MISP-STIX

The Holy Grail for MISP and STIX formats

MISP core team - Christian Studer

TLP:WHITE

MISP Project
https://www.misp-project.org/

CTI Summit (CTIS-2022)

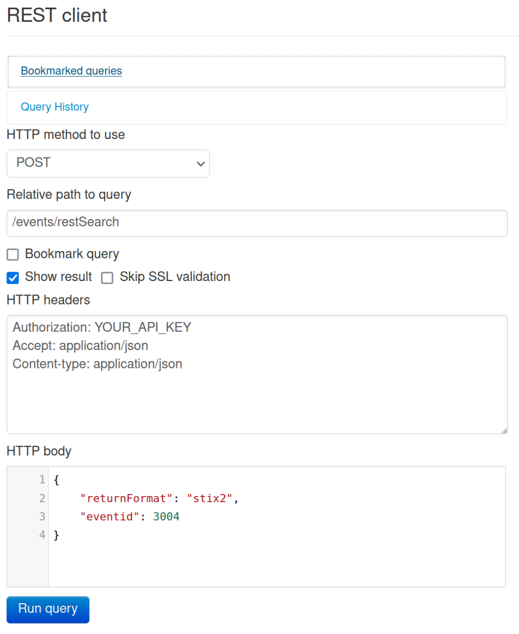
Summary

- Past & current status
- Recent changes
- Continuous improvement & future roadmap
- Challenges we face
- Evolution perspectives
- Demo (?)

MISP & STIX

- **Built-in integration**
- Export & Import features
  - Export MISP Events collections
  - Import STIX files
- Supported version
  - STIX 1.1.1
  - STIX 2.0
- Accessible via restSearch

STIX conversion usage in MISP



REST client

Bookmarked queries

Query History

HTTP method to use

POST

Relative path to query

/events/restSearch

□ Bookmark query

☑ Show result □ Skip SSL validation

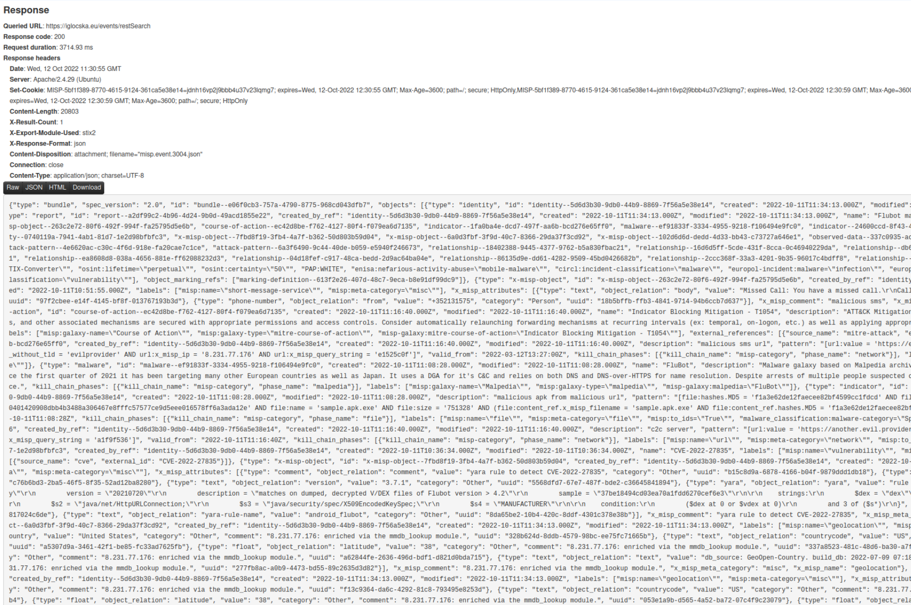
HTTP headers

```
Authorization: YOUR_API_KEY
Accept: application/json
Content-type: application/json
```

HTTP body

```
{
    "returnFormat": "stix2",
    "eventid": 3004
}
```

STIX conversion usage in MISP

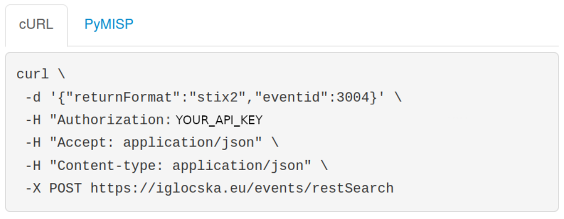


Response

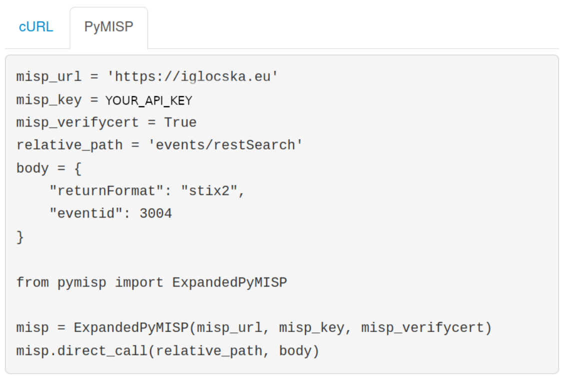
Queried URL: https://iglocska.eu/events/restSearch
Response code: 200
Request duration: 3714.93 ms
Response headers
Date: Wed, 12 Oct 2022 11:30:55 GMT
Server: Apache/2.4.29 (Ubuntu)
Set-Cookie: MISP-5bf1f389-8770-4615-9124-361ca5e38e14=jdnh16vp2j9bbb4u37v23lqmg7; expires=Wed, 12-Oct-2022 12:30:55 GMT; Max-Age=3600; path=/; secure; HttpOnly,MISP-5bf1f389-8770-4615-9124-361ca5e38e14=jdnh16vp2j9bbb4u37v23lqmg7; expires=Wed, 12-Oct-2022 12:30:59 GMT; Max-Age=3600
expires=Wed, 12-Oct-2022 12:30:59 GMT; Max-Age=3600; path=/; secure; HttpOnly
Content-Length: 20803
X-Result-Count: 1
X-Export-Module-Used: stix2
X-Response-Format: json
Content-Disposition: attachment; filename="misp.event.3004.json"
Connection: close
Content-Type: application/json; charset=UTF-8

```
{"type": "bundle", "spec_version": "2.0", "id": "bundle--e06f0cb3-757a-4790-8775-968cd043dfb7", "objects": [{"type": "identity", "id": "identity--5d6d3b30-9db0-44b9-8869-7f56a5e38e14", "created": "2022-10-11T11:34:13.000Z", "modified":
ype": "report", "id": "report--a2df99c2-4b96-4d24-9b0d-49acd1855e22", "created_by_ref": "identity--5d6d3b30-9db0-44b9-8869-7f56a5e38e14", "created": "2022-10-11T11:34:13.000Z", "modified": "2022-10-11T11:34:13.000Z", "name": "Flubot ma
sp-object--263c2e72-80f6-492f-994f-fa25795d5e6b", "course-of-action--ec42d8be-f762-4127-80f4-f079ea6d7135", "indicator--1fa0ba4e-dcd7-497f-aa6b-bcd276e65ff0", "malware--ef91833f-3334-4955-9218-f106494e9fc0", "indicator--24600ccd-8f43-4
ty--0740119a-7941-4ab1-81d7-1e2d98bfbfc3", "x-misp-object--7fbd8f19-3fb4-4a7f-b362-50d803b59d04", "x-misp-object--6a0d3fbf-3f9d-40c7-8366-29da37f3cd92", "x-misp-object--102d6d6d-dedd-4d33-bb43-c73727a646e1", "observed-data--337c0935-ac
tack-pattern--4e6620ac-c30c-4f6d-918e-fa20cae7c1ce", "attack-pattern--6a3f6490-9c44-40de-b059-e5940f246673", "relationship--18402388-9445-4377-9762-b5a830fbac21", "relationship--16d6d5ff-5cde-431f-8cca-0c46940229da", "relationship--db6
1", "relationship--ea8608d8-038a-4656-881e-ff62088232d3", "relationship--04d18fef-c917-48ca-bedd-2d9ac64ba04e", "relationship--86135d9e-dd61-4282-9509-45bd0426682b", "relationship--2ccc368f-33a3-4201-9b35-96017c4bdff8", "relationship--
TIX-Converter\"", "osint:lifetime=\"perpetual\"", "osint:certainty=\"50\"", "PAP:WHITE", "enisa:nefarious-activity-abuse=\"mobile-malware\"", "circl:incident-classification=\"malware\"", "europol-incident:malware=\"infection\"", "europ
lassification=\"vulnerability\""], "object_marking_refs": ["marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"]}, {"type": "x-misp-object", "id": "x-misp-object--263c2e72-80f6-492f-994f-fa25795d5e6b", "created_by_ref": "identity
ed": "2022-10-11T10:51:55.000Z", "labels": ["misp:name=\"short-message-service\"", "misp:meta-category=\"misc\""], "x_misp_attributes": [{"type": "text", "object_relation": "body", "value": "Missed Call: You have a missed call.\r\nCall
uuid": "97f2cbee-e14f-4145-bf8f-013767193b3d"}, {"type": "phone-number", "object_relation": "from", "value": "+352131575", "category": "Person", "uuid": "18b5bffb-ffb3-4841-9714-94b6ccb7d637"}], "x_misp_comment": "malicious sms", "x_mi
-action", "id": "course-of-action--ec42d8be-f762-4127-80f4-f079ea6d7135", "created": "2022-10-11T11:16:40.000Z", "modified": "2022-10-11T11:16:40.000Z", "name": "Indicator Blocking Mitigation - T1054", "description": "ATT&CK Mitigation
s, and other associated mechanisms are secured with appropriate permissions and access controls. Consider automatically relaunching forwarding mechanisms at recurring intervals (ex: temporal, on-logon, etc.) as well as applying appropr
bels": ["misp:galaxy-name=\"Course of Action\"", "misp:galaxy-type=\"mitre-course-of-action\"", "misp-galaxy:mitre-course-of-action=\"Indicator Blocking Mitigation - T1054\""], "external_references": [{"source_name": "mitre-attack", "e
b-bcd276e65ff0", "created_by_ref": "identity--5d6d3b30-9db0-44b9-8869-7f56a5e38e14", "created": "2022-10-11T11:16:40.000Z", "modified": "2022-10-11T11:16:40.000Z", "description": "malicious sms url", "pattern": "[url:value = 'https://e
_without_tld = 'evilprovider' AND url:x_misp_ip = '8.231.77.176' AND url:x_misp_query_string = 'e1525c0f']", "valid_from": "2022-03-12T13:27:00Z", "kill_chain_phases": [{"kill_chain_name": "misp-category", "phase_name": "network"}], "l
e\""]}, {"type": "malware", "id": "malware--ef91833f-3334-4955-9218-f106494e9fc0", "created": "2022-10-11T11:08:28.000Z", "modified": "2022-10-11T11:08:28.000Z", "name": "FluBot", "description": "Malware galaxy based on Malpedia archiv
ce the first quarter of 2021 it has been targeting many other European countries as well as Japan. It uses a DGA for it's C&C and relies on both DNS and DNS-over-HTTPS for name resolution. Despite arrests of multiple people suspected o
ce.", "kill_chain_phases": [{"kill_chain_name": "misp-category", "phase_name": "malpedia"}], "labels": ["misp:galaxy-name=\"Malpedia\"", "misp:galaxy-type=\"malpedia\"", "misp-galaxy:malpedia=\"FluBot\""]}, {"type": "indicator", "id":
0-9db0-44b9-8869-7f56a5e38e14", "created": "2022-10-11T11:08:28.000Z", "modified": "2022-10-11T11:08:28.000Z", "description": "malicious apk from malicious url", "pattern": "[file:hashes.MD5 = 'f1a3e62de12faecee82bf4599cc1fdcd' AND fil
0401420908dbb4b3488a306467e8fffc57577ce9d5eee016578ff6a3ada12e' AND file:name = 'sample.apk.exe' AND file:size = '751328' AND (file:content_ref.x_misp_filename = 'sample.apk.exe' AND file:content_ref.hashes.MD5 = 'f1a3e62de12faecee82bf
-10-11T11:08:28Z", "kill_chain_phases": [{"kill_chain_name": "misp-category", "phase_name": "file"}], "labels": ["misp:name=\"file\"", "misp:meta-category=\"file\"", "misp:to_ids=\"True\"", "malware_classification:malware-category=\"Sp
6", "created_by_ref": "identity--5d6d3b30-9db0-44b9-8869-7f56a5e38e14", "created": "2022-10-11T11:16:40.000Z", "modified": "2022-10-11T11:16:40.000Z", "description": "c2c server", "pattern": "[url:value = 'https://another.evil.provider
x_misp_query_string = 'a1f9f536']", "valid_from": "2022-10-11T11:16:40Z", "kill_chain_phases": [{"kill_chain_name": "misp-category", "phase_name": "network"}], "labels": ["misp:name=\"url\"", "misp:meta-category=\"network\"", "misp:to_
7-1e2d98bfbfc3", "created_by_ref": "identity--5d6d3b30-9db0-44b9-8869-7f56a5e38e14", "created": "2022-10-11T10:36:34.000Z", "modified": "2022-10-11T10:36:34.000Z", "name": "CVE-2022-27835", "labels": ["misp:name=\"vulnerability\"", "mi
[{"source_name": "cve", "external_id": "CVE-2022-27835"}]}, {"type": "x-misp-object", "id": "x-misp-object--7fbd8f19-3fb4-4a7f-b362-50d803b59d04", "created_by_ref": "identity--5d6d3b30-9db0-44b9-8869-7f56a5e38e14", "created": "2022-10-
a\"", "misp:meta-category=\"misc\""], "x_misp_attributes": [{"type": "comment", "object_relation": "comment", "value": "yara rule to detect CVE-2022-27835", "category": "Other", "uuid": "b15c8d9a-6878-4166-b04f-9879ddd1db18"}, {"type":
"c76b6bd3-2ba5-46f5-8f35-52ad12ba8280"}, {"type": "text", "object_relation": "version", "value": "3.7.1", "category": "Other", "uuid": "5568dfd7-67e7-487f-bde2-c36645841894"}, {"type": "yara", "object_relation": "yara", "value": "rule
y\"\r\n        version = \"20210720\"\r\n        description = \"matches on dumped, decrypted V/DEX files of Flubot version > 4.2\"\r\n        sample = \"37be18494cd03ea70a1fdd6270cef6e3\"\r\n\r\n    strings:\r\n        $dex = \"dex\"\
r\n        $s2 = \"java/net/HttpURLConnection;\"\r\n        $s3 = \"java/security/spec/X509EncodedKeySpec;\"\r\n        $s4 = \"MANUFACTURER\"\r\n\r\n    condition:\r\n        ($dex at 0 or $vdex at 0)\r\n        and 3 of ($s*)\r\n}",
817024c6de"}, {"type": "text", "object_relation": "yara-rule-name", "value": "android_flubot", "category": "Other", "uuid": "8da65be2-10b4-420c-8ddf-4301c378e38b"}], "x_misp_comment": "yara rule to detect CVE-2022-27835", "x_misp_meta_
ct--6a0d3fbf-3f9d-40c7-8366-29da37f3cd92", "created_by_ref": "identity--5d6d3b30-9db0-44b9-8869-7f56a5e38e14", "created": "2022-10-11T11:34:13.000Z", "modified": "2022-10-11T11:34:13.000Z", "labels": ["misp:name=\"geolocation\"", "misp
ountry", "value": "United States", "category": "Other", "comment": "8.231.77.176: enriched via the mmdb_lookup module.", "uuid": "328b624d-8ddb-4579-98bc-ee75fc71665b"}, {"type": "text", "object_relation": "countrycode", "value": "US",
"uuid": "a5307d9a-3461-42f1-be85-fc33ad7625fb"}, {"type": "float", "object_relation": "latitude", "value": "38", "category": "Other", "comment": "8.231.77.176: enriched via the mmdb_lookup module.", "uuid": "337a8523-481c-48d6-ba30-a7f
y": "Other", "comment": "8.231.77.176: enriched via the mmdb_lookup module.", "uuid": "a62844fe-2636-496d-bdf1-d821d0bda715"}, {"type": "text", "object_relation": "text", "value": "db_source: GeoOpen-Country. build_db: 2022-07-09 07:18
31.77.176: enriched via the mmdb_lookup module.", "uuid": "277fb8ac-a0b9-4473-bd55-89c2635d3d82"}], "x_misp_comment": "8.231.77.176: enriched via the mmdb_lookup module.", "x_misp_meta_category": "misc", "x_misp_name": "geolocation"},
"created_by_ref": "identity--5d6d3b30-9db0-44b9-8869-7f56a5e38e14", "created": "2022-10-11T11:34:13.000Z", "modified": "2022-10-11T11:34:13.000Z", "labels": ["misp:name=\"geolocation\"", "misp:meta-category=\"misc\""], "x_misp_attribut
y": "Other", "comment": "8.231.77.176: enriched via the mmdb_lookup module.", "uuid": "f13c9364-da6c-4292-81c8-793495e8253d"}, {"type": "text", "object_relation": "countrycode", "value": "US", "category": "Other", "comment": "8.231.77.
b4"}, {"type": "float", "object_relation": "latitude", "value": "38", "category": "Other", "comment": "8.231.77.176: enriched via the mmdb_lookup module.", "uuid": "053e1a9b-d565-4a52-ba72-07c4f9c23079"}, {"type": "float", "object_rela
```

STIX CONVERSION USAGE IN MISP



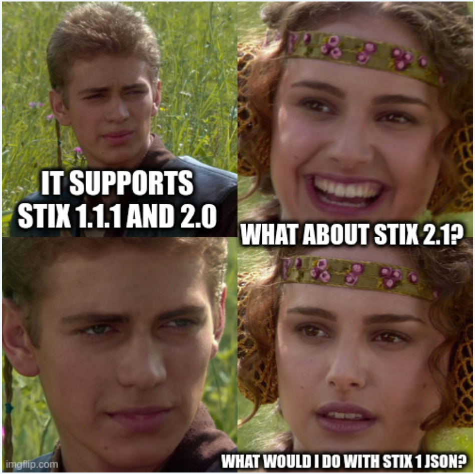
```
curl \
 -d '{"returnFormat":"stix2","eventid":3004}' \
 -H "Authorization: YOUR_API_KEY
 -H "Accept: application/json" \
 -H "Content-type: application/json" \
 -X POST https://iglocska.eu/events/restSearch
```



```
misp_url = 'https://iglocska.eu'
misp_key = YOUR_API_KEY
misp_verifycert = True
relative_path = 'events/restSearch'
body = {
    "returnFormat": "stix2",
    "eventid": 3004
}

from pymisp import ExpandedPyMISP

misp = ExpandedPyMISP(misp_url, misp_key, misp_verifycert)
misp.direct_call(relative_path, body)
```

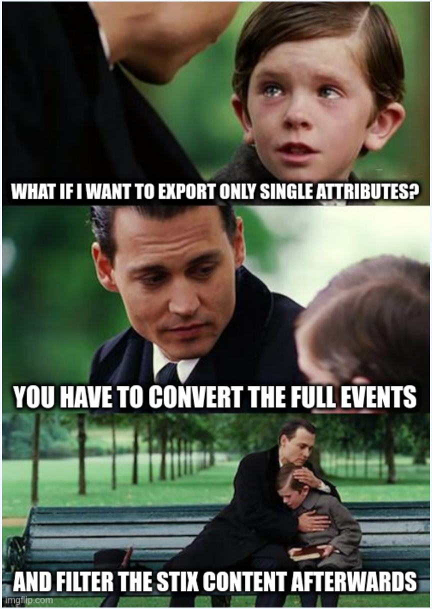
Former feature limitations

- **Supported versions**
  - 1.1.1 XML (& JSON)
  - 2.0
- Data type support


IT SUPPORTS STIX 1.1.1 AND 2.0
WHAT ABOUT STIX 2.1?
WHAT WOULD I DO WITH STIX 1 JSON?
imgflip.com

Former feature limitations

- Supported versions
  - 1.1.1 XML (& JSON)
  - 2.0
- **Data type support**


WHAT IF I WANT TO EXPORT ONLY SINGLE ATTRIBUTES?
YOU HAVE TO CONVERT THE FULL EVENTS
AND FILTER THE STIX CONTENT AFTERWARDS
imgflip.com

Former practical & Organisational limitations

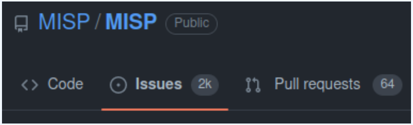
- Export and import features only available via MISP
    - Need an automation key (and/or to deal with the UI)

- **Github**: STIX issues lost within the MISP core issues

Former practical & Organisational limitations

- Export and import features only available via MISP
  - Need an automation key (and/or to deal with the UI)

- **Github**: STIX issues lost within the MISP core issues



The solution

Key features

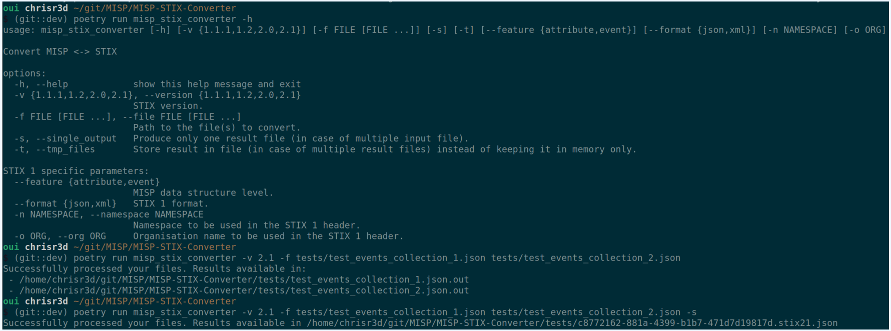
- Support all the STIX versions
  - **STIX 2.1 Support**
  - 1.1.1, 1.2, 2.0 Support enhanced
- Various MISP data collection supported
- **Mapping documentation**

Handling the conversion with a python library

- Used in MISP built-in export modules
- Enable a **stand-alone** use of the python code[1]
  - Pass filenames & get the converted content written in 1 or more result file(s)
- Possible integration within python code
  - Give it a list of filenames
  - MISP standard format <-> STIX
    - JSON or PyMISP

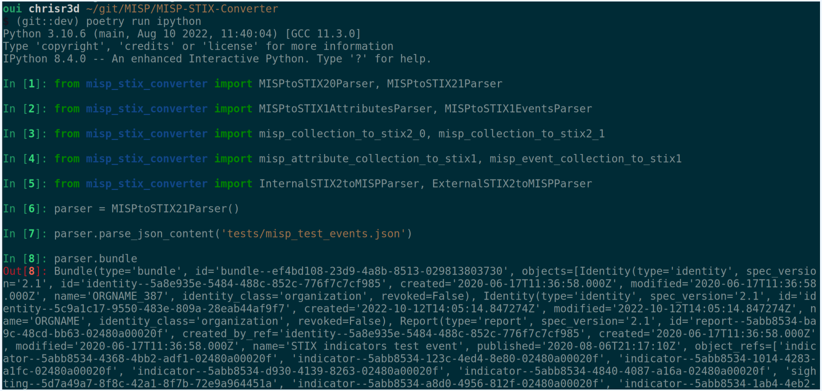
[1] i.e command line

Library usage - Command line



```
oui chrisr3d ~/git/MISP/MISP-STIX-Converter
$ (git::dev) poetry run misp_stix_converter -h
usage: misp_stix_converter [-h] [-v {1.1.1,1.2,2.0,2.1}] [-f FILE [FILE ...]] [-s] [-t] [--feature {attribute,event}] [--format {json,xml}] [-n NAMESPACE] [-o ORG]

Convert MISP <-> STIX

options:
  -h, --help            show this help message and exit
  -v {1.1.1,1.2,2.0,2.1}, --version {1.1.1,1.2,2.0,2.1}
                        STIX version.
  -f FILE [FILE ...], --file FILE [FILE ...]
                        Path to the file(s) to convert.
  -s, --single_output   Produce only one result file (in case of multiple input file).
  -t, --tmp_files       Store result in file (in case of multiple result files) instead of keeping it in memory only.

STIX 1 specific parameters:
  --feature {attribute,event}
                        MISP data structure level.
  --format {json,xml}   STIX 1 format.
  -n NAMESPACE, --namespace NAMESPACE
                        Namespace to be used in the STIX 1 header.
  -o ORG, --org ORG     Organisation name to be used in the STIX 1 header.
oui chrisr3d ~/git/MISP/MISP-STIX-Converter
$ (git::dev) poetry run misp_stix_converter -v 2.1 -f tests/test_events_collection_1.json tests/test_events_collection_2.json
Successfully processed your files. Results available in:
 - /home/chrisr3d/git/MISP/MISP-STIX-Converter/tests/test_events_collection_1.json.out
 - /home/chrisr3d/git/MISP/MISP-STIX-Converter/tests/test_events_collection_2.json.out
oui chrisr3d ~/git/MISP/MISP-STIX-Converter
$ (git::dev) poetry run misp_stix_converter -v 2.1 -f tests/test_events_collection_1.json tests/test_events_collection_2.json -s
Successfully processed your files. Results available in /home/chrisr3d/git/MISP/MISP-STIX-Converter/tests/c8772162-881a-4399-b1b7-471d7d19817d.stix21.json
```

Library usage - Python integration

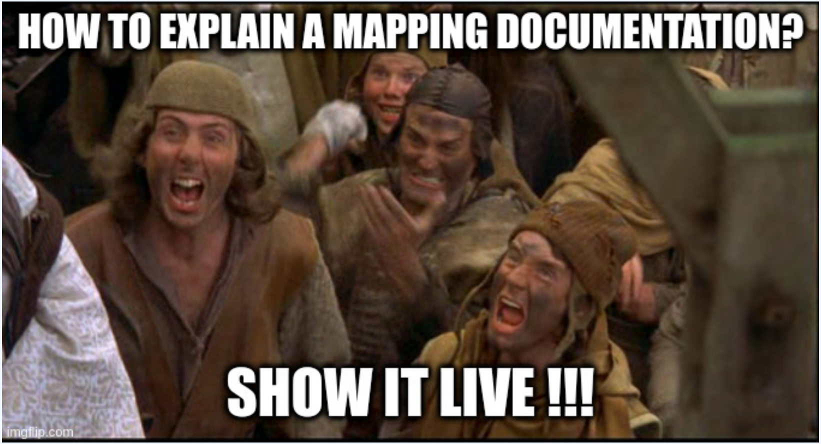


```
oui chrisr3d ~/git/MISP/MISP-STIX-Converter
$ (git::dev) poetry run ipython
Python 3.10.6 (main, Aug 10 2022, 11:40:04) [GCC 11.3.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 8.4.0 -- An enhanced Interactive Python. Type '?' for help.

In [1]: from misp_stix_converter import MISPtoSTIX20Parser, MISPtoSTIX21Parser

In [2]: from misp_stix_converter import MISPtoSTIX1AttributesParser, MISPtoSTIX1EventsParser

In [3]: from misp_stix_converter import misp_collection_to_stix2_0, misp_collection_to_stix2_1

In [4]: from misp_stix_converter import misp_attribute_collection_to_stix1, misp_event_collection_to_stix1

In [5]: from misp_stix_converter import InternalSTIX2toMISPParser, ExternalSTIX2toMISPParser

In [6]: parser = MISPtoSTIX21Parser()

In [7]: parser.parse_json_content('tests/misp_test_events.json')

In [8]: parser.bundle
Out[8]: Bundle(type='bundle', id='bundle--ef4bd108-23d9-4a8b-8513-029813803730', objects=[Identity(type='identity', spec_versio
n='2.1', id='identity--5a8e935e-5484-488c-852c-776f7c7cf985', created='2020-06-17T11:36:58.000Z', modified='2020-06-17T11:36:58
.000Z', name='ORGNAME_387', identity_class='organization', revoked=False), Identity(type='identity', spec_version='2.1', id='id
entity--5c9a1c17-9550-483e-809a-28eab44af9f7', created='2022-10-12T14:05:14.847274Z', modified='2022-10-12T14:05:14.847274Z', n
ame='ORGNAME', identity_class='organization', revoked=False), Report(type='report', spec_version='2.1', id='report--5abb8534-ba
9c-48cd-bb63-02480a00020f', created_by_ref='identity--5a8e935e-5484-488c-852c-776f7c7cf985', created='2020-06-17T11:36:58.000Z'
, modified='2020-06-17T11:36:58.000Z', name='STIX indicators test event', published='2020-08-06T21:17:10Z', object_refs=['indic
ator--5abb8534-4368-4bb2-adf1-02480a00020f', 'indicator--5abb8534-123c-4ed4-8e80-02480a00020f', 'indicator--5abb8534-1014-4283-
a1fc-02480a00020f', 'indicator--5abb8534-d930-4139-8263-02480a00020f', 'indicator--5abb8534-4840-4087-a16a-02480a00020f', 'sigh
ting--5d7a49a7-8f8c-42a1-8f7b-72e9a964451a', 'indicator--5abb8534-a8d0-4956-812f-02480a00020f', 'indicator--5abb8534-1ab4-4eb2-
```

Mapping documentation

- Mapping overview
  - Quick overview on how MISP data structures are mapped with STIX objects
- Detailed mapping
  - Extended explanation on how each granular data is mapped with STIX objects fields

Mapping explained



Work in Progress & Continuous development

- **STIX 2 -> MISP import feature**

- Current mapping improvement
  - Support for Custom Galaxy clusters
  - Better support of existing STIX objects libraries[2]
  - Support custom STIX format[3]

[2] e.g: `https://github.com/mitre/cti`

[3] e.g: ACS custom markings

Work in Progress & Continuous development

- **STIX 2 -> MISP import feature**
- Current mapping improvement
  - Support for Custom Galaxy clusters
  - Better support of existing STIX objects libraries[2]
  - Support custom STIX format[3]
- **TAXII integration**

[2] e.g: `https://github.com/mitre/cti`

[3] e.g: ACS custom markings

What comes next?

- Extend the export feature to any kind of data collection

- Add notes on any data structure
- Sightings on context layers

- Port the STIX 1 -> MISP import feature

Handling different STIX content creation designs

- Impossible to control the content created by external parties
- We want to keep UUIDs

Handling different STIX content creation designs

- Impossible to control the content created by external parties
- We want to keep UUIDs

- Facing UUIDs validation issues
  - Loading error

An easy fix: a STIX 2 python library fork[4]

- No change on the content validation
  - Differs only on the UUIDs validation process
- MISP has now the same UUIDs requirements
  - We keep a reference to the initial UUID
  - A UUID v5 is generated

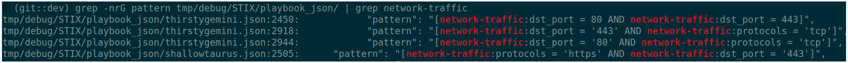
[4] https://github.com/MISP/cti-python-stix2 & https://pypi.org/project/misp-lib-stix2/

Minding the gap between formats

- From a sharing platform to an threat intelligence exchange format
  - Custom STIX objects
  - Custom fields in existing objects
  - STIX extensions
- Handling the infinite possibilities of a patterning language
  - Importing STIX 2 patterns in separate MISP objects

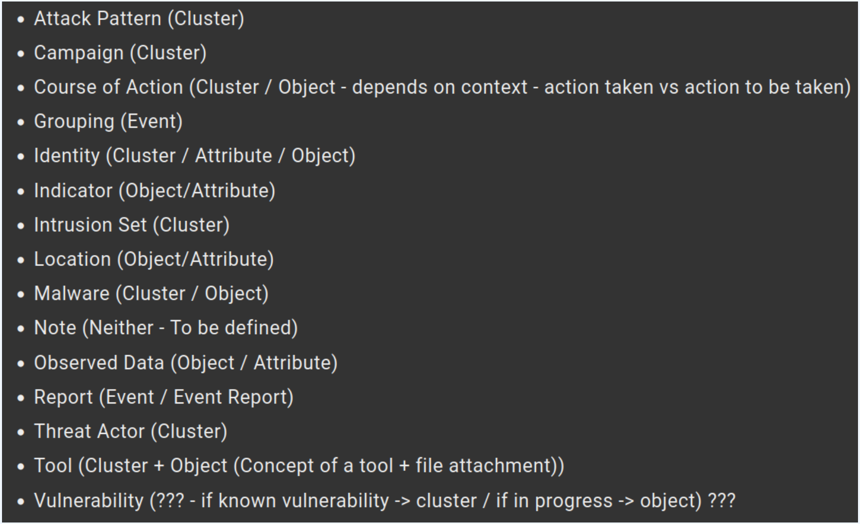
Minding the gap between formats

- From a sharing platform to an threat intelligence exchange format
    - Custom STIX objects
    - Custom fields in existing objects
    - STIX extensions
- Handling the infinite possibilities of a patterning language
    - Importing STIX 2 patterns in separate MISP objects



```
$ (git::dev) grep -nrG pattern tmp/debug/STIX/playbook_json/ | grep network-traffic
tmp/debug/STIX/playbook_json/thirstygemini.json:2450:           "pattern": "[network-traffic:dst_port = 80 AND network-traffic:dst_port = 443]",
tmp/debug/STIX/playbook_json/thirstygemini.json:2918:           "pattern": "[network-traffic:dst_port = '443' AND network-traffic:protocols = 'tcp']",
tmp/debug/STIX/playbook_json/thirstygemini.json:2944:           "pattern": "[network-traffic:dst_port = '80' AND network-traffic:protocols = 'tcp']",
tmp/debug/STIX/playbook_json/shallowtaurus.json:2505:       "pattern": "[network-traffic:protocols = 'https' AND network-traffic:dst_port = '443']",
```

Mapping challenges



- Attack Pattern (Cluster)
- Campaign (Cluster)
- Course of Action (Cluster / Object - depends on context - action taken vs action to be taken)
- Grouping (Event)
- Identity (Cluster / Attribute / Object)
- Indicator (Object/Attribute)
- Intrusion Set (Cluster)
- Location (Object/Attribute)
- Malware (Cluster / Object)
- Note (Neither - To be defined)
- Observed Data (Object / Attribute)
- Report (Event / Event Report)
- Threat Actor (Cluster)
- Tool (Cluster + Object (Concept of a tool + file attachment))
- Vulnerability (??? - if known vulnerability -> cluster / if in progress -> object) ???

Evolution perspectives

OASIS OPEN

- Members of the Oasis CTI TC
  - Our involvement
    - Participating to the development process
  - Our proposal: Go for the open source way
    - Make the contribution process more accessible
      => Bring more contributers / contributions
    - Easier access to the resources
      => More visibility

How to report bugs/issues

- Github issues
  - **`https://github.com/MISP/misp-stix/issues`**
  - `https://github.com/MISP/MISP/issues`
- Please provide details
  - How did the issue happen
  - **Recommendation**: provide samples
- Any feedback welcome

Useful links

- https://github.com/MISP/misp-stix
- https://github.com/MISP/misp-stix/tree/main/documentation

- https://github.com/MISP
- https://www.misp-project.org/
- https://twitter.com/MISPProject
- https://twitter.com/chrisred_68

Demo time