stix2-validator Documentation

Release 3.1.3

OASIS Open

Contents:

1	Installation	
2	Usage 2.1 As A Script	6
3	Options	9
4	Checking STIX Content 4.1 Mandatory Checks - STIX 2.1	13 13 14
5	Contributing 5.1 Setting up a development environment 5.2 Code style 5.3 Testing 5.4 Adding a dependency 5.5 Updating the STIX JSON schemas	26 26 26
6	Indices and tables	29

The STIX Validator checks that STIX JSON content conforms to the requirements specified in the latest STIX 2 specifications. In addition to checking conformance with the JSON schemas, the validator checks conformance with requirements that cannot be specified in JSON schema, as well as with established "best practices." This validator is non-normative; in cases of conflict with the STIX specification, the specification takes precedence.

The STIX 2 specification contains two types of requirements: mandatory "MUST" requirements, and recommended "SHOULD" best practice requirements. The validator checks documents against the "MUST" requirements using JSON schemas. Some of these mandatory requirements cannot be implemented in JSON Schema, however, so the validator uses Python functions to check them. The "SHOULD" requirements are all checked by Python functions, and options may be used to ignore some or all of these recommended "best practices."

The STIX Validator uses the stix2-patterns validator to check that Indicator patterns conform to the STIX Patterning language and only reference properties valid for the objects in the pattern.

The validator also color-codes its output to make it easier to tell at a glance whether validation passed.

Contents: 1

2 Contents:

CHAPTER 1

Installation

Note: The STIX 2 validator requires Python 2.7 or 3.4+.

The easiest way to install the STIX 2 validator is with pip:

```
$ pip install stix2-validator
```

Note that if you instead install it by cloning or downloading the repository, you will need to set up the submodules before you install it:

```
$ git clone https://github.com/oasis-open/cti-stix-validator.git
$ cd cti-stix-validator/
$ git submodule update --init --recursive
$ python setup.py install
```

CHAPTER 2

Usage

2.1 As A Script

The validator comes with a bundled script which you can use to validate a JSON file containing STIX content:

```
$ stix2_validator <stix_file.json>
```

2.2 As A Library

You can also use this library to integrate STIX validation into your own tools. You can validate a JSON file:

```
from stix2validator import validate_file, print_results

results = validate_file("stix_file.json")
print_results(results)
```

You can also validate a JSON string, and check if the input passed validation:

```
from stix2validator import validate_string, print_results

stix_json_string = "..."
results = validate_string(stix_json_string)
if results.is_valid:
    print_results(results)
```

If your STIX is already in a Python dictionary (for example if you have already run json.loads()), use validate_instance() instead:

```
import json
from stix2validator import validate_instance, print_results
```

(continues on next page)

(continued from previous page)

```
stix_json_string = "..."
stix_obj = json.loads(stix_json_string)
results = validate_instance(stix_obj)
if results.is_valid:
    print_results(results)
```

You can pass a ValidationOptions object into validate_file(), validate_string(), or validate_instance() if you want behavior other than the default:

```
from stix2validator import ValidationOptions

options = ValidationOptions(strict=True)
results = validate_string(stix_json_string, options)
```

2.3 STIX 2 Versions

By default the validator will check content against the latest version of the STIX 2 specification. However, older versions can be checked with the version option. For example:

```
$ stix2_validator --version=2.0 <stix_file.json>
```

or in Python:

```
options = ValidationOptions(strict=True, version="2.0")
results = validate_string(stix_json_string, options)
```

2.4 Additional Schemas

The validator uses the STIX 2 JSON schemas as the basis for its validation, but you can also validate with your own additional schemas. This can help if you want to validate STIX content using extensions or (now deprecated) custom objects, properties, or observables.

To do this use the --schemas argument:

```
$ stix2_validator --schemas /path/to/my/schemas <stix_file.json>
```

or in Python, using schema_dir:

You can see some examples of custom schemas here.

Note: The schema's filename must match the extension definition id of the extension it describes so the validator can apply it correctly. For example, a schema defining a new extension with an id of

6 Chapter 2. Usage

extension-definition-bfaece0b-efa6-4dfa-8248-3d340e2030f8 should be named extension-definition-bfaece0b-efa6-4dfa-8248-3d340e2030f8 should be named extension-definition-bfaece0b-efa6-4dfa-8248-3d340e2030f8.

Note: Custom objects and properties using the x_a and x_b prefixes have been deprecated in STIX 2.1. However, if you need a schema for validating them, the validator can parse it as long as the schema's filename matches the type name of the STIX object type it should apply to. For example, a schema defining a new property on Indicators should be named indicator.json. A schema defining a new object type, "my-cool-thing", would need to be named my-cool-thing.json.

Note: When using additional schemas, the validator's built-in schemas are still checked against. Thus custom schemas only need to contain the properties that differ from the standard.

8 Chapter 2. Usage

$\mathsf{CHAPTER}\,3$

Options

These are the different options that can be set, whether the validator is used as a command-line script or as a Python library. When using the validator as a library, these options can be passed as parameters to the ValidationOptions constructor.

Script	Library	Description
FILES	files	A whitespace separated list of STIX files or directories of STIX files to validate.
-r,recursive	recursi	Recursively descend into input directories.
-s SCHEMA_DIR,	schema_o	Chustom schema directory. If provided, input will be validated against
schemas		these schemas in addition to the STIX schemas bundled with this script.
SCHEMA_DIR		
version	version	The version of the STIX specification to validate against (e.g. "2.0").
-v,verbose	verbose	Print informational notes and more verbose error messages.
-q,silent	silent	Silence all output to stdout.
-d DISABLED,	disable	A comma-separated list of recommended best practice checks to skip.
disable		By default, no checks are disabled. Example: –disable 202,210
DISABLED,ignore		
DISABLED		
-e ENABLED,	enabled	1
enable ENABLED,		If the –disable option is not used, no other checks will be run. By default,
select ENABLED		all checks are enabled. Example: –enable 218
strict	strict	Treat warnings as errors and fail validation if any are found.
strict-types	strict_	Finesure that no custom object types are used, only those defined in the
		STIX specification.
strict-properties	strict_]	Finseretthetsno custom properties are used, only those defined in the
		STIX specification.
no-cache		Disable the caching of external source values.
refresh-cache	refresh	Clears the cache of external source values, then during validation down-
		loads them again.
clear-cache		Chear the cache of external source values after validation.
enforce-refs	enforce	TENSUSTESS that all SDOs being referenced by SROs are contained within
		the same bundle.

For the list of checks that can be used with the "enabled" or "disabled" options, see the *Best Practices page*.

10 Chapter 3. Options

CHAPTER 4

Checking STIX Content

The validator will always validate input against all of the mandatory "MUST" requirements from the spec. By default it will issue warnings if the input fails any of the "SHOULD" recommendations, but validation will still pass. To turn these "best practice" warnings into errors and cause validation to fail, use the --strict option with the command-line script, or create a ValidationOptions object with strict=True when using the library.

You cannot select which of the "MUST" requirement checks will be performed; all of them will always be performed. However, you may select which of the "SHOULD" checks to perform. Use the codes from the table below to enable or disable these checks. For example, to disable the checks for the report label and tool label vocabularies, use --disable 218,222 or disabled="218,222". All the other checks will still be performed. Conversely, to only check that custom property names adhere to the recommended format but not run any of the other "best practice" checks, use --enable 103 or enabled="103".

Enabling supersedes disabling. Simultaneously enabling and disabling the same check will result in the validator performing that check.

Some checks access Internet resources to determine valid values for certain properties. For instance, the 'mimetype' check accesses the IANA's list of registered MIME types. These web requests are cached to conserve bandwidth, will expire after one week, and are stored in a file called 'cache.sqlite' in the same directory the script is run from. The cache can be refreshed manually with the --refresh-cache or refresh_cache=True, or cleared with --clear-cache or clear_cache=True. This caching can be disabled entirely with --no-cache or no cache=True.

4.1 Mandatory Checks - STIX 2.1

the syntax of the pattern.

Name	e Ensures	Errors/Warnings
times	- timestamps contain sane	' <pre>'<pre>c '<pre>c '<pre>c</pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre>
tamp	months, days, hours, min-	' <object>': '<property>': '<timestamp>' is not a valid timestamp: <mes-< td=""></mes-<></timestamp></property></object>
1	utes, seconds	sage>
	,	' <object>': '<extension>': '<property>': '<timestamp>' is not a valid</timestamp></property></extension></object>
		timestamp: <message></message>
		' <object>': '<property>': '<embedded-property>' is not a valid timestamp:</embedded-property></property></object>
		<message></message>
times	- timestamp properties with a	' <operand_1>' (<operand1_value>) must be <comparison_op></comparison_op></operand1_value></operand_1>
	_ccompareison are valid	' <operand2>' (<operand2_value)< td=""></operand2_value)<></operand2>
ob-	cyber observable timestamp	In object ' <identifier>', '<operand_1>' (<operand1_value>) must be <com-< td=""></com-<></operand1_value></operand_1></identifier>
serv-	properties with a compari-	parison_op> ' <operand_2>' (<operand2_value>)</operand2_value></operand_2>
	tinountanon iremantante valid	T
ob-	that marking definitions do	'object_marking_refs' cannot contain any references to this marking defini-
	n andt in go gʻa ciu lar <u>ir</u> cefkar refer-	tion object (no circular references)
]	ences (i.e., they do not refer-	
	ence themselves in the 'ob-	
	ject_marking_refs' property	
gran-	that marking definitions	'granular markings' cannot contain any references to this marking definition
u-	do not contain circular	object (no circular references)
	arkfegsnæiscu(ine.refsthey do	object (no chedial fereigness)
	not reference themselves	
	in the 'granular_markings'	
	property	
mark-	selectors in granular mark-	' <selector>' is not a valid selector because '<index>' is not a valid index</index></selector>
	elingsorrefyntaxitems which are	' <selector' '<selector_segment'="" a="" a<="" because="" is="" not="" selector="" td="" valid=""></selector'>
III_5_5	actually present in the object	list.
	actuary present in the object	' <selector>' is not a valid selector because '<selector_segment>' is not a</selector_segment></selector>
		property.
ob-	certain observable object	' <pre>'<pre>'<pre>can't resolve '<embed-< pre=""></embed-<></pre></pre></pre>
serv-	properties reference the	property>' reference ' <identifier>'</identifier>
	olojande atete penote object	' <pre>'<pre>'<pre>reference 'ddentifier' '<pre>' must refer to an object of</pre></pre></pre></pre>
	o a jeu care per me moje e c	type ' <type(s)>'</type(s)>
ar-	the 'mime_type' property of	the 'mime_type' property of object ' <identifier>' ('<mime_type>') must be</mime_type></identifier>
ti-	artifact objects comes from	an IANA registered MIME Type of the form 'type/subtype'.
	mithee Tiempe late column in the	
	IANA media type registry	
char-	certain properties of cy-	The 'path_enc' property of object ' <identifier>' ('<path_enc>') must be an</path_enc></identifier>
ac-	ber observable objects come	IANA registered character set.
	et from the IANA Character	The 'name_enc' property of object ' <identifier>' ('<name_enc>') must be</name_enc></identifier>
	Set list.	IANA registered character set.
lan-	the 'lang' property of SDOs	' <lang>' is not a valid RFC 5646 language code.</lang>
	e is a valid RFC 5646 lan-	claires is not a varie of 50 to language code.
Suase	guage code	
soft-	the 'language' property of	The 'languages' property of object ' <identifier>' contains an invalid code</identifier>
	_language objects is a valid	(' <lang>').</lang>
,, 410	ISO 639-2 language code	
pat-	that the syntax of the pattern	' <object>' is not a valid observable type name</object>
terns	of an indicator is valid, and	Custom Observable Object type ' <object>' should start with 'x-' followed</object>
W1115	that objects and properties	by a source unique identifier (like a domain name with dots replaced by
	referenced by the pattern	hyphens), a hyphen and then the name
	are valid. This runs the	Custom Observable Object type ' <object>' should start with 'x-'</object>
.1. M	latidatory Checks r- \$11X s2. //github.com/oasis-open/cti-	' <pre></pre>
	pattern-validator) to check	'x_' followed by a source unique identifier (like a domain name with dots
	patiern-vanuator) to check	1 A_ TOHOWER BY A SOURCE HINGUE RECHRING (TIKE A ROTHAILI HAIRE WILLI ROTS

replaced by underscores), an underscore and then the name

Criban Obsamiable Object quetom man

4.2 Optional Checks - STIX 2.1

Code	Name	Ensures	Errors/Warnings
1	format-checks	all 1xx checks are run.	
		Specifically:	

Table 1 – continued from previous page

101	Table 1 – continued	<u></u>	N. m
101	custom-prefix	names of custom object	Note: This checks func-
		types, properties, observ-	tionality that has been
		able objects, observable	deprecated and replaced
		object properties, and observable object extensions	by extensions. Thus, this check only runs if
		follow the correct format	extensions-use (401) is
		10110W the correct format	disabled.
			custom object type ' <ob-< th=""></ob-<>
			ject>' should start with 'x-
			, followed by a source
			unique identifier (like a
			domain name with dots re-
			placed by hyphens), a hy-
			phen and then the name.
			custom property ' <pre>rop-</pre>
			erty>' should have a type
			that starts with 'x_' fol-
			lowed by a source unique identifier (like a domain
			name with dots replaced
			by a hyphen), a hyphen
			and then the name.
			Custom Observable
			Object type ' <observ-< th=""></observ-<>
			able_object>' should start
			with 'x-' followed by a
			source unique identifier
			(like a domain name
			with dots replaced by
			hyphens), a hyphen and then the name.
			Custom Cyber Observ-
			able Object extension
			type ' <observable-object-< th=""></observable-object-<>
			extension>' should start
			with 'x-' followed by a
			source unique identifier
			(like a domain with dots
			replaced by hyphens),
			a hyphen and then the
			name. Cyber Observ-
			able Object custom
			property ' <observ-< th=""></observ-<>
			able_object_property>'
			should start with 'x_'
			followed by a source
			unique identifier (like a
			domain name with dots
			replaced by hyphens),
			a hyphen and then the
			name.
			Cyber Observable Object
			custom property ' <pre>crty>' in the <extension></extension></pre>
4.2. Optional Checks - S	TIX 2.1		erty>' in the <extension> extension should star15</extension>
• pt.onai oncoko • o			with 'x_' followed by
			a source unique (like a
			domain name with dots
	1		

Table 1 – continued from previous page

nient; no source identifier needed in prefix tionality that has been deprecated and replaced by extensions. Thus, this check only runs if extensions use (401) is disabled. custom object type ' <objects' '<observable="" '<pre="" 'spropertys'="" 'x-'="" 'x-'.="" 2="" a="" be="" compatible="" custom="" cyber="" extension'="" future="" have="" in="" object="" observable="" of="" order="" property="" should="" specification.="" start="" starts="" stix="" that="" the="" to="" type="" versions="" with=""> custom property '<pre> in the <pre> custom property '</pre> in the <pre> custom property '</pre> in the <pre> custom property '<pre> custom property '<pre> custom property '<pre> custom property '<pre> in the <extension '<pre="" 'x-'.="" custom="" cyber="" object="" observable="" property="" should="" start="" with=""> custom property '<pre> custom property '</pre> c</pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></extension></pre></pre></pre></pre></pre></pre></objects'>	102	custom prefix lay	same as 101 but more le-	Note: This checks func-
deprecated and replaced by extensions. Thus, this check only runs if extensions-use (401) is disabled. custom object type ' <objects' '<pre="" 'x-'="" 2="" be="" compatible="" custom="" future="" in="" of="" order="" property="" should="" specification.="" start="" stix="" the="" to="" versions="" with="">cutys' should have a type that starts with 'x_' in order to be compatible with future versions of the STIX 2 specification. Custom Observable Object type '<observable_objects' '<observable_object_extension'="" '<pre="" 'x_'.="" custom="" cyber="" extension="" object="" observable="" property="" should="" start="" type="" with="">crtys' should start with 'x_'. Cyber Observable Object custom property '<membedded_propertys' <pre="" in="" the="">cpropertys' of the <observable_object_object_should '<pre="" 'x_'.="" custom="" cyber="" object="" observable="" property="" start="" with="">crtys' in the <pre>cycler object_should start with 'x_'. Cyber Observable Object custom property '<pre>crtys' in the <pre>cycler object_should start with 'x_'. Cyber Observable Object custom property '<pre>crtys' in the <pre>cycler object_should start with 'x_'. Cyber Observable Object custom property '<pre>crtys' in the <pre>cycler observable Object custom property '<pre>crtys' in the <pre>cycler observable Object custom property '<pre>crtys' observable Object custom property '<pre>crtys' observable Object custom property '<pre>cyporetys' in the <pre>cycler observable Object custom property '<pre>cyporetys' in the <<pre>cycler observable Object custom property '<pre>cyporetys' in the <</pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></observable_object_object_should></membedded_propertys'></observable_objects'></objects'>	102	custom-prefix-lax		
by extensions. Thus, this check only runs if extensions-use (401) is disabled. custom object type 'cob-ject>' should start with 'x-' in order to be compatible with future versions of the STIX 2 specification. custom property 'sproperty>' should have a type that starts with 'x-' in order to be compatible with future versions of the STIX 2 specification. Custom observable object type 'cobservable_object' should start with 'x-'. Custom Observable Object type 'cobservable_object' should start with 'x-'. Custom Observable Object extensions' should start with 'x-'. Cyber Observable Object custom property 'cproperty>' should start with 'x-'. Cyber Observable Object custom property 'cproperty>' should start with 'x-'. Cyber Observable Object custom property 'cproperty> of the <object 'cproperty="" custom="" property=""> in the <pre>cycloper observable Object custom property 'cproperty> in the <pre>cxtension should start with 'x-'. Cyber Observable Object custom property 'cproperty> in the <pre>cxtension should start with 'x-'. Cyber Observable Object custom property 'cproperty> in the <pre>cxtension should start with 'x-'. Cyber Observable Object custom property 'cproperty> in the <pre>cxtension should start with 'x-'. Cyber Observable Object custom property 'cproperty> in the <pre>cxtension should start with 'x-'. Cyber Observable Object custom property 'cproperty> property> in the <pre>cxtension should start with 'x-'. Cyber Observable Object custom property> propert</pre></pre></pre></pre></pre></pre></pre></object>				=
this check only runs if extensions-use (401) is disabled. custom object type ' <object's '<observable="" 'eproperty's="" 'epropertys'="" 'extension="" 'extensions'="" 'should="" 'x,'="" 'x,'.="" 'x_'.<="" 2="" a="" be="" compatible="" custom="" cyber="" extension="" extension's="" future="" have="" in="" object="" object'="" object,="" observable="" of="" order="" property="" should="" specification.="" start="" starts="" stix="" td="" that="" the="" to="" type="" versions="" with=""><td></td><td></td><td>needed in prefix</td><td>=</td></object's>			needed in prefix	=
extensions-use (401) is disabled. custom object type ' <objects' 'cembedded_propertys'="" 'cobservable_object_extension'="" 'cobservable_objects'="" 'cproperty's="" 'cpropertys'="" 'x-'="" 'x-'.="" 'x_'="" 'x_'.="" 2="" <object="" a="" be="" compatible="" custom="" cyber="" cypo<="" cypopertys'="" extension="" future="" have="" in="" object="" observable="" of="" order="" property="" should="" specification.="" start="" starts="" stix="" td="" that="" the="" to="" type="" versions="" with="" yise=""><td></td><td></td><td></td><td>•</td></objects'>				•
disabled. custom object type ' <objects' 'cembedded_propertys'="" 'cobservable="" 'coppert<="" 'coppertys'="" 'cpropertys'="" 'propertys'="" 'x-'="" 'x-'.="" 'x_'="" 2="" a="" be="" compatible="" custom="" cyber="" extension="" extension'="" future="" have="" in="" object="" observable="" of="" order="" property="" should="" specification.="" start="" starts="" stix="" sttx="" td="" that="" the="" to="" type="" versions="" with="" ye'=""><td></td><td></td><td></td><td></td></objects'>				
custom object type 'cobjects' should start with 'x- 'in order to be compatible with future versions of the STIX 2 specification. custom property 'cpropertys' should have a type that starts with 'x_' in order to be compatible with future versions of the STIX 2 specification. Custom Observable With future versions of the STIX 2 specification. Custom Observable Object type 'cobservable-object' should start with 'x_'. Custom Observable Object extension type 'cobservable-object extension type 'cobservable-object extension type 'sobservable-object extension type 'sobservable Object custom property 'cproperty's should start with 'x_'. Cyber Observable Object custom property 'sem- bedded_propertys' in the cypopertys' of the <object 'cpropertys'="" 'x_'.="" 'x_'.<="" <extension="" custom="" cyber="" in="" ject="" ob-="" object="" observable="" property="" should="" start="" td="" the="" to="" with=""><td></td><td></td><td></td><td>extensions-use (401) is</td></object>				extensions-use (401) is
ject>'should start with 'x-' in order to compatible with future versions of the STIX 2 specification. custom property 'cproperty>' should have a type that starts with 'x_' in order to be compatible with future versions of the STIX 2 specification. Custom Observable Object type ' <observable '<observable-object_extensions'="" '<pre="" 'x-'.="" custom="" cyber="" extension="" object="" objects'="" observable="" property="" should="" start="" type="" with="">custom property '<pre>certy>' should start with 'x_'. Cyber Observable Object custom property '<mbedded_property>' in the <pre>cproperty> of the <object '<mbedded_property="" 'x_'.="" custom="" cyber="" object="" observable="" property="" should="" start="" with="">' in the <pre>cproperty> of the <object '<pre="" 'x_'.="" custom="" cyber="" object="" observable="" property="" should="" start="" with="">perty> in the <pre>custom property '<mbedded_property> in the <pre>perty> in the <extensions '<pre="" 'x_'.="" custom="" cyber="" object="" observable="" property="" should="" start="" with="">perty> in the <extension '<pre="" 'x_'.="" custom="" cyber="" object="" observable="" property="" should="" start="" with="">property> in the <extension property=""> in the <extension 'x_'.<="" should="" start="" td="" with=""><td></td><td></td><td></td><td>disabled.</td></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extensions></pre></mbedded_property></pre></object></pre></object></pre></mbedded_property></pre></observable>				disabled.
in order to be compatible with future versions of the STIX 2 specification. custom property ' <pre>custom property '<pre>custom property '<pre>custom property '<pre>custom property '<pre>custom property '<pre>custom property '<pre>custom property custom observable</pre></pre></pre></pre></pre></pre></pre>				custom object type ' <ob-< td=""></ob-<>
with future versions of the STIX 2 specification. custom property 'cyrop- erty>' should have a type that starts with 'x.' in order to be compatible with future versions of the STIX 2 specification. Custom Observable Object type 'cobservable Object type 'cobservable Object extension type 'cobservable- object_extension>' should start with 'x-'. Cyber Observable Object custom property 'cyrop- erty>' should start with 'x.'. Cyber Observable Object custom property 'cyrop- erty>' should start with 'x.'. Cyber Observable Object custom property 'cyrop- erty>' in the 'cyrop-				ject>' should start with 'x-
with future versions of the STIX 2 specification. custom property 'cyrop- erty>' should have a type that starts with 'x.' in order to be compatible with future versions of the STIX 2 specification. Custom Observable Object type 'cobservable Object type 'cobservable Object extension type 'cobservable- object_extension>' should start with 'x-'. Cyber Observable Object custom property 'cyrop- erty>' should start with 'x.'. Cyber Observable Object custom property 'cyrop- erty>' should start with 'x.'. Cyber Observable Object custom property 'cyrop- erty>' in the 'cyrop-				'in order to be compatible
STIX 2 specification. custom property ' <pre>retys' should have a type that starts with 'x_' in order to be compatible with future versions of the STIX 2 specification. Custom Observable Object type '<observable_objects' '<observable-object_extensions'="" '<pre="" 'x_'.="" custom="" cyber="" extension="" object="" observable="" property="" should="" start="" type="" with="">retrys' should start with 'x_'. Cyber Observable Object custom property '<pre>retrys' should start with 'x_'. Cyber Observable Object custom property '<cm- <pre="" bedded_propertys'="" in="" the=""><pre>cpropertys</pre> of the <obs '<pre="" 'x_'.="" custom="" cyber="" jects="" object="" observable="" property="" should="" start="" with="">retrys' in the <extensions '<pre="" 'x_'.="" custom="" cyber="" extension="" object="" observable="" property="" should="" start="" with="">retrys' in the <extensions '<pre="" 'x_'.="" custom="" cyber="" extension="" object="" observable="" property="" should="" start="" with="">retrys' in the <extension '<pre="" property="">retrys' in the <extension '<="" pre="" property=""></extension></extension></extension></extension></extension></extension></extensions></extensions></obs></cm-></pre></observable_objects'></pre>				-
custom property ' <property>' should have a type that starts with 'x.' in order to be compatible with future versions of the STIX 2 specification. Custom Observable Object (pp: '<observable_object>' should start with 'x'. Custom Observable Object extension type '<observable_object_extension>' should start with 'x'. Cyber Observable Object custom property '<property>' should start with 'x.'. Cyber Observable Object custom property '<pre> custom property '<mbox bedded_property="">' in the '<pre> <pre> <pre> </pre> <pre> Cyber Observable Object custom property of the <object '<mbox="" 'x.'.="" bedded_property="" custom="" cyber="" object="" observable="" property="" should="" start="" with="">' in the '<pre> <pre> <pre> <pre> <pre> property of the <object '<pre="" 'x.'.="" custom="" cyber="" object="" observable="" property="" should="" start="" with=""> Cyber Observable Object custom property '<pre> Cyber Observable Object custom property '<pre< td=""><td></td><td></td><td></td><td></td></pre<></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></object></pre></pre></pre></pre></pre></object></pre></pre></pre></mbox></pre></property></observable_object_extension></observable_object></property>				
erty>' should have a type that starts with 'x_' in order to be compatible with future versions of the STIX 2 specification. Custom Observable Object type ' <observable_objects' '<observable-object_extension="" 'x-'.="" custom="" extension="" object="" observable="" should="" start="" type="" with="">' should start with 'x-'. Cyber Observable Object custom property '<pre>custom property '<em- bedded_property=""> in the <pre>property> of the <object '<pre="" custom="" property="">property> in the <pre>property> in the <extension 'x_'.<="" pre="" should="" start="" with=""> Cyber Observable Object custom property '<pre>property> in the <extension 'x_'.<="" pre="" should="" start="" with=""> Cyber Observable Object custom property '<pre>property> in the <extension property=""> in the <extensio< td=""><td></td><td></td><td></td><td></td></extensio<></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></extension></pre></extension></pre></extension></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></object></pre></em-></pre></observable_objects'>				
that starts with 'x_' in order to be compatible with future versions of the STIX 2 specification. Custom Observable Object type ' <observable_object>'should start with 'x-'. Custom Observable Object extension type '<observable-object_extensions' '<propertys'="" 'cembedded_propertys'="" 'x-'.="" 'x_'.="" <pre="" custom="" cyber="" in="" object="" observable="" observable-object_extensions'="" property="" should="" start="" the="" with=""></observable-object_extensions'></observable_object>				
order to be compatible with future versions of the STIX 2 specification. Custom Observable Object type ' <observable_object> should start with 'x.'. Custom Observable Object extension type '<observable-object_extensions' '<pre="" 'x.'.="" custom="" cyber="" object="" observable="" property="" should="" start="" with="">crty>' should start with 'x.'. Cyber Observable Object custom property '<embedded_property>' in the <pre>croperty> of the <object 'sproperty="" 'x.'.="" custom="" cyber="" object="" observable="" property="" should="" start="" with=""> in the <pre>croperty> of the <object 'sproperty="" 'x.'.="" custom="" cyber="" object="" observable="" property="" should="" start="" with="">' in the <extension 'cyproperty="" 'x.'.="" custom="" cyber="" object="" observable="" property="" should="" start="" with="">' in the <extension 'cyproperty="" 'x.'.="" custom="" cyber="" object="" observable="" property="" should="" start="" with=""> in the <extension 'cyproperty="" property=""> in the <extension 'cyproperty="" property=""> of the <extension 'x.'.<="" <extension="" extension="" of="" property="" should="" sono="" start="" td="" the="" with=""><td></td><td></td><td></td><td></td></extension></extension></extension></extension></extension></object></pre></object></pre></embedded_property></observable-object_extensions'></observable_object>				
with future versions of the STIX 2 specification. Custom Observable Object type 'cobservable_objectz' should start with 'x-'. Custom Observable Object extension type 'cobservable-object_extensions' should start with 'x-'. Cyber Observable Object custom property 'cyroperty>' should start with 'x_'. Cyber Observable Object custom property 'cembedded_property>' in the <pre></pre>				
STIX 2 specification. Custom Observable Object type ' <observ- able_object="">' should start with 'x-'. Custom Observable Object extension type '<observable- object_extension="">' should start with 'x-'. Cyber Observable Object custom property '<property>' should start with 'x_'. Cyber Observable Object custom property of the <object> object should start with 'x_'. Cyber Observable Object custom property>' in the <property> of the <object> object should start with 'x_'. Cyber Observable Object custom property '<property>' in the <extension> extension should start with 'x_'. Cyber Observable Object custom property '<property>' cyroperty>' in the <extension '<property="" 'x_'.="" custom="" cyber="" object="" observable="" property="" should="" start="" with="">' in the <extension '<property="" property=""> in the <extension '<property="" <extension="" of="" of<="" property="" td="" the=""><td></td><td></td><td></td><td></td></extension></extension></extension></property></extension></property></object></property></object></property></observable-></observ->				
Custom Observable Object type 'cobserv- able_objects' should start with 'x-'. Custom Observable Object extensions' should start with 'x-'. Cyber Observable Object custom property 'cyrop- ertys' should start with 'x_'. Cyber Observable Object custom property 'cem- bedded_propertys' in the <pre> <pre> <pre> <pre> <pre> custom property 'cyrop- ertys' object should start with 'x_'. Cyber Observable Object custom property 'cyrop- ertys' in the <extensions '<="" 'cyrop-="" 'x_'.="" <extensions="" custom="" cyber="" ertys'="" extension="" in="" ject="" ob-="" observable="" property="" should="" start="" td="" the="" with=""><td></td><td></td><td></td><td></td></extensions></pre></pre></pre></pre></pre>				
Object type ' <observable_object>' should start with 'x-'. Custom Observable Object extension type '<observable-object_extension>' should start with 'x-'. Cyber Observable Object custom property '<pre>erty>' should start with 'x_'. Cyber Observable Object custom property '<embedded_property>' in the <pre>qproperty> of the <object '<pre="" 'x_'.="" custom="" cyber="" object="" observable="" property="" should="" start="" with="">crty>' in the <pre>cypoperty>' in the <pre>cypoperty> in cypoperty> in cypoperty> in the <pre>cypoperty> in the <pre>cypoperty> in the <pre>cypoperty> in cypoperty> in cy</pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></object></pre></embedded_property></pre></observable-object_extension></observable_object>				-
able_object>' should start with 'x-'. Custom Observable Object extension type ' <observable-object_extension>' should start with 'x-'. Cyber Observable Object custom property '<pre>cproperty>' should start with 'x_'. Cyber Observable Object custom property '<embedded_property>' in the <pre>property> of the <object '<pre="" 'x_'.="" <object="" custom="" cyber="" object="" observable="" of="" property="" should="" start="" the="" with="">cproperty>' in the <extension> extension should start with 'x_'. Cyber Observable Object custom property '<pre>cproperty>' in the <extension_property> in the <extension_property> property of the <extension_property> property of the <extension 'x_'.<="" should="" start="" td="" with=""><td></td><td></td><td></td><td></td></extension></extension_property></extension_property></extension_property></pre></extension></object></pre></embedded_property></pre></observable-object_extension>				
with 'x-'. Custom Observable Object extension type ' <observable- object_extension="">' should start with 'x-'. Cyber Observable Object custom property '<property>' should start with 'x_'. Cyber Observable Object custom property > of the <object> object should start with 'x_'. Cyber Observable Object custom property> of the <object> object should start with 'x_'. Cyber Observable Object custom property '<property>' in the <extension> extension should start with 'x_'. Cyber Observable Ob- ject custom property '<property>' in the <extension_property> property of the <extension_property> property of the <extension> extension should start with 'x_'.</extension></extension_property></extension_property></property></extension></property></object></object></property></observable->				
Custom Observable Object extension type ' <observable- object_extension="">' should start with 'x-'. Cyber Observable Object custom property '<property>' should start with 'x_'. Cyber Observable Object custom property '<embedded_property>' in the <property> of the <object '<property="" 'x_'.="" custom="" cyber="" object="" observable="" property="" should="" start="" with=""> of the <object '<property="" 'x_'.="" custom="" cyber="" object="" observable="" property="" should="" start="" with="">' in the <extension> extension should start with 'x_'. Cyber Observable Object custom property '<property>' in the <extension- '<property="" extension_property="">' in the <extension_property '<property="">' in the <extension_property '<property="">' of the <extension> extension property '<property>' in the <extension> extension property '<pre> cyproperty> in the <extension> extension property '<pre> cyproperty> in the <extension> extension property '<pre> cyproperty of the <extension> extension should start with 'x_'.</extension></pre></extension></pre></extension></pre></extension></property></extension></extension_property></extension_property></extension-></property></extension></object></object></property></embedded_property></property></observable->				
Object extension type ' <observable-object_extension>' should start with 'x-'. Cyber Observable Object custom property 'cproperty>' should start with 'x_'. Cyber Observable Object custom property 'cembedded_property>' in the <property> of the <object 'cproperty="" 'x_'.="" custom="" cyber="" object="" observable="" property="" should="" start="" with=""> object should start with 'x_'. Cyber Observable Object custom property 'cproperty>' in the <extension> extension should start with 'x_'. Cyber Observable Object custom property 'cproperty>' in the <extension 'x_'.<="" should="" start="" td="" with=""><td></td><td></td><td></td><td></td></extension></extension></object></property></observable-object_extension>				
type ' <observable- object_extension="">' should start with 'x-'. Cyber Observable Object custom property '<property>' should start with 'x_'. Cyber Observable Object custom property '<em- bedded_property="">' in the <pre></pre></em-></property></observable->				
object_extension>' should start with 'x-'. Cyber Observable Object custom property ' <property>' should start with 'x_'. Cyber Observable Object custom property '<embedded_property>' in the <pre><pre><pre><pre></pre></pre></pre></pre></embedded_property></property>				3
should start with 'x-'. Cyber Observable Object custom property ' <property>' should start with 'x_'. Cyber Observable Object custom property '<embedded_property>' in the <property> of the <object '<property="" 'x_'.="" custom="" cyber="" object="" observable="" property="" should="" start="" with=""> in the <extension> extension should start with 'x_'. Cyber Observable Object custom property '<property>' in the <extension '<property="" 'x_'.="" custom="" cyber="" object="" observable="" property="" should="" start="" with="">' in the <extension '<property="" property="">' in the <extension 'x_'.<="" <extension="" of="" property="" should="" start="" td="" the="" with=""><td></td><td></td><td></td><td>V 1</td></extension></extension></extension></property></extension></object></property></embedded_property></property>				V 1
Cyber Observable Object custom property ' <pre>'<pre>crty>' should start with 'x_'. Cyber Observable Object custom property '<em- bedded_property="">' in the <pre><pre>cproperty> of the <ob- ject=""> object should start with 'x_'. Cyber Observable Object custom property '<pre>crty>' in the <extension> extension should start with 'x_'. Cyber Observable Ob- ject custom property '<pre>'<pre>crustom property</pre> '<pre>in the <extension_property> property> in the <extension_property> property of the <extension> extension should start with 'x_'.</extension></extension_property></extension_property></pre></pre></extension></pre></ob-></pre></pre></em-></pre></pre>				
custom property ' <property>' should start with 'x_'. Cyber Observable Object custom property '<embedded_property>' in the <pre></pre></embedded_property></property>				
erty>' should start with 'x_'. Cyber Observable Object custom property ' <embedded_property>' in the <pre></pre></embedded_property>				Cyber Observable Object
'x_'. Cyber Observable Object custom property ' <embedded_property>' in the <pre></pre></embedded_property>				custom property ' <prop-< td=""></prop-<>
Cyber Observable Object custom property ' <embedded_property>' in the <pre></pre></embedded_property>				erty>' should start with
custom property ' <embedded_property>' in the <pre></pre></embedded_property>				'x_'.
bedded_property>' in the <pre></pre>				Cyber Observable Object
<pre><pre><pre><pre><pre><pre><pre><pre></pre></pre></pre></pre></pre></pre></pre></pre>				custom property ' <em-< td=""></em-<>
<pre><pre><pre><pre><pre><pre><pre><pre></pre></pre></pre></pre></pre></pre></pre></pre>				bedded_property>' in the
ject> object should start with 'x_'. Cyber Observable Object custom property ' <property>' in the <extension> extension should start with 'x_'. Cyber Observable Object custom property '<property>' in the <extension_property> property of the <extension> sion> extension should start with 'x_'.</extension></extension_property></property></extension></property>				
with 'x_'. Cyber Observable Object custom property ' <property>' in the <extension> extension should start with 'x_'. Cyber Observable Object custom property '<property>' in the <extension_property> property of the <extension> extension should start with 'x_'.</extension></extension_property></property></extension></property>				
Cyber Observable Object custom property ' <pre> custom property '<pre> erty>' in the <extension> extension should start with 'x_'. Cyber Observable Object custom property '<pre> '<pre> property>' in the <extension_property> property of the <extension> extension should start with 'x_'. </extension></extension_property></pre></pre></extension></pre></pre>				
custom property ' <pre>'<pre>rety>' in the <extension> extension should start with 'x_'. Cyber Observable Ob- ject custom property '<pre>'<pre>'<pre>property>' in the <extension_property> property of the <extension> extension should start with 'x_'.</extension></extension_property></pre></pre></pre></extension></pre></pre>				
erty>' in the <extension> extension should start with 'x_'. Cyber Observable Ob- ject custom property '<property>' in the <extension_property> property of the <extension> extension should start with 'x_'.</extension></extension_property></property></extension>				•
extension should start with 'x_'. Cyber Observable Object custom property ' <property>' in the <extension_property> property of the <extension> extension should start with 'x_'.</extension></extension_property></property>				
with 'x_'. Cyber Observable Object custom property ' <property>' in the <extension_property> property of the <extension> extension should start with 'x_'.</extension></extension_property></property>				•
Cyber Observable Object custom property ' <pre>'<pre>'<pre>'<pre>'<pre>property>' in the </pre> extension_property> property of the <extension> extension should start with 'x_'.</extension></pre></pre></pre></pre>				
ject custom property ' <property>' in the <extension_property> property of the <extension> extension should start with 'x_'.</extension></extension_property></property>				
' <pre>'<pre>cytension_property> property of the <extension 'x_'.<="" pre="" should="" start="" with=""></extension></pre></pre>				-
<pre> <extension_property> property of the <extension> extension should start with 'x_'. </extension></extension_property></pre>				
property of the <extension> extension should start with 'x_'.</extension>				
sion> extension should start with 'x_'.				
start with 'x_'.				
				start with 'x_'. Continued on next page

Table 1 – continued from previous page

	Table 1 – Continued		
103	uuid-check	objects use the recommended versions of UUID (v5 for SCOs, v4 for the rest)	Cyber Observable ID value <identifier> is not a valid UUIDv5 ID. Given ID value <identifier> is not a valid UUIDv4 ID.</identifier></identifier>
111	open-vocab-format	values of open vocabularies follow the correct format	Open vocabulary value ' <value>' should be all lowercase and use hyphens instead of spaces or underscores as word separators.</value>
121	kill-chain-names	kill-chain-phase name and phase follow the correct format	kill_chain_name ' <chain_name>' should be all lowercase and use hyphens instead of spaces or underscores as word separators. phase_name '<phase_name>' should be all lowercase and use hyphens instead of spaces or underscores as word separators</phase_name></chain_name>
141	observable-object-keys	observable object keys follow the correct format	' <key_value>' is not a good key value. Observ- able Objects should use non- negative integers for their keys.</key_value>
142	observable-dictionary- keys	dictionaries in cyber ob- servable objects follow the correct format	As a dictionary key, ' <key_value>' should be lowercase.</key_value>
143	malware-analysis-product	malware analysis product names follow the correct format	The 'product' property of object ' <identifier>' should be all lowercase with words separated by dash.</identifier>
149	windows-process- priority-format	windows-process-ext's 'priority' follows the correct format	The 'priority' property of object ' <identifier>' should end in '_CLASS'.</identifier>

Table 1 – continued from previous page

150	hash-length	keys in 'hashes'-type	Object ' <identifier>'</identifier>
130	nasn-tength	properties are not too long	has a 'hashes' dictio-
		properties are not too long	nary with a hash of type
			' <hash_type>', which is</hash_type>
			longer than 30 characters.
			Object ' <identifier>' has</identifier>
			an NTFS extension with
			an alternate data stream
			that has a 'hashes' dictio-
			nary with a hash of type
			' <hash_type>', which is</hash_type>
			longer than 30 characters.
			Object ' <identifier>' has</identifier>
			a Windows PE Binary
			File extension with a file
			header hash of ' <hash>',</hash>
			which is longer than 30
			characters.
			Object ' <identifier>' has a</identifier>
			Windows PE Binary File
			extension with an optional
			header that has a hash of
			' <hash>', which is longer</hash>
			than 30 characters.
			Object ' <identifier>' has</identifier>
			a Windows PE Binary
			File extension with a sec-
			tion that has a hash of
			' <hash>', which is longer</hash>
			_
			than 30 characters. Object ' <identifier>'</identifier>
			3
			hash a 'hashes' dictio-
			nary with a hash of type
			' <hash_type>', which is</hash_type>
			longer than 30 characters.
2	approved-values	all 2xx checks are run.	
		Specifically:	
201	marking-definition-type	marking definitions use a	Marking definition 'def-
		valid definition_type	inition_type' should
			be one of: <marking-< td=""></marking-<>
			definition-type>.

Table 1 – continued from previous page

202		ed Irom previous page	4 1
202	relationship-types	relationships are among those defined in the spec-	' <object>' is not a sug- gested relationship source</object>
		ification	object for the ' <relation-< td=""></relation-<>
			ship>' relationship.
			' <relationship>' is not</relationship>
			a suggested relation-
			ship type for ' <object>'</object>
			objects.
			' <object>' is not a sug-</object>
			gested relationship target
			object for ' <object>' ob-</object>
			jects with the ' <relation-< td=""></relation-<>
			ship>' relationship.
203	duplicate-ids	objects in a bundle with	Duplicate ID ' <iden-< td=""></iden-<>
		duplicate IDs have differ-	tifier>' has identical
		ent <i>modified</i> timestamps	'modified' timestamp. If
			they are different versions
			of the same object, they
			should have different
210	11 1	11 6 4 6 11	'modified' properties,
210	all-vocabs	all of the following open	(
		vocabulary checks are run	' <pre>'<pre>contains a value not in</pre></pre>
			the <vocab_name>-</vocab_name>
			ov vocabulary.
211	attack-motivation	certain property values	' <pre>'<pre>contains a</pre></pre>
		are from the attack-	value not in the attack-
		motivation vocabulary	motivation-ov vocabulary
212	attack-resource-level	certain property values are	' <pre>'<pre>contains a</pre></pre>
		from the attack-resource-	value not in the attack-
		from the attack-resource- level vocabulary	resource-level-ov vocabu-
212		level vocabulary	resource-level-ov vocabu- lary
213	identity-class	level vocabulary certain property values are	resource-level-ov vocabulary ' <pre>'<pre>contains a</pre></pre>
213		certain property values are from the identity-class vo-	resource-level-ov vocabulary ' <pre>'<pre>contains a value not in the identity-</pre></pre>
	identity-class	certain property values are from the identity-class vocabulary	resource-level-ov vocabulary ' <pre>'<pre>'<pre>contains a value not in the identity- class-ov vocabulary</pre></pre></pre>
213		certain property values are from the identity-class vocabulary certain property values are	resource-level-ov vocabulary ' <pre>'<pre>'<pre>contains a value not in the identity- class-ov vocabulary '<pre>'<pre>contains a</pre></pre></pre></pre></pre>
	identity-class	certain property values are from the identity-class vo-cabulary certain property values are from the indicator-types	resource-level-ov vocabulary ' <pre>'<pre>'<pre>'<pre>contains a value not in the identity- class-ov vocabulary '<pre>'<pre>contains a value not in the indicator-</pre></pre></pre></pre></pre></pre>
214	identity-class indicator-types	level vocabulary certain property values are from the identity-class vocabulary certain property values are from the indicator-types vocabulary	resource-level-ov vocabulary ' <pre>'<pre>'<pre>'<pre>contains a value not in the identity- class-ov vocabulary '<pre>'<pre>contains a value not in the indicator- types-ov vocabulary</pre></pre></pre></pre></pre></pre>
	identity-class	level vocabulary certain property values are from the identity-class vocabulary certain property values are from the indicator-types vocabulary certain property values are	resource-level-ov vocabulary ' <pre>'<pre>'<pre>'<pre>'<pre>contains a value not in the identity- class-ov vocabulary '<pre>'<pre>'<pre>contains a value not in the indicator- types-ov vocabulary '<pre>'<pre>'<pre>contains a</pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre>
214	identity-class indicator-types	level vocabulary certain property values are from the identity-class vocabulary certain property values are from the indicator-types vocabulary certain property values are from the industry-sector	resource-level-ov vocabulary ' <pre>'<pre>'<pre>'<pre>'<pre>contains a value not in the identity- class-ov vocabulary '<pre>'<pre>contains a value not in the indicator- types-ov vocabulary '<pre>'<pre>contains a value not in the industry- </pre></pre></pre></pre></pre></pre></pre></pre></pre>
214	identity-class indicator-types industry-sector	level vocabulary certain property values are from the identity-class vocabulary certain property values are from the indicator-types vocabulary certain property values are from the industry-sector vocabulary	resource-level-ov vocabulary ' <pre>'<pre>'<pre>'<pre>'<pre>contains a value not in the identity- class-ov vocabulary '<pre>contains a value not in the indicator- types-ov vocabulary '<pre>contains a value not in the industry- sector-ov vocabulary </pre></pre></pre></pre></pre></pre></pre>
214	identity-class indicator-types	level vocabulary certain property values are from the identity-class vocabulary certain property values are from the indicator-types vocabulary certain property values are from the industry-sector vocabulary certain property values are	resource-level-ov vocabulary ' <property>' contains a value not in the identity-class-ov vocabulary '<property>' contains a value not in the indicator-types-ov vocabulary '<property>' contains a value not in the industry-sector-ov vocabulary '<property>' contains a '<property>' contains a value not in the industry-sector-ov vocabulary '<property>' contains a</property></property></property></property></property></property>
214	identity-class indicator-types industry-sector	level vocabulary certain property values are from the identity-class vocabulary certain property values are from the indicator-types vocabulary certain property values are from the industry-sector vocabulary certain property values are from the malware-types	resource-level-ov vocabulary ' <property>' contains a value not in the identity-class-ov vocabulary '<property>' contains a value not in the indicator-types-ov vocabulary '<property>' contains a value not in the industry-sector-ov vocabulary '<property>' contains a value not in the industry-sector-ov vocabulary '<property>' contains a value not in the malware-</property></property></property></property></property>
214	identity-class indicator-types industry-sector malware-types	level vocabulary certain property values are from the identity-class vocabulary certain property values are from the indicator-types vocabulary certain property values are from the industry-sector vocabulary certain property values are	resource-level-ov vocabulary ' <property>' contains a value not in the identity-class-ov vocabulary '<property>' contains a value not in the indicator-types-ov vocabulary '<property>' contains a value not in the industry-sector-ov vocabulary '<property>' contains a value not in the industry-sector-ov vocabulary '<property>' contains a value not in the malware-types-ov vocabulary</property></property></property></property></property>
214 215 216	identity-class indicator-types industry-sector	level vocabulary certain property values are from the identity-class vocabulary certain property values are from the indicator-types vocabulary certain property values are from the industry-sector vocabulary certain property values are from the malware-types vocabulary	resource-level-ov vocabulary ' <property>' contains a value not in the identity-class-ov vocabulary '<property>' contains a value not in the indicator-types-ov vocabulary '<property>' contains a value not in the industry-sector-ov vocabulary '<property>' contains a value not in the industry-sector-ov vocabulary '<property>' contains a value not in the malware-</property></property></property></property></property>
214 215 216	identity-class indicator-types industry-sector malware-types	level vocabulary certain property values are from the identity-class vocabulary certain property values are from the indicator-types vocabulary certain property values are from the industry-sector vocabulary certain property values are from the malware-types vocabulary certain property values are from the malware-types vocabulary certain property values are	resource-level-ov vocabulary ' <pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre>'<pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre>
214 215 216	identity-class indicator-types industry-sector malware-types	level vocabulary certain property values are from the identity-class vocabulary certain property values are from the indicator-types vocabulary certain property values are from the industry-sector vocabulary certain property values are from the malware-types vocabulary certain property values are from the malware-types vocabulary certain property values are from the report-types vo-	resource-level-ov vocabulary ' <pre>'<pre>'<pre>'<pre>'<pre>' contains a value not in the identity- class-ov vocabulary '<pre>'<pre>'<pre>'<pre>'<pre>contains a value not in the indicator- types-ov vocabulary '<pre>'<pre>'<pre>'<pre>contains a value not in the industry- sector-ov vocabulary '<pre>'<pre>'<pre>contains a value not in the malware- types-ov vocabulary '<pre>'<pre>contains a value not in the malware- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a</pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre>
214 215 216 218	identity-class indicator-types industry-sector malware-types report-types	level vocabulary certain property values are from the identity-class vocabulary certain property values are from the indicator-types vocabulary certain property values are from the industry-sector vocabulary certain property values are from the malware-types vocabulary certain property values are from the malware-types vocabulary certain property values are from the report-types vocabulary	resource-level-ov vocabulary ' <property>' contains a value not in the identity-class-ov vocabulary '<property>' contains a value not in the indicator-types-ov vocabulary '<property>' contains a value not in the industry-sector-ov vocabulary '<property>' contains a value not in the malware-types-ov vocabulary '<property>' contains a value not in the malware-types-ov vocabulary '<property>' contains a value not in the report-types-ov vocabulary</property></property></property></property></property></property>
214 215 216 218	identity-class indicator-types industry-sector malware-types report-types	level vocabulary certain property values are from the identity-class vocabulary certain property values are from the indicator-types vocabulary certain property values are from the industry-sector vocabulary certain property values are from the malware-types vocabulary certain property values are from the report-types vocabulary certain property values are from the report-types vocabulary certain property values	resource-level-ov vocabulary ' <pre>'<pre>'<pre>'<pre>'<pre>' contains a value not in the identity- class-ov vocabulary '<pre>'<pre>'<pre>'<pre>'<pre>contains a value not in the indicator- types-ov vocabulary '<pre>'<pre>'<pre>'<pre>contains a value not in the industry- sector-ov vocabulary '<pre>'<pre>'<pre>contains a value not in the malware- types-ov vocabulary '<pre>'<pre>contains a value not in the malware- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a value not in the report- types-ov vocabulary '<pre>contains a</pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre>

Table 1 – continued from previous page

		nom previous page	
220	threat-actor-role	certain property values are	' <pre>'<pre>contains a</pre></pre>
		from the threat_actor_role	value not in the threat-
		vocabulary	actor-role-ov vocabulary
221	threat-actor-sophistication	certain property val-	' <pre>'<pre>contains a</pre></pre>
		ues are from the	value not in the threat-
		threat_actor_sophistication	actor-sophistication-ov
		vocabulary	vocabulary
222	tool-types	certain property values are	' <pre>'<pre>contains a</pre></pre>
		from the tool_types vo-	value not in the tool-
		cabulary	types-ov vocabulary
223	region	certain property values are	' <pre>'<pre>contains a</pre></pre>
		from the region vocabu-	value not in the region-ov
		lary	vocabulary
225	grouping-context	certain property values are	' <pre>'<pre>contains a</pre></pre>
		from the grouping-context	value not in the grouping-
		vocabulary	context-ov vocabulary
226	implementation-	certain property values are	' <property>' con-</property>
	languages	from the implementation-	tains a value not in
		languages vocabulary	the implementation-
			languages-ov vocabulary
227	infrastructure-types	certain property values are	' <pre>'<pre>contains</pre></pre>
		from the infrastructure-	a value not in the
		types vocabulary	infrastructure-types-ov
		Ţ	vocabulary
228	malware-capabilities	certain property values	' <pre>'<pre>contains a</pre></pre>
		are from the malware-	value not in the malware-
		capabilities vocabulary	capabilities-ov vocabulary
230	processor-architecture	certain property values	' <pre>'<pre>contains a</pre></pre>
		are from the processor-	value not in the processor-
		architecture vocabulary	architecture-ov vocabu-
		, and the second se	lary
231	malware-result	certain property values are	' <pre>'<pre>contains a</pre></pre>
		from the malware-result	value not in the malware-
		vocabulary	result-ov vocabulary
	I.	•	•

Table 1 – continued from previous page

241			Olaiset (2:3-4:6-5)
241	hash-algo	certain property values are	Object ' <identifier>'</identifier>
		from the hash-algo vocab-	has a 'hashes' dictio-
		ulary	nary with a hash of type
			' <hash_type>', which</hash_type>
			is not a value in the
			hash-algorithm-ov vocab-
			ulary nor a custom value
			prepended with 'x_'.
			Object ' <identifier>'</identifier>
			has an NTFS extension
			with an alternate data
			stream that has a 'hashes'
			dictionary with a hash
			of type ' <hash_type>',</hash_type>
			which is not a value in
			the hash- algorithm-ov
			vocabulary nor a custom
			value prepended with
			'x_'.
			Object ' <identifier>'</identifier>
			has a Windows PE Bi-
			nary File extension with
			a file header hash of
			' <hash_type>', which is</hash_type>
			not a value in the hash-
			algorithm- vocabulary nor
			a custom value prepended
			with 'x_'.
			Object ' <identifier>' has a</identifier>
			Windows PE Binary File
			extension with an optional
			header that has a hash
			of ' <hash_type>', which</hash_type>
			is not a value in the
			hash-algorithm-ov vocab-
			ulary nor a custom value
			prepended with 'x_'.
			Object ' <identifier>' has</identifier>
			a Windows PE Binary
			File extension with a
			section that has a hash
			of ' <hash_type>', which</hash_type>
			is not a value in the
			hash-algorithm-ov vocab-
			ulary nor a custom value
			prepended with 'x_'.
	1		Continued on next page

Table 1 – continued from previous page

Table 1 – continued from previous page				
243	windows-pebinary-type	certain property values are from the windows- pebinary-type vocabulary	Object ' <identifier>' has a Windows PE Binary File extension with a 'pe_type' of '<pe_type>', which is not a value in the windows-pebinary-type-ov vocabulary.</pe_type></identifier>	
244	account-type	certain property values are from the account-type vo-cabulary	Object ' <identifier>'is a User Account Object with an 'account_type' of '<account_type>', which is not a value in the account-type-ov vocabulary.</account_type></identifier>	
245	indicator-pattern-types	certain property values are from the pattern-type vo- cabulary	' <pre>'<pre>'<pre>contains a value not in the pattern- type-ov vocabulary</pre></pre></pre>	
270	all-external-sources	all of the following exter- nal source checks are run		
271	mime-type	file.mime_type is a valid IANA MIME type	The 'mime_type' property of object ' <identifier>' ('<mime_type>') should be an IANA registered MIME Type of the form 'type/subtype'.</mime_type></identifier>	
272	protocols	certain property values are valid IANA Service and Protocol names	The 'protocols' property of object ' <identifier>' contains a value ('<protocol>') not in IANA Service Name and Transport Protocol Port Number Registry.</protocol></identifier>	
273	ipfix	certain property values are valid IANA IP Flow In- formation Export (IPFIX) Entities	The 'ipfix' property of object ' <identifier>' contains a key ('<ipfix>') not in IANA IP Flow Information Export (IPFIX) Entities Registry.</ipfix></identifier>	
274	http-request-headers	certain property values are valid HTTP request header names	The 'request_header' property of object ' <identifier>' contains an invalid HTTP header ('<http_request_header>').</http_request_header></identifier>	
275	socket-options	certain property values are valid socket options	The 'options' property of object ' <identifier>' contains a key ('<option>') that is not a valid socket option (SOIICMPICMP6IIPIPV6I MCASTITCPIRLMP)_*.</option></identifier>	

Table 1 – continued from previous page

		i irom previous page	
276	pdf-doc-info	certain property values are	The 'document_info_dict'
		valid PDF Document In-	property of object ' <iden-< td=""></iden-<>
		formation Dictionary keys	tifier>' contains a key
			(' <key>') that is not a</key>
			valid PDF Document In-
			formation Dictionary key.
277	countries	certain property values	Location 'country' should
		are valid ISO 3166-1	be a valid ISO 3166-1
		ALPHA-2 codes	ALPHA-2 Code.
301	network-traffic-ports	network-traffic objects	The Network Traffic ob-
301	network traine ports	contain both src_port and	ject ' <identifier>' should</identifier>
		dst_port	contain both the 'src_port'
		dst_port	_
202			and 'dst_port' properties.
302	extref-hashes	external references	External reference ' <src>'</src>
		SHOULD have hashes if	has a URL but no hash.
		they have a url	
303	indicator-properties	Indicator objects have	Both the name and
		both name and description	description properties
		properties	SHOULD be present.
304	deprecated-properties	certain properties which	Included property ' <prop-< td=""></prop-<>
		have been deprecated are	erty>' is deprecated
		not being used	within the indicated spec
		not being used	version.
305	extension-description	Extension Definitions	The 'description' property
303	extension-description	1	1
		have a description prop-	SHOULD be populated.
206		erty	
306	extension-properties	Ensure toplevel-property-	For extensions of the
		extensions include the	'toplevel- property-
		extension_properties	extension' type, the
		property	'extension_properties'
			property SHOULD
			include one or more
			property names.
401	extensions-use	custom objects, proper-	Custom object type ' <ob-< td=""></ob-<>
		ties, and observable ex-	ject>' should be imple-
		tensions have been im-	mented using an extension
		plemented with Extension	with an 'extension_type'
		Definitions	of 'new-sdo'.
		Demittons	Custom property ' <prop-< td=""></prop-<>
			erty>' should be 'imple-
			mented using an extension
			with an 'extension_type'
			of 'property- extension' or
			'toplevel-property- exten-
			sion'.
			Custom Cyber Observ-
		i .	
			able Object extension
			type ' <extension>' should</extension>
			type ' <extension>' should be implemented using</extension>
			type ' <extension>' should</extension>

Contributing

We're thrilled that you're interested in contributing to the stix2-validator! 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!

5.1 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-validator.git
```

2. Install develoment-related dependencies and set up git submodules:

```
$ cd cti-stix-validator
$ pip install -r requirements.txt
$ git submodule update --init --recursive
$ git submodule foreach -q --recursive 'git switch $(git config -f $toplevel/.gitmodules submodule.$);
```

3. Install pre-commit git hooks:

```
$ pre-commit install
```

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

5.2 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).

5.3 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 stix2validator/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=stix2validator
$ 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.

5.4 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.

5.5 Updating the STIX JSON schemas

When updates have been made to the STIX JSON schemas repository, the schemas included in this library must also be updated. To do so:

\$ git submodule update --remote

CHAPTER 6

Indices and tables

- genindex
- modindex
- search