49:53.997Z",
   "name": "Poison Ivy",
   "type": "malware"
}
```

4.9 Observed Data

The Observed Data object in STIX 2.0 corresponds to the `Observable` object in CybOX 2.x. Each Observed Data objects contain one or more *related* cyber observable objects.

STIX 2.0 adds two properties: `first_observed` and `last_observed`. These properties are related to the `number_observed` property, because it is possible for Observed Data to indicate that either one, or multiple instances of the same cyber observable occurred. If the `number_observed` property is 1, then the `first_observed` and `last_observed` properties contain the same timestamp, otherwise they are the timestamp of the first and last times that cyber observable occurred.

The `sighting_count` property of STIX 1.x may seem to be the same concept as `number_observed` property, but because STIX 2.0 has made explicit the difference between sightings and observed data, this is not the case. See the STIX 2.0 specification for more details. The sightings count is captured on the Sighting SRO.

STIX 1.x Properties Mapped Directly to STIX 2.0 Properties

STIX 1.x property	STIX 2.0 property
`sighting_count`	not to be confused with **number_observed**
`Keywords`	`labels`

STIX 1.x Properties Translated to STIX 2.0 Properties

STIX 1.x property	STIX 2.0 property
`Object`	`objects`

STIX 1.x Properties Mapped Using STIX 2.0 Relationships

none

STIX 1.x Properties Recorded in the STIX 2.0 Description Property

none

STIX 1.x Properties Not Mapped

- `negate`
- `Event`
- `Title`
- `Description`
- `Pattern_Fidelity`
- `Observable_Source`

An Example

STIX 1.x in XML

```
<cybox:Observable id="example:observable-c8c32b6e-2ea8-51c4-6446-7f5218072f27">
   <cybox:Object id="example:object-d7fcce87-0e98-4537-81bf-1e7ca9ad3734">
        <cybox:Properties xsi:type="FileObj:FileObjectType">
            <FileObj:File_Name>iprip32.dll</FileObj:File_Name>
            <FileObj:File_Path>/usr/local</FileObj:File_Path>
        </cybox:Properties>
   </cybox:Object>
</cybox:Observable>
```

STIX 2.0 in JSON

```
{
   "created": "2017-01-27T13:49:41.345Z",
   "first_observed": "2017-01-27T13:49:41.345Z",
   "id": "observed-data--c8c32b6e-2ea8-51c4-6446-7f5218072f27",
   "last_observed": "2017-01-27T13:49:41.345Z",
   "modified": "2017-01-27T13:49:41.345Z",
   "number_observed": 1,
   "objects": {
       "0": {
           "file_name": "iprip32.dll",
           "parent_directory_ref": "1",
           "type": "file"
       },
       "1": {
           "path": "/usr/local",
           "type": "directory"
       }
   },
   "type": "observed-data"
}
```

In STIX 2.0 cyber observables are only used within `observed-data` objects to represent something that has actually been seen. In STIX 1.x if an `Observable` is contained in an `Indicator`, it is instead expressing a pattern to match against observed data.

The pattern expression to match the example cyber observable, when it is located in an indicator object, would be:

```
[(file:file_name = 'iprip32.dll' AND file:parent_directory_ref.path = '/usr/local')]
```

4.10 Report

The Report object in STIX 2.0 does not contain objects, but only object references to STIX objects that are specified elsewhere (the location of the actual objects may not be contained in the same bundle that contains the `report` object).

In STIX 2.0, properties that were associated with the report header in STIX 1.x are located in the `report` object itself. The `labels` property contains vocabulary literals similar to the ones contain in the `Intent` property in STIX 1.x.

The `published` property is required in STIX 2.0, so the timestamp of the STIX 1.0 Report is used.

STIX 1.x Properties Mapped Directly to STIX 2.0 Properties

none

STIX 1.x Properties Translated to STIX 2.0 Properties

STIX 1.x property	STIX 2.0 property
`Observables`	`object_refs`
`Indicators`	`object_refs`
`TTPs`	`object_refs`
`Exploit_Targets`	`object_refs`
`Courses_Of_Action`	`object_refs`
`Campaigns`	`object_refs`
`Threat_Actors`	`object_refs`
`Report:Header.Intent`	`labels`

STIX 1.x Properties Mapped Using STIX 2.0 Relationships

STIX 1.x property	STIX 2.0 relationship type
`Related_Reports`	`related-to` (when not used for versioning)

An Example

STIX 1.x in XML

```
<stix:Report timestamp="2015-05-07T14:22:14.760467+00:00"
             id="example:Report-ab11f431-4b3b-457c-835f-59920625fe65"
             xsi:type='report:ReportType' version="1.0">
        <report:Header>
            <report:Title>Report on Adversary Alpha's Campaign against the Industrial␣
↪Control Sector</report:Title>
            <report:Intent xsi:type="stixVocabs:ReportIntentVocab-1.0">Campaign␣
↪Characterization</report:Intent>
            <report:Description>Adversary Alpha has a campaign against the ICS sector!
↪</report:Description>
        </report:Header>
        <report:Campaigns>
            <report:Campaign idref="example:campaign-1855cb8a-d96c-4859-a450-
↪abb1e7c061f2" xsi:type='campaign:CampaignType'/>
```

(continues on next page)

(continued from previous page)

```
        </report:Campaigns>
    </stix:Report>
```

STIX 2.0 in JSON

```
{
        "created": "2015-05-07T14:22:14.760Z",
        "created_by_ref": "identity--c1b58a86-e037-4069-814d-dd0bc75539e3",
        "description": "Adversary Alpha has a campaign against the ICS sector!
↪\n\nINTENT:\nCampaign Characterization",
        "id": "report--ab11f431-4b3b-457c-835f-59920625fe65",
        "labels": [
            "campaign-characterization"
        ],
        "modified": "2015-05-07T14:22:14.760Z",
        "name": "Report on Adversary Alpha's Campaign against the Industrial Control␣
↪Sector",
        "object_refs": [
            "campaign--1855cb8a-d96c-4859-a450-abb1e7c061f2"
        ],
        "type": "report"
    }
```

4.11 Threat Actor

STIX 1.x Properties Mapped Directly to STIX 2.0 Properties

STIX 1.x property	STIX 2.0 property
Intended_Effects	goals

STIX 1.x Properties Translated to STIX 2.0 Properties

STIX 1.x property	STIX 2.0 property
Motivation	primary_motivation, secondary_motivations, personal_motivations
Sophistication	sophistication

STIX 1.x Properties Mapped Using STIX 2.0 Relationships

STIX 1.x property	STIX 2.0 relationship type
Identity	attributed-to
Observed_TTPs	uses
Associated_Campaigns	attributed-to (reverse)
Associated_Actors	related-to (when not used for versioning)

STIX 1.x Properties Recorded in the STIX 2.0 Description Property

- Intended_Effect
- Planning_And_Operational_Support

STIX 1.x Properties Not Mapped

none

An Example

STIX 1.x in XML

```
<stix:Threat_Actor id="example:threatactor-56f3f0db-b5d5-431c-ae56-c18f02caf500"
                   xsi:type='ta:ThreatActorType'
                   timestamp="2016-08-08T15:50:10.983Z"
                   version="1.2">
     <ta:Title>Fake BPP (Branistan Peoples Party)</ta:Title>
     <ta:Identity id="example:Identity-8c6af861-7b20-41ef-9b59-6344fd872a8f">
        <stixCommon:Name>Franistan Intelligence</stixCommon:Name>
     </ta:Identity>
     <ta:Type>
        <stixCommon:Value xsi:type="stixVocabs:ThreatActorTypeVocab-1.0">State Actor /
↪ Agency</stixCommon:Value>
     </ta:Type>
     <ta:Intended_Effect>Influence the election in Branistan</ta:Intended_Effect>
     <ta:Motivation>
        <stixCommon:Value xsi:type="stixVocabs:MotivationVocab-1.1">Political</
↪stixCommon:Value>
     </ta:Motivation>
     <ta:Motivation>
        <stixCommon:Value xsi:type="stixVocabs:MotivationVocab-1.1">Ideological</
↪stixCommon:Value>
     </ta:Motivation>
     <ta:Motivation>
        <stixCommon:Value>Organizational Gain</stixCommon:Value>
     </ta:Motivation>
     <ta:Sophistication>
        <stixCommon:Value>Strategic</stixCommon:Value>
     </ta:Sophistication>
</stix:Threat_Actor>
```

STIX 2.0 in JSON

```
{
      "type": "threat-actor",
      "id": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500",
      "created_by_ref": "identity--f690c992-8e7d-4b9a-9303-3312616c0220",
      "created": "2016-08-08T15:50:10.983Z",
      "modified": "2016-08-08T15:50:10.983Z",
      "labels": ["nation-state"],
      "goals": ["Influence the election in Branistan"],
      "primary_motivation": "political",
      "secondary_motivations": ["ideology", "organizational-gain"],
      "name": "Fake BPP (Branistan Peoples Party)",
      "sophistication": "strategic"
}

{
      "type": "identity",
      "id": "identity--8c6af861-7b20-41ef-9b59-6344fd872a8f",
      "created_by_ref": "identity--f690c992-8e7d-4b9a-9303-3312616c0220",
      "created": "2016-08-08T15:50:10.983Z",
      "modified": "2016-08-08T15:50:10.983Z",
```

(continues on next page)

(continued from previous page)

```
      "name": "Franistan Intelligence",
      "identity_class": "organization"
}

{
  "type": "relationship",
  "id": "relationship--5b271699-d2ad-468c-903d-304ad7a17d71",
  "created": "2016-08-08T15:50:10.983Z",
  "modified": "2016-08-08T15:50:10.983Z",
  "relationship_type": "attributed-to",
  "source_ref": "threat-actor--56f3f0db-b5d5-431c-ae56-c18f02caf500",
  "target_ref": "identity--8c6af861-7b20-41ef-9b59-6344fd872a8f"
}
```

4.12 Tool

STIX 1.x Properties Mapped Directly to STIX 2.0 Properties

STIX 1.x property	STIX 2.0 property
`Name` (from CybOX)	`name`
`Type` (from CybOX)	`labels`
`Description` (from CybOX)	`description`
`Version` (from CybOX)	`tool_version`

STIX 1.x Properties Translated to STIX 2.0 Properties

STIX 1.x property	STIX 2.0 property
`ttp:Kill_Chain_Phases`	`kill_chain_phases`
`References` (from CybOX)	`external_references`

STIX 1.x Properties Mapped Using STIX 2.0 Relationships

STIX 1.x property | STIX 2.0 relationship type
`ttp:Related_TTPs` | `uses` (attack-pattern) (reverse), `related-to` (when not used for versioning), `targets` (identity)

STIX 1.x Properties Recorded in the STIX 2.0 Description Property

- `ttp:Intended_Effect`

STIX 1.x Properties Not Mapped

- `Compensation_Model` (from CybOX)
- `Errors` (from CybOX)
- `Execution_Environment` (from CybOX)
- `ttp:Exploit_Targets`
- `ttp:Kill_Chains`
- `Metadata` (from CybOX)

- `Service_Pack` (from CybOX)
- `Tool_Configuration` (from CybOX)
- `Tool_Hashes` (from CybOX)
- `Tool_Specific_Data` (from CybOX)
- `Vendor` (from CybOX)
- `ttp:Victim_Targeting`

An Example

STIX 1.x in XML

```
<stix:TTP id=example:tool--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f
          timestamp="2016-04-06T20:03:48.000Z">
  <ttp:Resources>
      <ttp:Tools>
         <ttp:Tool>
             <cyboxCommon:Name>VNCConnect</cyboxCommon:Name>
             <cyboxCommon:Type>remote-access</cyboxCommon:Name>
             <cyboxCommon:Vendor>RealVNC Ltd</cyboxCommon:Vendor>
             <cyboxCommon:Version>6.03</cyboxCommon:Version>
         </ttp:Tool>
     </ttp:Tools>
  </ttp:Resources>
</stix:ttp>
```

STIX 2.0 in JSON

```
{
  "type": "tool",
  "id": "tool--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
  "created": "2016-04-06T20:03:48.000Z",
  "modified": "2016-04-06T20:03:48.000Z",
  "labels": [ "remote-access"],
  "version": "6.03",
  "name": "VNCConnect"
}
```

4.13 Vulnerability

STIX 1.x Properties Mapped Directly to STIX 2.0 Properties

none

STIX 1.x Properties Translated to STIX 2.0 Properties

STIX 1.x property	STIX 2.0 mapping
CVE_ID	external_references
OSVDB_ID	external_references
References	external_references

STIX 1.x Properties Mapped Using STIX 2.0 Relationships

STIX 1.x property	STIX 2.0 relationship type
et:Potential_COAs	mitigates
et:Related_Exploit_Targets	related-to (when not used for versioning)

STIX 1.x Properties Recorded in the STIX 2.0 Description Property

none

STIX 1.x Properties Not Mapped

- is_known
- is_publicly_acknowledged
- CVSS_Score
- Discovered_DateTime
- Published_DateTime
- Affected_Software
- Source

An Example

STIX 1.x in XML

```
<stix:Exploit_Targets>
   <stixCommon:Exploit_Target id="example:et-e77c1e36-5b43-4c5c-b8cb-7b36035f2b90"␣
↪timestamp="2014-06-20T15:16:56.986650+00:00" xsi:type='et:ExploitTargetType'␣
↪version="1.2">
       <et:Title>Heartbleed</et:Title>
       <et:Vulnerability>
           <et:CVE_ID>CVE-2013-3893</et:CVE_ID>
       </et:Vulnerability>
   </stixCommon:Exploit_Target>
</stix:Exploit_Targets>
```

STIX 2.0 in JSON

```
{
   "created": "2014-06-20T15:16:56.986Z",
   "external_references": [
       {
           "external_id": "CVE-2013-3893",
           "source_name": "cve"
       }
   ],
   "id": "vulnerability--e77c1e36-5b43-4c5c-b8cb-7b36035f2b90",
   "modified": "2017-01-27T13:49:54.310Z",
   "name": "Heartbleed",
   "type": "vulnerability"
}
```

CHAPTER 5

Mappings from CybOX 2.x to STIX 2.0

The following table associates the CybOX 2.x object types with their STIX 2.0 cyber observable types. For each CybOX object the table also indicates if the elevator is able to convert the CybOX object to STIX 2.0.

CybOX object types not listed have no corresponding STIX 2.0 cyber observable type, and therefore are not converted by the elevator.

Cybox 2.x Object Type	STIX 2.0 Cyber Observable Type	Converted in version 1.1
Address	email-addr	yes
Address	ipv4-addr	yes
Address	ipv6-addr	yes
Address	mac-addr	yes
ArchiveFile	file:archive-ext	patterns only
Artifact	artifact	no
AutonomusSystem	autonomous-system	no
File	directory	yes
DomainName	domain-name	yes
DNSQuery	none	no
EmailMessage	email-message	yes
File	file	yes
HTTPClientRequest	network-traffic:http-request-ext	no
HTTPSession	network-traffic	no
ICMP``(``v4/v6)	network-traffic:icmp-ext	no
ImageFile	file:raster-image-ext	no
Link	*none*	no
Mutex	mutex	yes
NetworkConnection	network-traffic	yes
PDFFile	file:pdf-ext	no
Process	process	yes
Product	software	no
SocketAddress	network-traffic	yes
Hostname	domain-name	yes

Conti

Table 1 – continued from previous page

Cybox 2.x Object Type	STIX 2.0 Cyber Observable Type	Converted in version 1.1
Port	integer	yes
TCP	network-traffic:tcp-ext	no
URI	url	yes
UnixUserAccount	user-account:unix-account-ext	no
UserAccount/WinUserAccount	user-account	no
WindowsRegistryKey	window-registry-key	yes
WinExecutableFile	file:window-pebinary-ext	patterns only
WinFile	file:ntfs-ext	no
WinProcess	process:windows-process-ext	observables only
WinService	process:windows-service-ext	yes
X509Certificate	x509-certificate	no
X509V3Extensions	x509-certificate:x509-v3-extensions-type	no

5.1 Converting Network Cyber Observables

Most of the mappings between CybOX 2.x objects and STIX 2.0 cyber observables are straightforward, therefore, they will not be detailed in this document. However, it would be advantageous to detail the mappings of network-traffic, a "catch-all" STIX 2.0 cyber observable type for information previously represented in CybOX 2.x by:

- NetworkConnection
- HTTPSessionObject
- NetworkFlowObject
- NetworkPacket

This information is organized very differently than in CybOX 2.x. In addition, many CybOX 2.x properties are not available in the network-traffic object.

Notice that although both STIX 1.x and 2.0 have object types to represent TCP packets, they are not compatible, so no conversion is made.

CybOX 2.x Type	STIX 2.0 mapping
NetworkConnection	network-traffic
HTTPSessionObject/HTTPSessionObject/ HTTPClientRequest	network-traffic/ http-request-ext
NetworkFlowObject/UnidirectionalRecord/ IPFIXMessage	network-traffic/ipfix
NetworkPacket/InternetLayer/ICMPv(4/6)	network-traffic/icmp-ext

CHAPTER 6

Vocabularies

In STIX 2.0, vocabularies are referred to as "open". Although vocabularies in STIX 1.x were referred to as "controlled", the actual difference between them is negligible. In both standards, vocabulary literals were suggested, but not required to be used. Producers using either standards are free to use any string as a value. The most important difference is that in STIX 1.x it was possible to require that only suggested literals were used, and have that enforced through XML schema validation.

Certain STIX 2.0 vocabularies are either copied verbatim from STIX 1.x, or with few changes. Others, are revamped in STIX 2.0, and it might be difficult to find a corresponding literal to one from STIX 1.x. However, because all of these vocabularies are open in STIX 2.0, those values can be used directly.

STIX 1.x Vocabulary	STIX 2.0 Vocabulary
`AssetTypeVocab`	*not available in STIX 2.0*
`AttackerInfrastructureTypeVocab`	*not available in STIX 2.0*
`AttackerToolTypeVocab`	`tool-label-ov`
`AvailabilityLossTypeVocab`	*not available in STIX 2.0*
`COAStageVocab`	*not available in STIX 2.0*
`CampaignStatusVocab`	*not available in STIX 2.0*
`CourseOfActionTypeVocab`	`course-of-action-label-ov`
`DiscoveryMethodVocab`	*not available in STIX 2.0*
`HighMediumLowVocab`	*not used*
`ImpactQualificationVocab`	*not available in STIX 2.0*
`ImpactRatingVocab`	*not available in STIX 2.0*
`IncidentCategoryVocab`	*not available in STIX 2.0*
`IncidentEffectVocab`	*not available in STIX 2.0*
`IncidentStatusVocab`	*not available in STIX 2.0*
`IndicatorTypeVocab`	`indicator-label-ov`
`InformationSourceRoleVocab`	*not available in STIX 2.0*
`InformationTypeVocab`	*not available in STIX 2.0*
`IntendedEffectVocab`	`attack-objective-ov`
`LocationClassVocab`	*not available in STIX 2.0*
`LossDurationVocab`	*not available in STIX 2.0*

Continued on next page

Table 1 – continued from previous page

STIX 1.x Vocabulary	STIX 2.0 Vocabulary
LossPropertyVocab	*not available in STIX 2.0*
MalwareTypeVocab	malware-label-ov
ManagementClassVocab	*not available in STIX 2.0*
MotivationVocab	attack-motivation-ov
OwnershipClassVocab	*not available in STIX 2.0*
PackageIntentVocab	*not used*
PlanningAndOperationalSupportVocab	resource-level-ov
ReportIntentVocab	report-label-ov
SecurityCompromiseVocab	*not used*
SystemTypeVocab	*not available in STIX 2.0*
ThreatActorSophisticationVocab	attack-sophistication-level-ov
ThreatActorTypeVocab	threat-actor-label-ov
VersioningVocab	*not used*

New vocabularies added in STIX 2.0 are:

- attack-resource-level-ov
- encryption-algo-ov
- hash-algorithm-ov
- identity-class-ov
- industry-sector-ov
- marking-definition-ov
- threat-actor-role-ov
- windows-pebinary-type-ov

In addition, the STIX 2.0 specification contains enumerations. These are mostly for cyber observables. These are different from open vocabularies because only values explicitly defined in the enumeration can be used. The enumerations defined in STIX 2.0 are:

- network-socket-type-enum
- windows-service-start-type-enum
- windows-service-status-enum
- windows-service-type-enum

which correspond to similar enumerations defined in STIX 1.x.

CHAPTER 7

Conversion Issues

This section discusses some techniques to facilitate the conversion of STIX 1.x data to STIX 2.0. These techniques cover non-obvious issues that might present an impediment to re-using STIX 1.x data.

7.1 Assumptions

7.1.1 Timestamps, Identifiers and Object Creators

In STIX 1.x most properties were optional. This includes properties that correspond to required properties in STIX 2.0. In particular, all STIX Objects in 2.0 are required to have `id`, `created` and `modified` properties. These are often not specified in a STIX 1.x object, but can sometimes be inferred from another STIX 1.x object in the same package.

Content in STIX 1.x was often hierarchical unlike content in STIX 2.0 which is relatively flat, and this can help to determine required properties. For instance, a timestamp on a STIX 1.x package could be construed as the timestamp for all objects it contains. Likewise, an object could assume that its parent object's timestamp is also the timestamp of that object, unless that object possessed its own timestamp. Of course, if no timestamp is present for any of the objects, included the top level package, some other timestamp outside of the content must be used. In most cases, this would probably result in using the current timestamp when the conversion is made.

Most top-level STIX 1.x objects contained an `id` (or an `idref`), however when converting STIX 1.x TTPs and Exploit Targets the id must be assigned to the STIX 2.0 object that results. For instance, a TTP might have contain an attack pattern object, but the id was not a property of the attack pattern, but the TTP.

In certain circumstances, no id is available or in the case of TTPs and Exploit Targets, there may be more than one STIX 2.0 object created. In these cases, a new `id` must be used.

In STIX 1.x, all top-level objects had a `Information_Source` property to hold information about, among other things, the object creator. However, this property was optional. `created_by_ref`, which is a common property on all STIX 2.0 Objects, is also optional. It should be noted however, that the object creator can also be "inherited" from its parent object, as with the timestamp. This fact can be useful to derive a more robust STIX 2.0 object.

7.1.2 Special Considerations for TTPs and Exploit Target Conversions

When converting a STIX 1.x TTP or Exploit Target certain properties exist at the top-level, and not in the subsidiary object which will form the basis of the STIX 2.0 object. However, those properties must be used when creating the subsidiary object. See section *Attack Pattern* for an example. The conversion of that STIX 1.x TTP will yield a STIX 2.0 Attack Pattern, whose `name` and `created_by_ref` are determined from the TTP itself, and not the STIX 1.x Attack Pattern.

7.1.3 Minor Issues

- The `condition` property was optional in STIX 1.x Observables. If it was not specified for an Observable used for patterning, the condition used in the STIX 2.0 pattern will be assumed to be "=".
- The title property should be used for the `name` property, when necessary.
- STIX 1.2 introduced versioning of objects. Currently, there is no guidance to converting STIX 1.2 versioning to STIX 2.0 versioning. In most cases, a STIX 1.x relationship between object instances of the same type will be converted to a `related-to` relationship in STIX 2.0, which could be undesirable.

7.2 Optional vs. Required

Certain fields are required in STIX 2.0 object that were optional in STIX 1.x. This goes beyond the properties such as ids, created/modified timestamps. The most frequently occurring example is the `labels` property (also a common property). The elevator will use a default value - `unknown`.

7.3 Issues with Patterns

Patterns in STIX 2.0 have certain restrictions that didn't explicitly appear in STIX 1.x. A pattern in STIX 2.0 has explicit rules about if the expression can refer to only one or many observed data instances. Because STIX 1.x patterns did not have any of these restrictions, a reasonable conversion of the pattern by the elevator might be illegal in STIX 2.0.

Additionally, the use of the NOT operator in STIX 2.0 is restricted to be used only with Comparison operators. Therefore, it is not possible to express a pattern such as NOT `(file.name == foo.bar" AND 'file.size == 123)` directly. To yield an equivalent pattern expression in STIX 2.0, DeMorgan's Law would need to be used to reduce the scope of the NOT operator: `(file.name != foo.bar" OR 'file.size != 123)`, but the elevator does not perform this functionality.

7.4 Single vs. Multiple

Some properties in STIX 1.x allowed for multiple values, but the corresponding property in STIX 2.0 does not. In these cases, the first value is used.

In certain situations, something specific to the properties can be helpful in handling this issue. For instance, the first entry in the STIX 1.x Threat Actors `motivation` property should be assumed to be the `primary_motivation`. Any others should be listed in the `secondary_motivations` property.

7.5 Data Markings

The stix-elevator currently supports global markings and object-level markings. Through the use of hashing, the elevator make the best effort to detect duplicate markings to prevent excessive object creation. Also, the marking types supported by the elevator is limited to: Simple, Terms of Use, TLP and AIS.

CHAPTER 8

Warning Messages

When the elevator makes an assumption during the conversion of some content, or is unable to convert the content, a warning message is output.

8.1 General

Message	Code	Level
Results produced by the stix2-elevator are not for production purposes.	201	warn
Observable Expressions should not contain placeholders	202	error
Placeholder *[id]* should be resolved	203	error
Found definition for *[id]*	204	info
At least one PLACEHOLDER idref was not resolved in *[id]*	205	warn
At least one observable could not be converted in *[id]*	206	warn
Options not initialized	207	error
EMPTY BUNDLE – No objects created from 1.x input document!	208	warn
Both console and output log have disabled messages.	209	warn
OSError *[message]*	210	error
silent option is not compatible with a policy	211	warn

8.2 Adding Content not supported in STIX 2.0 to Description

Message	Code	Level
The `Short_Description` property is no longer supported in STIX. The text was appended to the description property of *[id]*	301	warn
Appended *[property_name]* to description of *[id]*	302	warn
Title *[title]* used for `name`, appending `exploit_target` *[id]* title in description property	303	info
Appended `confidence` property content to description of *[id]*	304	warn
Appended `Statement` type content to description of *[id]*	305	warn
Appended ‘‘Tool ‘‘type content to description of *[id]*	306	warn

8.3 Dropping Content not supported in STIX 2.0

Message	Code	Level
`Information Source` on *[id]* is not representable in STIX 2.0	401	warn
`Related_Packages` type in *[id]* not supported in STIX 2.0	402	warn
`Campaign/Activity` type in *[id]* not supported in STIX 2.0	403	warn
Structured COAs type in *[id]* are not supported in STIX 2.0	404	warn
`ExploitTarget/Weaknesses` type in *[id]* not supported in STIX 2.0	405	warn
`ExploitTarget/Configurations` type in *[id]* not supported in STIX 2.0	406	warn
Indicator *[id]* has an observable or indicator composite expression which may not supported correctly in STIX 2.0 - please check this pattern	407	warn
`TTP/Behavior/Exploits/Exploit` in *[id]* not supported in STIX 2.0	408	warn
`Infrastructure` in *[id]* not part of STIX 2.0	409	warn
Targeted systems on *[id]* are not a victim target in STIX 2.0	410	warn
Targeted information on *[id]* is not a victim target in STIX 2.0	411	warn
Targeted technical details on *[id]* are not a victim target in STIX 2.0	412	warn
Kill Chains type in *[id]* not supported in STIX 2.0	413	warn
Victim Target in *[id]* did not yield any STIX 2.0 object	414	warn
TTP *[id]* did not generate any STIX 2.0 object	415	warn
No STIX 2.0 object generated from embedded object *[id]*	416	warn
[object type] did not yield any STIX 2.0 object	417	warn
The exports property of `WinExecutableFileObj` is not part of STIX 2.0	418	warn
The imports property of `WinExecutableFileObj` is not part of STIX 2.0	419	warn
Windows Handles are not a part of STIX 2.0	420	warn
The address type [address] is not part of STIX 2.0	421	warn
No pattern term was created from *[id]*	422	warn
[id] is used as a pattern, therefore it is not included as an observed_data instance	423	warn
[xxx] content is not supported in STIX 2.0	424	warn
Could not resolve Marking Structure *[id]*	425	warn
MAEC content in *[id]* cannot be represented in STIX 2.0	426	warn
The *[relationship name]* relationship involving *[id]* is not supported in STIX 2.0	427	warn
`roles` is not a property of a 2.0 identity (*[id]*). Perhaps the roles are associated with a related Threat Actor	428	warn

8.4 Multiple values are not supported in STIX 2.0

Message	Code	Level
`NO MESSAGE ASSIGNED`	501	
Only one person name allowed for *[id]* in STIX 2.0, used first one	502	warn
Only one organization name allowed for *[id]* in STIX 2.0, used first one	503	warn
YARA/SNORT patterns on *[id]* not supported in STIX 2.0	504	warn
`NO MESSAGE ASSIGNED`	505	
Only one alternative test mechanism allowed for *[id]* in STIX 2.0 - used first one, which was *[pattern_lang]*	506	warn
Only one valid time window allowed for *[id]* in STIX 2.0 - used first one	507	warn
Only one name for malware is allowed for *[id]* in STIX 2.0 - used first one	508	warn
No STIX 1.x vocab value given for *[property]*, using 'unknown'	509	warn
Only one *[property]* allowed in STIX 2.0 - used first one	510	warn
File size 'window' not allowed in top level observable, using first value	511	warn
Only one `Layer7_Connections/HTTP_Request_Response` used for `http-request-ext`, using first value	512	warn

8.5 Possible issue in original STIX 1.x content

Message	Code	Level
Dangling source reference *[source]* in *[id]*	601	warn
Dangling target reference *[target]* in *[id]*	602	warn
1.X ID: *[id]* was not mapped to STIX 2.0 ID	603	warn
Unable to determine the STIX 2.0 type for *[id]*	604	error
Malformed id *[id]*. Generated a new uuid	605	warn
Identity *[id]* has organization and person names	606	error
Dangling kill chain phase id in indicator *[id]*	607	error
`windows-registry-key` is required to have a `key` property	608	error
[condition] was used, but two values were not provided.	609	error
Trying to associate *[old_key]* with None	610	warn
Could not associate *[old_id]* with None	611	error
Identity *[id]* must have a name, using 'None'	612	error
No `WinExecutableFile` properties found in *[WinExeFile]*	613	warn
No `ArchiveFile` properties found in *[ArchiveFile]*	614	warn
No `WinProcess` properties found in *[WinProcess]*	615	warn
No `WinService` properties found in *[WinService]*	616	warn
The custom property name *[property name]* does not adhere to the specification rules	617	warn
No ISO code for *[value]* in *[identifying info]*	618	warn
No start time for the first valid time interval is available in *[id]*, other time intervals might be more appropriate	619	warn
Unable to create a pattern from a File object	620	warn
[stix 1.x property] contains no value	621	warn
No term was yielded for *[id]*	622	warn
Hive property, *[hive property name]*, is already a prefix of the key property, *[key property name]*	623	warn
The custom property name *[id]* contains whitespace, replacing it with underscores	624	warn
Found duplicate marking structure *[id]*	625	info
[hash_string] is not a valid *[hash_type]* hash	626	warn

8.6 STIX Elevator conversion based on assumptions

Message	Code	Level
Threat Actor identity *[id]* being used as basis of attributed-to relationship	701	info
Found STIX 1.X ID: *[old_id]* replaced by *[new_id]*	702	info
[old_id] is already associated other ids: *[tuple_of_new_ids]*	703	info
Including *id of relationship* in *id of report* and added the target_ref *target_ref* to the report	704	warn
Including *id of relationship* in *id of report* and added the source_ref *source_ref* to the report	705	warn
Including *id of relationship* in *id of report* although the target_ref is unknown	706	warn
Including *id of relationship* in *id of report* although the source_ref is unknown	707	warn
Not including *id of relationship* in *id of report* because there is no corresponding SDO for *target_ref*	708	warn
Not including *id of relationship* in *id of report* because there is no corresponding SDO for *source_ref*	709	warn
All associated *[xxx]* relationships of *[id]* are assumed to not represent STIX 1.2 versioning	710	warn
ciq name found in *[id]*, possibly overriding other name	711	warn
Only one type pattern can be specified in *[id]* - using cybox	712	warn
[id] generated an identity associated with a victim	713	warn
No condition given for *[current_observable]* - assume '='	714	warn
Used MATCHES operator for *[condition]*	715	warn
Based on CIQ information, *[id]* is assumed to be an organization	716	warn
Threat actor *[id]* title is used for name property	717	info
Using related-to for the *[property]* of *[id]*	718	warn
Using first Threat Actor motivation as `primary_motivation` value. If more, use `secondary_motivation`	719	info
The `published property` is required for STIX 2.0 Report *[id]*, using the created property	720	info

8.7 STIX elevator currently doesn't process this content

Message	Code	Level
Could not resolve Marking Structure *[id]*	801	warn
1.x full file paths are not processed, yet	802	warn
`process:startup_info` not handled yet	803	warn
`WinServiceObject.service_dll` is not handled, yet.	804	warn
CybOX object *[object]* not handled yet	805	warn
Email *[property]* not handled yet	806	warn
`file:extended_properties:windows_pebinary_ext:optional_header` is not implemented yet	807	warn
[object] found in *[id]* cannot be converted to a pattern, yet.	808	warn
Related Objects of cyber observables for *[id]* are not handled yet	809	warn
Negation of *[id]* is not handled yet	810	warn
`NO MESSAGE ASSIGNED`	811	
Condition on a hive property not handled.	812	warn
Cannot convert CybOX 2.x class name *[name]* to an object_path_root_name	813	error
Parameter Observables in *[id]* are not handled, yet.	814	warn
[property] in *[id]* are not handled, yet.	815	info
Ambiguous file path *[path]* was not processed	816	warn

8.8 Missing Required Timestamp

CHAPTER 9

Indices and tables

- genindex
- modindex
- search