stix2-slider Documentation

Release 1.0.0

OASIS Open

Apr 07, 2024

CONTENTS:

To convert STIX 1.x XML to STIX 2.x JSON use the stix2-elevator.

CHAPTER

ONE

INTRODUCTION

The stix-slider is a software tool for 'sliding' STIX 2.x JSON to STIX 1.x XML. Due to the differences between STIX 1.x and STIX 2.x, this conversion is a best-effort only. During the conversion, stix-slider produces many warning messages about the assumptions it needs to make to produce valid STIX 1.x XML, and what information was not able to be converted.

It important to emphasize that the slider is not for use in a *production* system without human inspection of the results it produces. It should be used to explore how STIX 2.x content could potentially be represented in STIX 1.x. Using the current version of the slider will provide insight to issues that might need to be mitigated to convert your STIX 2.x content for use in application that accept only STIX 1.x content.

CHAPTER

TWO

INSTALLING

2.1 Requirements

- Python 3.5+
- 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 >= 2.0.0
- stixmarx >= 1.0.7
- stix-validator >= 2.5.0

2.2 Installation Steps

Install with pip:

```
$ pip install stix2-slider
```

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-slider
```

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

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

CHAPTER

THREE

COMMAND LINE INTERFACE

The slider comes with a bundled script which you can use to convert STIX 2.x content to STIX 1.x content:

```
usage: stix2_slider [-h] [--no-squirrel-gaps] [--validator-args VALIDATOR_ARGS]
                    [-e ENABLE] [-d DISABLE] [-s]
                    [--message-log-directory MESSAGE_LOG_DIRECTORY]
                    [--log-level {DEBUG,INFO,WARN,ERROR,CRITICAL}]
                    [--use-namespace USE_NAMESPACE]
                    file

stix2-slider v3.0.0
```

The stix2-slider is a work-in-progress. It should be used to explore how existing STIX 2.x would potentially be represented in STIX 1.x. Using the current version of the stix2-slider will provide insight to issues that might need to be mitigated so you can use an application that supports only STIX 1.x content.

positional arguments:

```
file    The input STIX 2.x document to be 'slid' to STIX 1.x.
```

optional arguments:

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

--no-squirrel-gaps
      Do not include STIX 2.x content that cannot be
      represented directly in STIX 1.x using the description
      property.

--validator-args VALIDATOR_ARGS
      Arguments to pass to stix-validator. Example:
      stix2_slider <file> --validator-args="--best-
      practices"

-e ENABLE, --enable ENABLE
      A comma-separated list of the stix2-slider messages to
      enable. If the --disable option is not used, no other
      messages will be shown. Example: stix2_slider <file>
      --enable 250

-d DISABLE, --disable DISABLE
```

(continues on next page)

(continued from previous page)

```
      A comma-separated list of the stix2-slider messages to
      disable. Example: stix2_slider <file> --disable
      212,220

-s, --silent
      If this flag is set. All stix2-slider messages will be
      disabled.

--message-log-directory MESSAGE_LOG_DIRECTORY
      If this flag is set, all stix2-slider messages will be
      saved to 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:
      stix2_slider <file> --message-log-directory "../logs"

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

--use-namespace USE_NAMESPACE
      Override the 'example' namespace with the provided one.
      The format is the prefix, namespace uri and optionally
      the schema location separated by a space. Example:
      stix2_slider <file> --use-namespace="example http://example.com"
```

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

Note: disabling the message does not disable any functionality.

It is recommended that you ensure that the input STIX 2.x file is valid before submitting it to the slider. Use the stix2-validator.

CHAPTER

FOUR

MAPPINGS FROM STIX 2.X TO STIX 1.X

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

For each STIX 2.x object that was converted the following options are possible:

- **STIX 2.x property mapped directly to a STIX 1.x property.** This property's value is used unaltered in the conversion to 2.x.
- **STIX 2.x property translated into STIX 1.x property.** This property's value must undergo some minor processing to determine the corresponding content for 1.x.
- **STIX 2.x relationship mapped using STIX 1.x property.** This 2.x relationship object is used to construct an embedded STIX 1.x relationship. If the STIX 2.x `relationship-type` is not listed below, then that relationship will not be converted to an embedded STIX 1.x relationship. The "reverse" notation indicates the the STIX 1.x property is found on target object.
- **STIX 2.x property recorded in the STIX 1.x description property.** This 2.x property has no corresponding property in STIX 1.x, but its value can be (optionally) included in the description property of the 1.x object as text.

  If the STIX 2.x content was created using the elevator it might be the case that it recorded some 1.x properties in the description. However, the slider makes no attempt to examine the content of the 2.x descriptor property to determine if it can use information found within it to populate the original 1.x properties.
- **STIX 2.x property not mapped.** This property will not be included in the converted 1.x object.

Many of the examples below convert STIX 2.0 to STIX 1.x. Conversions of STIX 2.1 are similar.

4.1 Top Level Object Mappings

STIX 2.x object	STIX 1.x object
attack-pattern	ttp:Attack_Pattern
bundle	Package
campaign	Campaign
course-of-action	Course_Of_Action
grouping	*not converted*
identity	Information_Source or ttp:Victim_Targeting
indicator	Indicator
infrastructure	ttp:Infrastructure
intrusion-set	*not converted*
location	xpil:Address
malware	ttp:MalwareInstance
malware-analysis	*not converted*
note	*not converted*
observed-data	Observable
opinion	*not converted*
report	Report
threat-actor	Threat Actor
tool	ttp:Tool
vulnerability	et:Vulnerability

4.2 Common Properties

STIX 2.x Properties Mapped Directly to STIX 1.x Properties

STIX 2.x property	STIX 1.x property
created	*not converted* (see modified)
description	Description
modified	timestamp
name	Title

STIX 2.x Properties Translated to STIX 1.x Properties

STIX 2.x property	STIX 1.x property
type	*implicitly defined by its element name or explicitly using xsi:type*
id	id
created_by_ref	Information_Source
external_reference	Information_Source, et:Vulnerability.cve_id, ttp:Attack_Patterns.capec.id Description
object_markings_re	Handling
granular_markings	Handling

STIX 2.x Relationships Mapped Using STIX 1.x Relationships

none

STIX 2.x Properties Recorded in the STIX 1.x Description Property

none

STIX 2.x Properties Not Mapped

- `revoked`

4.3 Attack Pattern

STIX 2.x Properties Mapped Directly to STIX 1.x Properties

none

STIX 2.x Properties Translated to STIX 1.x Properties

STIX 2.x property	STIX 1.x property
`external_references`	`capec_id`
`kill_chain_phases`	`ttp:Kill_Chain_Phases`

STIX 2.x Relationships Mapped Using STIX 1.x Relationships

STIX 2.x relationship type	STIX 1.x property
`targets` (identity only)	`ttp:Victim_Targeting`
`targets` (vulnerability only)	`ttp:Exploit_Targets`
`uses` (malware, tool)	`ttp:Related_TTPs`

STIX 2.x Properties Recorded in the STIX 1.x Description Property

- `labels` (in 2.1)

STIX 2.x Properties Not Mapped

none

An Example

STIX 2.x in JSON

```
{
  "type": "attack-pattern",
  "id": "attack-pattern--19da6e1c-71ab-4c2f-886d-d620d09d3b5a",
  "created": "2016-08-08T15:50:10.983Z",
  "modified": "2017-01-30T21:15:04.127Z",
  "external_references": [
    {
      "external_id": "CAPEC-148",
      "source_name": "capec",
      "url": "https://capec.mitre.org/data/definitions/148.html"
    }
  ],
  "name": "Content Spoofing"
}
```

STIX 1.x in XML

```
<stix:TTP id="example:ttp-19da6e1c-71ab-4c2f-886d-d620d09d3b5a" timestamp="2017-01-
↪30T21:15:04.127000+00:00" xsi:type='ttp:TTPType'>
    <ttp:Behavior>
        <ttp:Attack_Patterns>
            <ttp:Attack_Pattern capec_id="CAPEC-148">
                <ttp:Title>Content Spoofing</ttp:Title>
            </ttp:Attack_Pattern>
        </ttp:Attack_Patterns>
    </ttp:Behavior>
    <ttp:Information_Source>
        <stixCommon:References>
            <stixCommon:Reference>https://capec.mitre.org/data/definitions/148.html</
↪stixCommon:Reference>
        </stixCommon:References>
    </ttp:Information_Source>
</stix:TTP>
```

4.4 Campaigns

STIX 2.x Properties Mapped Directly to STIX 1.x Properties

STIX 2.x property	STIX 1.x property
aliases	Names
objective	Intended_Effect

STIX 2.x Properties Translated to STIX 1.x Properties

none

STIX 2.x Relationships Mapped Using STIX 1.x Relationships

STIX 2.x relationship type	STIX 1.x property
uses	Related_TTPs
indicates (reverse)	Related_Indicators
attributed-to	Attribution
related-to (campaign)	Associated_Campaigns

STIX 2.x Properties Recorded in the STIX 1.x Description Property

- first_seen
- last_seen
- labels (in 2.1)

STIX 2.x Properties Not Mapped

none

An Example

STIX 2.x in JSON

```
{
        "created": "2014-08-08T15:50:10.983Z",
        "description": "Attacking ATM machines in the Eastern US",
        "external_references": [
            {
                "source_name": "ACME",
                "url": "http://foo.com/bar"
            },
            {
                "source_name": "wikipedia",
                "url": "https://en.wikipedia.org/wiki/Automated_teller_machine"
            },
            {
                "source_name": "ACME Bugzilla",
                "external_id": "1370",
                "url": "https://www.example.com/bugs/1370"
            }
        ],
        "id": "campaign--e5268b6e-4931-42f1-b379-87f48eb41b1e",
        "modified": "2014-08-08T15:50:10.983Z",
        "name": "Compromise of ATM Machines",
        "type": "campaign"
}
```


STIX 1.x in XML


```
<stix:Campaign id="example:campaign-e5268b6e-4931-42f1-b379-87f48eb41b1e" timestamp=
↪"2014-08-08T15:50:10.983000+00:00" xsi:type='campaign:CampaignType'>
        <campaign:Title>Compromise of ATM Machines</campaign:Title>
        <campaign:Description ordinality="1">Attacking ATM machines in the Eastern US</
↪campaign:Description>
        <campaign:Description ordinality="2">SOURCE: ACME Bugzilla - EXTERNAL ID: 1370</
↪campaign:Description>
        <campaign:Information_Source>
            <stixCommon:References>
                <stixCommon:Reference>http://foo.com/bar</stixCommon:Reference>
                <stixCommon:Reference>https://en.wikipedia.org/wiki/Automated_teller_
↪machine</stixCommon:Reference>
                <stixCommon:Reference>https://www.example.com/bugs/1370</
↪stixCommon:Reference>
            </stixCommon:References>
        </campaign:Information_Source>
    </stix:Campaign>
```

4.5 Course of Action

In STIX 2.x the course-of-action object is defined as a stub. This means that in STIX 2.x this object type is pretty "bare-bones", not containing most of the properties that were found in STIX 1.x.

STIX 2.x Properties Mapped Directly to STIX 1.x Properties

none

STIX 2.x Properties Translated to STIX 1.x Properties

STIX 2.x property	STIX 1.x property
`labels` (in 2.0)	`Type`

STIX 2.x Relationships Mapped Using STIX 1.x Relationships

STIX 2.x relationship type	STIX 1.x property
`related-to` (course-of-action)	`Related_COAs`

STIX 2.x Properties Recorded in the STIX 1.x Description Property

- `labels` (in 2.1)

STIX Properties Not Mapped

none

An Example

STIX 2.x in JSON

```
{
        "created": "2017-01-27T13:49:41.298Z",
        "description": "\n\nSTAGE:\n\tResponse\n\nOBJECTIVE: Block communication between␣
↪the PIVY agents and the C2 Server\n\nCONFIDENCE: High\n\nIMPACT:LowThis IP address is␣
↪not used for legitimate hosting so there should be no operational impact.\n\nCOST:Low\
↪n\nEFFICACY: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"
}
```

STIX 1.x in XML

```
<stix:Course_Of_Action id="example:course-of-action-495c9b28-b5d8-11e3-b7bb-000c29789db9
↪" timestamp="2017-01-27T13:49:41.298000+00:00" xsi:type='coa:CourseOfActionType'>
            <coa:Title>Block traffic to PIVY C2 Server (10.10.10.10)</coa:Title>
            <coa:Type xsi:type="stixVocabs:CourseOfActionTypeVocab-1.0">Perimeter␣
↪Blocking</coa:Type>
            <coa:Description>
```

(continues on next page)

(continued from previous page)

```
                STAGE:
                    Response
                OBJECTIVE: Block communication between the PIVY agents and the C2 Server
                CONFIDENCE: High
                IMPACT:LowThis IP address is not used for legitimate hosting so there␣
↪should be no operational impact.
                COST:Low
                EFFICACY:High
            </coa:Description>
</stix:Course_Of_Action>
```

Notice that although there is information in the STIX 2.x description property (from a previous use of the elevator) that could be used to populate STIX 1.x properties, the description property is transferred directly, with no additional processing.

4.6 Indicator

STIX 2.x Properties Mapped Directly to STIX 1.x Properties

STIX 2.x property	STIX 1.x property
valid_from, valid_until	Valid_Time_Position
created_by_ref	Producer

STIX 2.x Properties Translated to STIX 1.x Properties

STIX 2.x property	STIX 1.x property
kill_chain_phases	Kill_Chain_Phases
pattern	IndicatorExpression
indicator_types (in 2.1)	Type
labels (in 2.0)	Type

STIX 2.x Relationships Mapped Using STIX 1.x Relationships

STIX 2.x relationship type	STIX 1.x property
detects	Indicated_TTP
indicates (campaign)	Related_Campaigns
indicates (attack-pattern, malware, tool)	Indicated_TTPs
related-to (indicator)	Related_Indicators

STIX 2.x Properties Recorded in the STIX 1.x Description Property

- labels (in 2.1)

STIX 2.x Properties Not Mapped

none

An Example

STIX 2.x in JSON

```
{
        "created": "2014-05-08T09:00:00.000Z",
        "id": "indicator--53fe3b22-0201-47cf-85d0-97c02164528d",
        "labels": [
            "ip-watchlist"
        ],
        "modified": "2014-05-08T09:00:00.000Z",
        "name": "IP Address for known C2 channel",
        "pattern": "[ipv4-addr:value = '10.0.0.0']",
        "type": "indicator",
        "valid_from": "2014-05-08T09:00:00.000000Z"
}

{
        "created": "2014-05-08T09:00:00.000Z",
        "id": "relationship--9606dac3-965a-47d3-b270-8b17431ba0e4",
        "modified": "2014-05-08T09:00:00.000Z",
        "relationship_type": "indicates",
        "source_ref": "indicator--53fe3b22-0201-47cf-85d0-97c02164528d",
        "target_ref": "malware--73fe3b22-0201-47cf-85d0-97c02164528d",
        "type": "relationship"
    }
```

STIX 1.x in XML

```
<stix:Indicator id="example:indicator-53fe3b22-0201-47cf-85d0-97c02164528d" timestamp=
↪"2014-05-08T09:00:00+00:00" xsi:type='indicator:IndicatorType'>
        <indicator:Title>IP Address for known C2 channel</indicator:Title>
        <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">IP Watchlist</
↪indicator:Type>
        <indicator:Valid_Time_Position>
            <indicator:Start_Time precision="second">2014-05-08T09:00:00+00:00</
↪indicator:Start_Time>
        </indicator:Valid_Time_Position>
        <indicator:Observable id="example:Observable-9f9e8592-1a3a-42f0-8e16-56c062671a5c
↪">
            <cybox:Object id="example:Address-3923ec77-e675-4db7-b2bb-8c42717b2b3a">
                <cybox:Properties xsi:type="AddressObj:AddressObjectType" category="ipv4-
↪addr">
                    <AddressObj:Address_Value condition="Equals">10.0.0.0</
↪AddressObj:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </indicator:Observable>
        <indicator:Indicated_TTP>
            <stixCommon:TTP idref="example:ttp-73fe3b22-0201-47cf-85d0-97c02164528d"␣
↪xsi:type='ttp:TTPType'/>
        </indicator:Indicated_TTP>
    </stix:Indicator>
```

4.7 Infrastructure

STIX 2.x Properties Mapped Directly to STIX 1.x Properties

none

STIX 2.x Properties Translated to STIX 1.x Properties

STIX 2.x property	STIX 1.x property
`kill_chain_phases`	`ttp:Kill_Chain_Phases`
`infrastructure_types` (in 2.1)	`Type`
`labels` (in 2.0)	`Type`

STIX 2.x Relationships Mapped Using STIX 1.x Relationships

STIX 2.x relationship type	STIX 1.x property
`communicates-with` (infrastructure)	`ttp:Related_TTPs`
`consists-of` (infrastructure)	`ttp:Related_TTPs`
`controls` (infrastructure, malware)	`ttp:Related_TTPs`
`delivers` (malware)	`ttp:Related_TTPs`
`hosts` (malware, tool)	`ttp:Related_TTPs`
`uses` (infrastructure)	`ttp:Related_TTPs`

STIX 2.x Properties Recorded in the STIX 1.x Description Property

- `aliases`
- `first_seen`
- `labels` (in 2.1)
- `last_seen`

STIX 2.x Properties Not Mapped

none

An Example

STIX 2.x in JSON

```
{
    "created": "2014-05-08T09:00:00.000Z",
    "first_seen": "2014-05-08T09:00:00.000Z",
    "id": "infrastructure--dd955e08-16d0-4f08-a064-50d9e7a3104d",
    "infrastructure_types": [
        "malware-c2"
    ],
    "modified": "2014-05-08T09:00:00.000Z",
    "name": "Malware C2 Channel",
    "spec_version": "2.1",
    "type": "infrastructure"
}
```

STIX 1.x in XML

```
<stix:TTP id="example:infrastructure-dd955e08-16d0-4f08-a064-50d9e7a3104d"
          timestamp="2014-05-08T09:00:00+00:00" xsi:type='ttp:TTPType'>
    <ttp:Resources>
        <ttp:Infrastructure>
            <ttp:Title>Malware C2 Channel</ttp:Title>
            <ttp:Type>malware-c2</ttp:Type>
        </ttp:Infrastructure>
    </ttp:Resources>
</stix:TTP>
```

4.8 Kill Chains

STIX 1.x defined kill_chain objects for the Lockheed Martin Cyber Kill Chain. These are used by the elevator. Because they are defined outside of any partiicular content, the objects themselves will only be referred to using Kill_Chain_Phase_Reference object. Other kill chains found in the STIX 2.x will be converted as fully as possible, because all phases of a kill chain may not be present.

4.9 Location

STIX 2.x Properties Mapped Directly to STIX 1.x Properties

STIX 2.x property	STIX 1.x property
`administrative_area`	`administrative_area`
`country`	`country`

STIX 2.x Properties Translated to STIX 1.x Properties

none

STIX 2.x Relationships Mapped Using STIX 1.x Relationships

STIX 2.x relationship type	STIX 1.x property
`located-at` (identity)	`Addresses`
`located-at` (threat-actor)	`Identity/Addresses`

STIX 2.x Properties Recorded in the STIX 1.x free_text_address Property

- `latitude`
- `longitude`
- `precision`
- `region`
- `city`
- `code`
- `postal_code`

STIX 2.x Properties Not Mapped

none

An Example

STIX 2.x in JSON

```
{
  "administrative_area": "California",
  "country": "US",
  "created": "2014-11-19T23:39:03.893Z",
  "id": "location--c1445467-fd92-4532-9161-1c3024ab6467",
  "modified": "2014-11-19T23:39:03.893Z",
  "spec_version": "2.1",
  "type": "location"
}
```

STIX 1.x in XML

```
<xpil:Address>
    <xal:Country xmlns:xal="urn:oasis:names:tc:ciq:xal:3">
        <xal:NameElement>US</xal:NameElement>
    </xal:Country>
    <xal:AdministrativeArea xmlns:xal="urn:oasis:names:tc:ciq:xal:3">
        <xal:NameElement>California</xal:NameElement>
    </xal:AdministrativeArea>
</xpil:Address>
```

4.10 Malware

The Malware object in STIX 2.0 is a stub.

STIX 2.x Properties Mapped Directly to STIX 1.x Properties

none

STIX 2.x Properties Translated to STIX 1.x Properties

STIX 2.x property	STIX 1.x property
`kill_chain_phases`	`ttp:Kill_Chain_Phases`
`malware_types` (in 2.1)	`Type`
`labels` (in 2.0)	`Type`

STIX 2.x Relationships Mapped Using STIX 1.x Relationships

STIX 2.x relationship type	STIX 1.x property
`variant-of`	`ttp:Related_TTPs`
`uses`	`ttp:Related_TTPs`
`targets` (vulnerability only)	`ttp:Exploit_Targets`
`targets` (identity only)	`ttp:Victim_Targeting`

STIX 2.x Properties Recorded in the STIX 1.x Description Property

- `aliases`
- `labels` (in 2.1)

STIX 2.x Properties Not Mapped

none

An Example

STIX 2.x in JSON

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

STIX 1.x in XML

```
<stix:TTPs>
    <stix:TTP id="example:ttp-fdd60b30-b67c-11e3-b0b9-f01faf20d111" timestamp="2017-01-
↪27T13:49:53.997000+00:00" xsi:type='ttp:TTPType'>
        <ttp:Behavior>
            <ttp:Malware>
                <ttp:Malware_Instance>
                    <ttp:Type xsi:type="stixVocabs:MalwareTypeVocab-1.0">Remote Access␣
↪Trojan</ttp:Type>
                    <ttp:Name>Poison Ivy</ttp:Name>
                    <ttp:Description>Poison Ivy Trojan</ttp:Description>
                </ttp:Malware_Instance>
            </ttp:Malware>
        </ttp:Behavior>
    </stix:TTP>
</stix:TTPs>
```

4.11 Report

The Report object in 2.x 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). 1.x objects with only the `idref` property are created for each object reference in the STIX 2.x report.

STIX 2.x Properties Mapped Directly to STIX 1.x Properties

STIX 2.x property	STIX 1.x property
`name`	`Header.Title`
`description`	`Header.Description`

STIX 2.x Properties Translated to STIX 1.x Properties

STIX 2.x property	STIX 1.x property
`object_refs` (observed-data)	`Observables`
`object_refs` (indicator)	`Indicators`
`object_refs` (attack-pattern, malware, tool)	`TTPs`
`object_refs` (vulnerability)	`Exploit_Targets`
`object_refs` (course-of-action)	`Courses_Of_Action`
`object_refs` (campaign)	`Campaigns`
`object_refs` (threat-actor)	`Threat_Actors`
`object_refs` (identity, intrusion-set, relationship)	*not converted*
`report_types`	`Header.Intent`

STIX 2.x Properties Mapped Using STIX 1.x Relationships

none

STIX 2.x Properties Recorded in the STIX 1.x Description Property

- `labels` (in 2.1)
- `published`

STIX 2.x Properties Not Mapped

none

An Example

STIX 2.x 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!",
        "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",
            "indciator--66647c79-5766-4ca7-ab8a-a579056e3c83"
        ],
        "published": "2015-05-31T00:00:00.000Z",
        "type": "report"
    }
```

STIX 1.x in XML

```
<stix:Report timestamp="2015-05-07T14:22:14.760000+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␣
```

(continues on next page)

(continued from previous page)

```
↪Control Sector</report:Title>
            <report:Intent xsi:type="stixVocabs:ReportIntentVocab-1.0">Campaign␣
↪Characterization</report:Intent>
            <report:Description ordinality="1">Adversary Alpha has a campaign against␣
↪the ICS sector!
            <report:Description ordinality="2">published: 2015-05-31 00:00:00+00:00</
↪report:Description>
        </report:Header>
        <report:Campaigns>
            <report:Campaign idref="example:campaign-1855cb8a-d96c-4859-a450-abb1e7c061f2
↪" xsi:type='campaign:CampaignType'/>
        </report:Campaigns>
        <report:Indicators>
            <report:Indicator idref="example:indicator-66647c79-5766-4ca7-ab8a-
↪a579056e3c83" xsi:type='indicator:IndicatorType'/>
        </report:Indicators>
</stix:Report>
```

4.12 Threat Actor

STIX 2.x Properties Mapped Directly to STIX 1.x Properties

STIX 2.x property	STIX 1.x property
goals	Intended_Effects

STIX 2.x Properties Translated to STIX 1.x Properties

STIX 2.x property	STIX 1.x property
primary_motivation secondary_motivations personal_motivations	Motivation
sophistication	Sophistication
threat_actor_types (in 2.1)	Type
labels (in 2.0)	Type

STIX 2.x Relationships Mapped Using STIX 1.x Relationships

STIX 2.x relationship type	STIX 1.x property
uses	Observed_TTPs
attributed-to (reverse)	Associated_Campaigns
related-to (threat-actor)	Associated_Actors

STIX 2.x Properties Recorded in the STIX 1.x Description Property

- aliases
- labels (in 2.1)
- name

- resource_level
- roles

STIX 2.x Properties Not Mapped

none

An Example

STIX 2.x in JSON

```
{
        "created": "2017-01-27T13:49:54.326Z",
        "id": "threat-actor--9a8a0d25-7636-429b-a99e-b2a73cd0f11f",
        "labels": [
            "nation-state"
        ],
        "modified": "2017-01-27T13:49:54.326Z",
        "name": "Adversary Bravo",
        "sophistication": "advanced",
        "type": "threat-actor"
}
```

STIX 1.x in XML

```
<stix:Threat_Actor id="example:threat-actor-9a8a0d25-7636-429b-a99e-b2a73cd0f11f"
                   timestamp="2017-01-27T13:49:54.326000+00:00"
                   xsi:type='ta:ThreatActorType'>
        <ta:Title>Adversary Bravo</ta:Title>
        <ta:Type timestamp="2018-05-06T16:57:09.692723+00:00">
            <stixCommon:Value>State Actor / Agency</stixCommon:Value>
        </ta:Type>
        <ta:Sophistication timestamp="2018-05-06T16:57:09.692815+00:00">
            <stixCommon:Value>Expert</stixCommon:Value>
        </ta:Sophistication>
</stix:Threat_Actor>
```

4.13 Tool

STIX 2.x Properties Mapped Directly to STIX 1.x Properties

STIX 2.x property	STIX 1.x property
name	Name (from CybOX)
description	Description (from CybOX)
tool_version	Version (from CybOX)

STIX 2.x Properties Translated to STIX 2.x Properties

STIX 1.x property	STIX 1.x property
external_references	References (from CybOX)
kill_chain_phases	ttp:Kill_Chain_Phases
tool_types (in 2.1)	Type (from CybOX)
labels (in 2.0) ,	Type (from CybOX)

STIX 2.x Relationships Mapped Using STIX 1.x Relationships

STIX 2.x relationship type	STIX 1.x property
uses (attack-pattern) (reverse)	ttp:Related_TTPs
targets (identity)	ttp:Related_TTPs

STIX 2.x Properties Recorded in the STIX 1.x Description Property

- ttp:Intended_Effect

STIX 1.x Properties Not Mapped

- labels

An Example

STIX 2.x in JSON

```
{
  "type": "tool",
  "id": "tool--ce45f721-af14-4fc0-938c-000c16186418",
  "created": "2015-05-15T09:00:00.000Z",
  "modified": "2015-05-15T09:00:00.000Z",
  "name": "cachedump",
  "labels": [
    "credential-exploitation"
  ],
  "description": "This program extracts cached password hashes from a system's registry.
↪",
  "kill_chain_phases": [
    {
      "kill_chain_name": "mandiant-attack-lifecycle-model",
      "phase_name": "escalate-privileges"
    }
  ]
}
```

STIX 1.x in XML

```
<stix:TTP id="example:tool-ce45f721-af14-4fc0-938c-000c16186418" timestamp="2015-05-
↪15T09:00:00+00:00" xsi:type='ttp:TTPType'>
       <ttp:Resources>
           <ttp:Tools>
               <ttp:Tool>
                   <cyboxCommon:Description>This program extracts cached password␣
↪hashes from a system's registry.</cyboxCommon:Description>
                   <stixCommon:Title>cachedump</stixCommon:Title>
```

(continues on next page)

(continued from previous page)

```
            </ttp:Tool>
        </ttp:Tools>
    </ttp:Resources>
    <ttp:Kill_Chain_Phases>
        <stixCommon:Kill_Chain_Phase name="escalate-privileges"
                                     phase_id="example:TTP-17715bcf-84b9-4714-a3cd-
↪ffaf7fce9d10"
                                     kill_chain_name="mandiant-attack-lifecycle-model
↪"
                                     kill_chain_id="example:TTP-9df538ea-f0f0-4cf0-
↪a147-1397e51f0a63"/>
    </ttp:Kill_Chain_Phases>
</stix:TTP>
```

4.14 Vulnerability

STIX 2.x Properties Mapped Directly to STIX 1.x Properties

none

STIX 2.x Properties Translated to STIX 1.x Properties

STIX 2.x property	STIX 1.x property
external_references (source_name: cve)	CVE_ID
external_references (source_name: OSVDB_ID)	Reference

STIX 2.x Relationships Mapped Using STIX 1.x Relationships

STIX 2.x relationship type	STIX 1.x property
mitigates (reverse)	et:Potential_COAs
related-to (when not used for versioning)	et:Related_Exploit_Targets

STIX 2.x Properties Recorded in the STIX 1.x Description Property

- labels

STIX 2.x Properties Not Mapped

none

An Example

STIX 2.x in JSON

```
{
    "created": "2014-06-20T15:16:56.986Z",
    "external_references": [
        {
            "external_id": "CVE-2013-3893",
            "source_name": "cve"
        }
```

(continues on next page)

(continued from previous page)

```
    ],
    "id": "vulnerability--e77c1e36-5b43-4c5c-b8cb-7b36035f2b90",
    "modified": "2017-01-27T13:49:54.310Z",
    "name": "Heartbleed",
    "type": "vulnerability"
}
```

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>
```

CHAPTER

FIVE

MAPPINGS FROM STIX 2.X TO CYBOX 2.X

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

CybOX object types not listed have no corresponding STIX 2.x cyber observable type, and therefore are not converted by the slider.

STIX 2.x Cyber Observable Type	CybOX 2.x Type	Converted in version 2.1.0
artifact	Artifact	yes
autonomous-system	AutonomousSystem	yes
directory	File	yes
domain-name	DomainName	yes
email-addr	Address	yes
email-message	EmailMessage	yes
file	File	yes
file:archive-ext	ArchiveFile	yes
file:raster-image-ext	ImageFile	yes
file:ntfs-ext	WinFile	yes
file:pdf-ext	PDFFile	yes
file:window-pebinary-ext	WinExecutableFile	yes
ipv4-addr	Address	yes
ipv6-addr	Address	yes
mac-addr	Address	yes
mutex	Mutex	yes
network-traffic	NetworkConnection	yes
network-traffic:http-request-ext	NetworkConnection and HTTPClientRequest	yes
network-traffic:icmp-ext	NetworkConnection and ICMPv4Packet	yes
network-traffic:socket-ext	NetworkConnection and NetworkSocket	yes
network-traffic:tcp-ext	*none*	no
process	Process	yes
process:windows-process-ext	WinProcess	yes
process:windows-service-ext	WinService	yes
software	Product	yes
url	URI	yes
user-account	UserAccount, WinUser, UnixUserAccount	yes
user-account:unix-account-ext	UnixUserAccount	yes
window-registry-key	WinRegistryKey	yes
x509-certificate	X509Certificate	yes
x509-certificate:x509-v3-extensions-type	X509Certificate and X509V3Extensions	yes

CHAPTER

SIX

CONVERSION ISSUES

6.1 Single vs. Multiple

Some properties in STIX 2.x allowed for multiple values, but the corresponding property in STIX 1.x does not. In these cases, the first value is used and a warning message is output.

6.2 Related-To Relationships

It is assumed that all `related-to` relationship between the same type of object should be used to refer to self-referencing STIX 1.x relationships. For instance a `related-to` relationship between two `threat-actor` objects will be used to populate the STIX 1.x `AssociatedActors` property.

Other `related-to` relationships will be ignored and a warning message will be displayed.

6.3 Data Markings

The stix-slider currently supports object-level markings only. Granular markings are ignored and a warning message will be displayed. Since that is the highest level of data marking available in STIX 2.x, any object downgraded will contain embedded object-level markings in their STIX 1.X representation regardless of using the same marking definition in multiple places. Therefore, it can result in a verbose output compared to its 2.X counterpart. The marking-definition objects will be placed in the STIX_Header section of the document.

The supported marking types are: TLP, Statement and AIS.

6.4 Kill Chains

Kill chains and their phases in STIX 2.x are referred to by their names. There is no `id` associated with a kill chain phase. Additionally, kill chains are not defined within STIX 2.x content. The assumption is that if a kill chain is known among those sharing content, the names will be sufficient to identify them consistently.

According to the STIX 2.x specification, if the Lockheed Martin Cyber Kill Chain™ is used the `kill_chain_name` will be `lockheed-martin-cyber-kill-chain`. The phases will be converted based to STIX 1.x ids defined in https://stix.mitre.org/language/version1.2/stix_v1.2_lmco_killchain.xml

Because kill chains need to be explicitly defined within the STIX 1.x content, each kill chain phase found in the STIX 2.x content will be used to partially construct a kill chain definition. For this reason, the resultant kill chain will only contain the kill chain phases used.

6.5 Versioning

Both STIX 1.x and STIX 2.x support the versioning of objects, but there is no attempt by the slider to explicitly maintain versioning information when converting to STIX 1.x.

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.

CHAPTER

SEVEN

WARNING MESSAGES

7.1 General

Message	Code	Level
Observable Expressions should not contain placeholders	201	Error
Both console and output log have disabled messages	202	Warn
silent option is not compatible with a policy	203	Warn
options not initialized	204	Warn
Comparison Expressions in pattern of *[id]* should only have one type *[root-types]*	205	Error

7.2 Possible issue in original STIX 2.x content

Message	Code	Level
No source object exists for *[id]*. Dropping the relationship *[relationship]*	301	Warn
Unknown hash type *[hash_type]* used in *[id]*	302	Warn
NOT ASSIGNED	303	
Unknown address type *[type]* used in *[id]*	304	Warn
ref type *[type]* in *[id]* is not known	305	Warn
[cyber_observable_id] is not found. See *[id]*	306	Warn
No object *[id]* is found to add the reference to	307	Warn
[id1] is not in this bundle. Referenced from *[id2]*	308	Warn
`is_encrypted` in *[id]* is true, but no `encryption_algorithm` is given	309	Info
`is_encrypted` in *[id]* is false, but `encryption_algorithm` is given	310	Info
`is_encrypted` in *[id]* is true, but no `decryption_key` is given	311	Info
`is_encrypted` in *[id]* is false, but `decryption_key` is given	312	Info
The *[property1]* property in *[id]* should be '*[boolean]*' if the *[property2]* property is [not] present	313	Warn
Cannot convert *[id]* because it doesn't contain both a source_ref and a target_ref	314	Warn
No *[ref_property]* object exists for *[id]* in relationship *[rel-id]*	315	Warn
ref type *[type]* in *[id]* is not known	316	Warn
[id] referenced in *[id]* is not found	317	Warn
[phase_name] is not part of the Lockheed-Martin Kill Chain - see *[id]*	318	Warn

7.3 Multiple values are not supported in STIX 1.x

Message	Code	Level
[type] in STIX 2.x has multiple *[property]*, only one is allowed in STIX 1.x. Using first in list - *[value]* omitted	401	Warn
Only one dll can be represented in STIX 1.x for *[id]*, using first one - ignoring *[value]*	402	Warn

7.4 Dropping Content not supported in STIX 1.x

Message	Code	Le
The *[relationship]* relationship between *[id1]* and *[id2]* is not supported in STIX 1.x	501	W
Multiple File Extensions in *[id]* not supported yet	502	W
[property] is not representable in a STIX 1.x *[type]*. Found in *[id]*	503	W
[property] not representable in a STIX 1.x *[type]*. Found in the pattern of *[id]*	504	W
[op] cannot be converted to a STIX 1.x operator in the pattern of *[id]*	505	W
`account_type` property of *[id]* in STIX 2.x is not directly represented as a property in STIX 1.x	506	W
Received Line *[line]* in *[id]* has a prefix that is not representable in STIX 1.x	507	W
Unable to convert STIX 2.x sighting *[id]* because it doesn't refer to an indicator	508	W
Ignoring *[id]*, because a *[type]* object cannot be represented in STIX 1.1.1	509	W
Identity has no property to store `external-references` from *[id]*	510	W
pe_type SYS in *[id]* is valid in STIX 2.x, but not in STIX 1.x	511	W
pe_type [pe_type] in *[id]* is allowed in STIX 2.x, but not in STIX 1.x	512	W
[property] is an XML attribute of *[cybox object type]* in STIX 1.x, so the operator 'equals' is assumed in *[id]*	513	W
Order may not be maintained for `pdfids` in *[id]*	514	W
The `groups` property of `unix-account-ext` contains strings, but the STIX 1.x property expects integers in *[property]*	515	W
No file name provided for `binary_ref` of *[id]*, therefore it cannot be represented in the STIX 1.x `Process` object	516	W
Hashes of the `binary_ref` of *[id]* process cannot be represented in the STIX 1.x `Process` object	517	W
resolves_to_refs in *[id]* not representable in STIX 1.x	518	W
Multiple Network Traffic extensions in *[id]* not supported yet	519	W
The user_id property of *[id]* in STIX 2.x is only represented as a property in STIX 1.x on `UnixUserAccount` objects	520	W
The `path` property in *[id]* is the only directory property supportable in STIX 1.x. *[property]* is ignored	521	W
Nested Archive Files in *[id]* not handled yet	522	W
STIX 1.x can only store the body and headers of an email message in *[id]* independently	523	W
[type] pattern type in *[id]* cannot be represented in STIX 1.x	524	W
[id] is not explicitly a member of a STIX 1.x `Report`	525	W
[id] cannot be represented in STIX 1.x	526	W
Relationship between *[id]* and a location is not supported in STIX 1.x	527	W
Ignoring *[id]*, because a *[type]* object cannot be represented in STIX 1.x	528	W
Unable to populate sub-property *[property]* of *[id]*, therefore *[property]* cannot be represented in the STIX 1.x object	529	W
Extensions in *[id]* not supported in STIX 1.x	530	W
Custom extension *[extension name]* of STIX 2.1 in *[id]* are not supported	531	W
[id] does not support descriptions, so the external reference has been dropped	532	W
Ignoring *[id]*, because only new-sco extensions are supported	533	W
Ignoring *[id]*, because (deprecated) custom objects are not supported	534	W
The user account type *[type]* can not be explicitly represented in a STIX 1.x Account. See *[id]*	535	W

7.5 STIX Slider currently doesn't process this content

Message	Code	Level
The *[property]* property in *[id]* can refer to any object, so it is not handled yet.	601	Warn
number indicies in *[id]* not handled, yet	602	Warn
Unable to determine STIX 1.x type for *[id]*	603	Error
Granular Markings present in *[id]* are not supported by stix2slider	604	Warn
Source name *[name]* in external references of *[id]* not handled, yet	605	Warn
[property] property in *[id]* not handled yet	606	Warn
`contains_refs` in *[id]* not handled	607	Warn
`protocols` property in *[id]* not handled, yet	608	Warn
`tcp-ext` in *[id]* not handled, yet	609	Warn
Operator for `Artifact.Raw_Artifact` in *[id]* not handled yet	610	Warn
Nested extensions and references in patterns are not handled, yet. Found in pattern of *[id]*	611	Warn
[ref_id] in *[id]* cannot be represented in STIX 1.x	612	Warn
Multiple extensions in *[id]* are not handled, yet	613	Warn
[property] is an illegal or custom property in the pattern of *[id]*, which is not handled, yet"	614	Warn

7.6 STIX Slider conversion based on assumptions

Message	Code	Level
Assuming imcp packet in *[id]* is v4	701	Info
`InformationSource` descriptions order or content in may not correspond to the references in *[id]*	702	Info
[ref_id] in *[id]* cannot be represented explicitly as a member of a STIX 1.x report	703	Info

CHAPTER

EIGHT

CONTRIBUTING

We're thrilled that you're interested in contributing to the stix2-slider! Here are some things you should know:

- contribution-guide.org has great ideas for contributing to any open-source project (not just this one).
- All contributors must sign a Contributor License Agreement. See CONTRIBUTING.md in the project repository for specifics.
- If you are planning to implement a major feature (vs. fixing a bug), please discuss with a project maintainer first to ensure you aren't duplicating the work of someone else, and that the feature is likely to be accepted.

Now, let's get started!

8.1 Setting up a development environment

We recommend using a virtualenv.

1. Clone the repository. If you're planning to make pull request, you should fork the repository on GitHub and clone your fork instead of the main repo:

```
$ git clone https://github.com/yourusername/cti-stix-slider.git
```

2. Install develoment-related dependencies:

```
$ cd cti-stix-slider
$ pip install -r requirements.txt
```

3. Install pre-commit git hooks:

```
$ pre-commit install
```

At this point you should be able to make changes to the code.

8.2 Code style

All code should follow PEP 8. We allow for line lengths up to 160 characters, but any lines over 80 characters should be the exception rather than the rule. PEP 8 conformance will be tested automatically by Tox and Travis-CI (see below).

8.3 Testing

Note: All of the tools mentioned in this section are installed when you run `pip install -r requirements.txt`.

This project uses pytest for testing. We encourage the use of test-driven development (TDD), where you write (failing) tests that demonstrate a bug or proposed new feature before writing code that fixes the bug or implements the features. Any code contributions should come with new or updated tests.

To run the tests in your current Python environment, use the `pytest` command from the root project directory:

```
$ pytest
```

This should show all of the tests that ran, along with their status.

You can run a specific test file by passing it on the command line:

```
$ pytest stix2slider/test/test_<xxx>.py
```

To ensure that the test you wrote is running, you can deliberately add an `assert False` statement at the beginning of the test. This is another benefit of TDD, since you should be able to see the test failing (and ensure it's being run) before making it pass.

tox allows you to test a package across multiple versions of Python. Setting up multiple Python environments is beyond the scope of this guide, but feel free to ask for help setting them up. Tox should be run from the root directory of the project:

```
$ tox
```

We aim for high test coverage, using the coverage.py library. Though it's not an absolute requirement to maintain 100% coverage, all code contributions must be accompanied by tests. To run coverage and look for untested lines of code, run:

```
$ pytest --cov=stix2slider
$ coverage html
```

then look at the resulting report in `htmlcov/index.html`.

All commits pushed to the `master` branch or submitted as a pull request are tested with Travis-CI automatically.

8.4 Adding a dependency

One of the pre-commit hooks we use in our develoment environment enforces a consistent ordering to imports. If you need to add a new library as a dependency please add it to the *known_third_party* section of *.isort.cfg* to make sure the import is sorted correctly.

CHAPTER

NINE

INDICES AND TABLES

- genindex
- modindex
- search