

# 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)



- Past & current status
- Recent changes
- Continuous improvement & future roadmap
- Organisational & philosophical aspects
- Demo (?)

- **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

```
1 {  
2   "returnFormat": "stix2",  
3   "eventId": 3004  
4 }
```

Run query

## STIX CONVERSION USAGE IN MISP

### Response

Queried URL: <https://gloska.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.5bf1389-8770-4615-9124-361ca5e38e14-idm16vc29bb4437v23jmo7; expires=Wed, 12-Oct-2022 12:30:55 GMT; Max-Age=3600; path=/; secure; HttpOnly MISP.5bf1389-8770-4615-9124-361ca5e38e14-idm16vc29bb4437v23jmo7; expires=Wed, 12-Oct-2022 12:30:55 GMT; Max-Age=3600

expires=Wed, 12-Oct-2022 12:30:59 GMT; Max-Age=3600; path=/; secure; HttpOnly

Content-Length: 20903

X.Result.Count: 1

X-Export-Module-Used: stx2

X-Response-Format: json

Content-Disposition

Connection: close

Content-Type: application/json; c

[illegible]

# STIX CONVERSION USAGE IN MISP

cURL

PyMISP

```
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
```

cURL

PyMISP

```
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**



# FORMER FEATURE LIMITATIONS

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

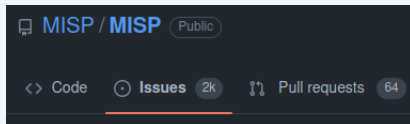




- Export and import features only available via MISP
  - ▶ Need an automation key (and/or to deal with the UI)
- **Github:** STIX issues lost within the MISP core issues

# 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



- 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**

- Used in MISP built-in export modules
- Enable a **stand-alone** use of the python code<sup>1</sup>
  - ▶ 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

---

<sup>1</sup>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 chris3d ~/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 version='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='identity--5c9a1c17-9550-483e-809a-28eab44af9f7', created='2022-10-12T14:05:14.847274Z', modified='2022-10-12T14:05:14.847274Z', name='ORGNAME', identity class='organization', revoked=False), Report(type='report', spec version='2.1', id='report--5abb8534-ba9c-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=['indicator--5abb8534-4368-4bb2-adf1-02480a00020f', 'indicator--5abb8534-123c-4ed4-8e80-02480a00020f', 'indicator--5abb8534-1014-4283-alfc-02480a00020f', 'indicator--5abb8534-d930-4139-8263-02480a00020f', 'indicator--5abb8534-4840-4087-a16a-02480a00020f', 'sighting--5d7a49a7-8f8c-42a1-8f7b-72e9a964451a', 'indicator--5abb8534-a8d0-4956-812f-02480a00020f', 'indicator--5abb8534-1ab4-4eb2-
```

## ■ 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



- **STIX 2 -> MISP import feature**
- New MISP object templates & Galaxy clusters
- Better support for Custom Galaxy clusters

- **STIX 2 -> MISP import feature**
- New MISP object templates & Galaxy clusters
- Better support for Custom Galaxy clusters

- **TAXII integration**



- Better support of existing STIX objects libraries<sup>2</sup>
- Support custom STIX format<sup>3</sup>
- Mapping improvement
  - ▶ MISP object templates -> STIX
  - ▶ Improve the STIX 2 patterns & Observable objects -> MISP

---

<sup>2</sup><https://github.com/mitre/cti>

<sup>3</sup>Especially while importing STIX data, **and as long as we can implement support of well defined versions**

# 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

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

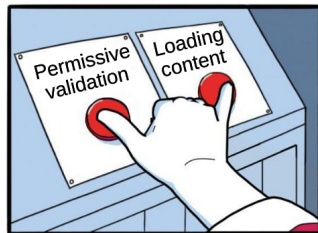
# HANDLING DIFFERENT STIX CONTENT CREATION DESIGNS

- 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<sup>4</sup>

- 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



<sup>4</sup><https://github.com/MISP/cti-python-stix2> &  
<https://pypi.org/project/misp-lib-stix2/>

- 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:2459:      "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:2585:      "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) ???



- 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 contributors / 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

- <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](https://twitter.com/chrisred_68)

