
stix2-elevator Documentation

Release 1.0.0

OASIS Open

Mar 29, 2018

Contents:

1	STIX Elevator Log Messages	3
2	Indices and tables	7

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

CHAPTER 1

STIX Elevator Log Messages

Use the following table for reference. You can also enable or disable certain messages using the `-e` or `-d` flags. Refer to the elevator help or README for more information on how to handle logging messages.

Message
Results produced by the stix2-elevator are not for production purposes.
Observable Expressions should not contain placeholders
Placeholder [id] should be resolved
Found definition for [id]
At least one PLACEHOLDER idref was not resolved in [id]
At least one observable could not be converted in [id]
Options not initialized
EMPTY BUNDLE – No objects created from 1.x input document!
Both console and output log have disabled messages.
OSError [message]
silent option is not compatible with a policy
The Short_Description property is no longer supported in STIX. The text was appended to the description property of [id]
Appended [property_name] to description of [id]
Title [title] used for name, appending exploit_target [id] title in description property
Appended confidence property content to description of [id]
Appended Statement type content to description of [id]
Appended Tool type content to description of [id]
Information Source on [id] is not representable in STIX 2.0
Related_Packages type in [id] not supported in STIX 2.0
Campaign/Activity type in [id] not supported in STIX 2.0
Structured COAs type in [id] are not supported in STIX 2.0
ExploitTarget/Weaknesses type in [id] not supported in STIX 2.0
ExploitTarget/Configurations type in [id] not supported in STIX 2.0
Indicator %s has an observable or indicator composite expression which may not supported correctly in STIX 2.0 - please check this p
TTP/Behavior/Exploits/Exploit in [id] not supported in STIX 2.0
Infrastructure in [id] not part of STIX 2.0

Message
Targeted systems on [id] are not a victim target in STIX 2.0
Targeted information on [id] is not a victim target in STIX 2.0
Targeted technical details on [id] are not a victim target in STIX 2.0
Kill Chains type in [id] not supported in STIX 2.0
Victim Target in [id] did not yield any STIX 2.0 object
TTP [id] did not generate any STIX 2.0 object
No STIX 2.0 object generated from embedded object [id]
[object type] did not yield any STIX 2.0 object
The exports property of WinExecutableFileObj is not part of STIX 2.0
The imports property of WinExecutableFileObj is not part of STIX 2.0
Windows Handles are not a part of STIX 2.0
The address type [address] is not part of STIX 2.0
No pattern term was created from [id]
[id] is used as a pattern, therefore it is not included as an onobserved_data instance
[xxx] content is not supported in STIX 2.0
Could not resolve Marking Structure [id]
MAEC content in [id] cannot be represented in STIX 2.0
NO MESSAGE ASSIGNED
Only one person name allowed for [id] in STIX 2.0, used first one
Only one organization name allowed for [id] in STIX 2.0, used first one
YARA/SNORT patterns on [id] not supported in STIX 2.0
NO MESSAGE ASSIGNED
Only one alternative test mechanism allowed for [id] in STIX 2.0 - used first one, which was [pattern_lang]
Only one valid time window allowed for [id] in STIX 2.0 - used first one
Only one name for malware is allowed for [id] in STIX 2.0 - used first one
No STIX 1.x vocab value given for [property], using 'unknown'
Only one [property] allowed in STIX 2.0 - used first one
File size window not allowed in top level observable, using first value
Only one Layer7_Connections/HTTP_Request_Response used for http-request-ext, using first value
Dangling source reference [source] in [id]
Dangling target reference [target] in [id]
1.X ID: {0} was not mapped to STIX 2.0 ID
Unable to determine the STIX 2.0 type for [id]
Malformed id [id]. Generated a new uuid
Identity [id] has organization and person names
Dangling kill chain phase id in indicator [id]
windows-registry-key is required to have a key property
[condition] was used, but two values were not provided.
Trying to associate [old_key] with None
Could not associate [old_id] with None
Identity [id] must have a name, using 'None'
No WinExecutableFile properties found in [WinExeFile]
No ArchiveFile properties found in [ArchiveFile]
No WinProcess properties found in [WinProcess]
No WinService properties found in [WinService]
The custom property name [property name] does not adhere to the specification rules
No ISO code for [value] in [identifying info]
No start time for the first valid time interval is available in %s, other time intervals might be more appropriate
Unable to create a pattern from a File object

Message
[stix 1.x property] contains no value
No term was yielded for %s
Hive property, %s, is already a prefix of the key property, %s
The custom property name %s contains whitespace, replacing it with underscores
Found duplicate marking structure [id]
'[hash_string]' is not a valid [hash_type] hash
Threat Actor identity [id] being used as basis of attributed-to relationship
Found STIX 1.X ID: [old_id] replaced by [new_id]
[old_id] is already associated other ids: [tuple_of_new_ids]
Including rel["id"] in rep["id"] and added the target_ref rel["target_ref"] to the report
Including rel["id"] in rep["id"] and added the source_ref rel["source_ref"] to the report
Including rel["id"] in rep["id"] although the target_ref is unknown
Including rel["id"] in rep["id"] although the source_ref is unknown
Not including rel["id"] in rep["id"] because there is no corresponding SDO for rel["target_ref"]
Not including rel["id"] in rep["id"] because there is no corresponding SDO for rel["source_ref"]
All associated [xxx] relationships of [id] are assumed to not represent STIX 1.2 versioning
ciq name found in [id], possibly overriding other name
Only one type pattern can be specified in [id] - using cybox
[id] generated an identity associated with a victim
No condition given for [current_observable] - assume '='
Used MATCHES operator for [condition]
Based on CIQ information, [id] is assumed to be an organization
Threat actor [id] title is used for name property
Using related-to for the [xxx] of [id]
Using first Threat Actor motivation as primary_motivation. If more, as secondary_motivation
Could not resolve Marking Structure [id]
1.x full file paths are not processed, yet
process:startup_info not handled yet
WinServiceObject.service_dll is not handled, yet.
CybOX object [object] not handled yet
Email [property] not handled yet
<i>file:extended_properties:windows_pebinary_ext:optional_header</i> is not implemented yet
[object] found in [id] cannot be converted to a pattern, yet.
Related Objects of cyber observables for [id] are not handled yet
Negation of [id] is not handled yet
Network Connection not implemented, yet.
Condition on a hive property not handled.
Cannot convert CybOX 2.x class name [name] to an object_path_root_name
Parameter Observables in [id] are not handled, yet.
[xxx] in [id] are not handled, yet.
Ambiguous file path '%s' was not processed
'first_observed' and 'last_observed' data not available directly on {id} - using timestamp
Using parent object timestamp on [identifying info]
No valid time position information available in [id], using parent timestamp
No 'first_seen' data on [id] - using timestamp
Timestamp not available for [entity], using current time

CHAPTER 2

Indices and tables

- `genindex`
- `modindex`
- `search`