MISP-STIX Project

Python library to convert MISP <-> STIX

MISP core team

TLP:WHITE

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

MISP Training

MISP & STIX

- **Built-in integration**
  - Available from the UI
  - Accessible via restSearch
- Export & Import features
  - Export MISP data collections
  - Import STIX files
- Supported version
  - STIX 1.1.1 & 1.2
  - STIX 2.0 & 2.1

misp-stix - Key features

- MISP $\Longleftrightarrow$ STIX conversion
  - Used by MISP core to handle the conversion ability
  - Preserve as much content & context as possible
- Support all the STIX versions
  - **STIX 2.1 Support**
  - 1.1.1, 1.2, 2.0 Support enhanced

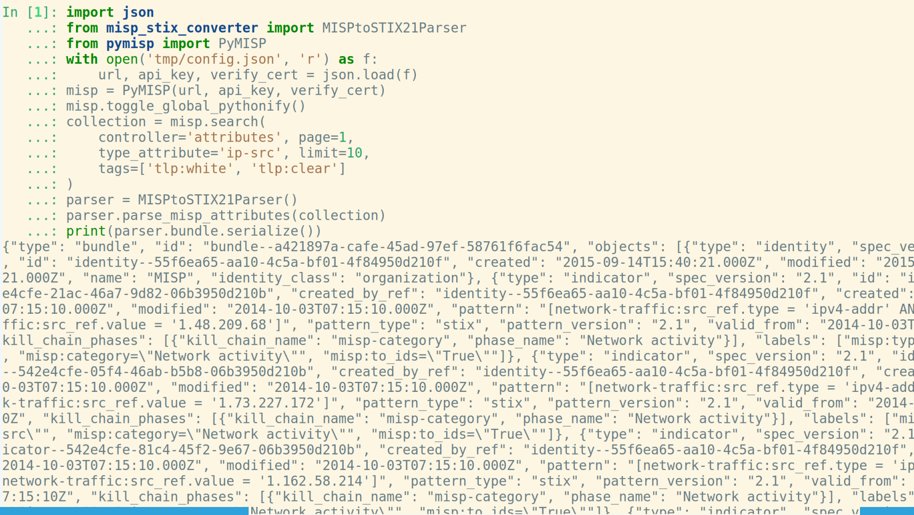
- **Mapping documentation**[1]
- Package available on PyPI[2]

[1] https://github.com/misp/misp-stix/tree/main/documentation#readme

[2] https://pypi.org/project/misp-stix/

Handling the conversion with a python library

- Integration in python code
    - Automation made easier by a close coupling with PyMISP
        - Export content from MISP

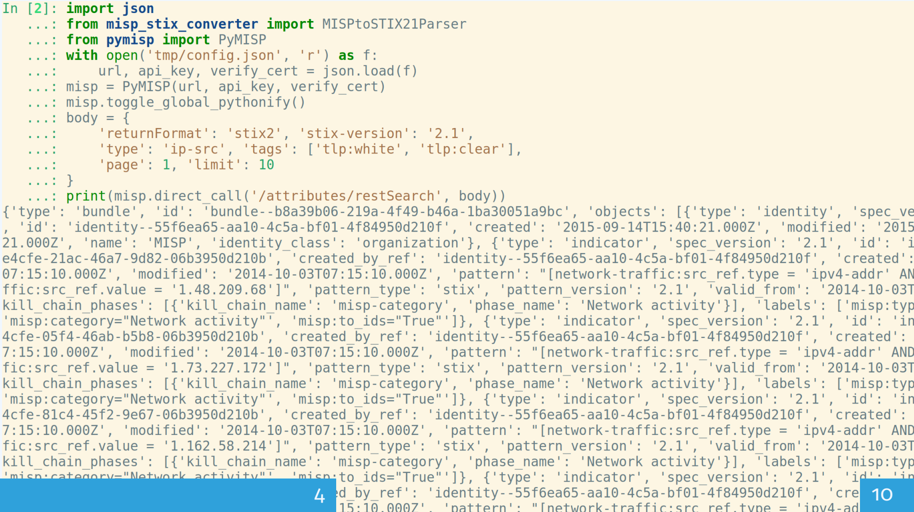


```
In [1]: import json
   ...: from misp_stix_converter import MISPtoSTIX21Parser
   ...: from pymisp import PyMISP
   ...: with open('tmp/config.json', 'r') as f:
   ...:     url, api_key, verify_cert = json.load(f)
   ...: misp = PyMISP(url, api_key, verify_cert)
   ...: misp.toggle_global_pythonify()
   ...: collection = misp.search(
   ...:     controller='attributes', page=1,
   ...:     type_attribute='ip-src', limit=10,
   ...:     tags=['tlp:white', 'tlp:clear']
   ...: )
   ...: parser = MISPtoSTIX21Parser()
   ...: parser.parse_misp_attributes(collection)
   ...: print(parser.bundle.serialize())
```

```
{"type": "bundle", "id": "bundle--a421897a-cafe-45ad-97ef-58761f6fac54", "objects": [{"type": "identity", "spec_ve
, "id": "identity--55f6ea65-aa10-4c5a-bf01-4f84950d210f", "created": "2015-09-14T15:40:21.000Z", "modified": "2015
21.000Z", "name": "MISP", "identity_class": "organization"}, {"type": "indicator", "spec_version": "2.1", "id": "i
e4cfe-21ac-46a7-9d82-06b3950d210b", "created_by_ref": "identity--55f6ea65-aa10-4c5a-bf01-4f84950d210f", "created":
07:15:10.000Z", "modified": "2014-10-03T07:15:10.000Z", "pattern": "[network-traffic:src_ref.type = 'ipv4-addr' AN
ffic:src_ref.value = '1.48.209.68']", "pattern_type": "stix", "pattern_version": "2.1", "valid_from": "2014-10-03T
kill_chain_phases": [{"kill_chain_name": "misp-category", "phase_name": "Network activity"}], "labels": ["misp:typ
, "misp:category=\"Network activity\"", "misp:to_ids=\"True\""]}, {"type": "indicator", "spec_version": "2.1", "id
--542e4cfe-05f4-46ab-b5b8-06b3950d210b", "created_by_ref": "identity--55f6ea65-aa10-4c5a-bf01-4f84950d210f", "crea
0-03T07:15:10.000Z", "modified": "2014-10-03T07:15:10.000Z", "pattern": "[network-traffic:src_ref.type = 'ipv4-add
k-traffic:src_ref.value = '1.73.227.172']", "pattern_type": "stix", "pattern_version": "2.1", "valid_from": "2014-
0Z", "kill_chain_phases": [{"kill_chain_name": "misp-category", "phase_name": "Network activity"}], "labels": ["mi
src\"", "misp:category=\"Network activity\"", "misp:to_ids=\"True\""]}, {"type": "indicator", "spec_version": "2.1
icator--542e4cfe-81c4-45f2-9e67-06b3950d210b", "created_by_ref": "identity--55f6ea65-aa10-4c5a-bf01-4f84950d210f",
2014-10-03T07:15:10.000Z", "modified": "2014-10-03T07:15:10.000Z", "pattern": "[network-traffic:src_ref.type = 'ip
network-traffic:src_ref.value = '1.162.58.214']", "pattern_type": "stix", "pattern_version": "2.1", "valid_from":
7:15:10Z", "kill_chain_phases": [{"kill_chain_name": "misp-category", "phase_name": "Network activity"}], "labels"
```

Handling the conversion with a python library

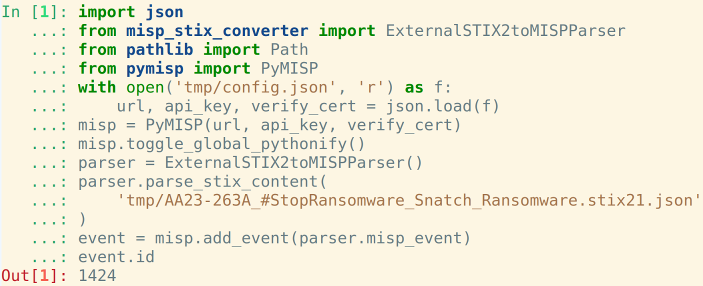
- Integration in python code
  - Automation made easier by a close coupling with PyMISP
    - Export content from MISP
    - Using the STIX return format directly



```
In [2]: import json
   ...: from misp_stix_converter import MISPtoSTIX21Parser
   ...: from pymisp import PyMISP
   ...: with open('tmp/config.json', 'r') as f:
   ...:     url, api_key, verify_cert = json.load(f)
   ...: misp = PyMISP(url, api_key, verify_cert)
   ...: misp.toggle_global_pythonify()
   ...: body = {
   ...:     'returnFormat': 'stix2', 'stix-version': '2.1',
   ...:     'type': 'ip-src', 'tags': ['tlp:white', 'tlp:clear'],
   ...:     'page': 1, 'limit': 10
   ...: }
   ...: print(misp.direct_call('/attributes/restSearch', body))
{'type': 'bundle', 'id': 'bundle--b8a39b06-219a-4f49-b46a-1ba30051a9bc', 'objects': [{'type': 'identity', 'spec_ve
, 'id': 'identity--55f6ea65-aa10-4c5a-bf01-4f84950d210f', 'created': '2015-09-14T15:40:21.000Z', 'modified': '2015
21.000Z', 'name': 'MISP', 'identity_class': 'organization'}, {'type': 'indicator', 'spec_version': '2.1', 'id': 'i
e4cfe-21ac-46a7-9d82-06b3950d210b', 'created_by_ref': 'identity--55f6ea65-aa10-4c5a-bf01-4f84950d210f', 'created':
07:15:10.000Z', 'modified': '2014-10-03T07:15:10.000Z', 'pattern': "[network-traffic:src_ref.type = 'ipv4-addr' AN
ffic:src_ref.value = '1.48.209.68']", 'pattern_type': 'stix', 'pattern_version': '2.1', 'valid_from': '2014-10-03T
kill_chain_phases': [{'kill_chain_name': 'misp-category', 'phase_name': 'Network activity'}], 'labels': ['misp:typ
'misp:category="Network activity"', 'misp:to_ids="True"']}, {'type': 'indicator', 'spec_version': '2.1', 'id': 'in
4cfe-05f4-46ab-b5b8-06b3950d210b', 'created_by_ref': 'identity--55f6ea65-aa10-4c5a-bf01-4f84950d210f', 'created':
7:15:10.000Z', 'modified': '2014-10-03T07:15:10.000Z', 'pattern': "[network-traffic:src_ref.type = 'ipv4-addr' AND
fic:src_ref.value = '1.73.227.172']", 'pattern_type': 'stix', 'pattern_version': '2.1', 'valid_from': '2014-10-03T
kill_chain_phases': [{'kill_chain_name': 'misp-category', 'phase_name': 'Network activity'}], 'labels': ['misp:typ
'misp:category="Network activity"', 'misp:to_ids="True"']}, {'type': 'indicator', 'spec_version': '2.1', 'id': 'in
4cfe-81c4-45f2-9e67-06b3950d210b', 'created_by_ref': 'identity--55f6ea65-aa10-4c5a-bf01-4f84950d210f', 'created':
7:15:10.000Z', 'modified': '2014-10-03T07:15:10.000Z', 'pattern': "[network-traffic:src_ref.type = 'ipv4-addr' AND
fic:src_ref.value = '1.162.58.214']", 'pattern_type': 'stix', 'pattern_version': '2.1', 'valid_from': '2014-10-03T
kill_chain_phases': [{'kill_chain_name': 'misp-category', 'phase_name': 'Network activity'}], 'labels': ['misp:typ
'misp:category="Network activity"', 'misp:to_ids="True"']}, {'type': 'indicator', 'spec_version': '2.1', 'id': 'in
                                  ed_by_ref': 'identity--55f6ea65-aa10-4c5a-bf01-4f84950d210f', 'cre
                                  15:10.000Z', 'pattern': "[network-traffic:src_ref.type = 'ipv4-ad
```

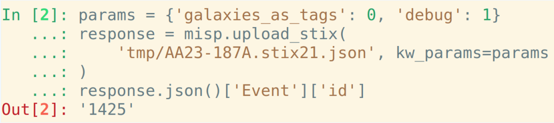
Handling the conversion with a python library

- Integration in python code
  - Automation made easier by a close coupling with PyMISP
    - Converting STIX content and adding the resulting Event



```
In [1]: import json
   ...: from misp_stix_converter import ExternalSTIX2toMISPParser
   ...: from pathlib import Path
   ...: from pymisp import PyMISP
   ...: with open('tmp/config.json', 'r') as f:
   ...:     url, api_key, verify_cert = json.load(f)
   ...: misp = PyMISP(url, api_key, verify_cert)
   ...: misp.toggle_global_pythonify()
   ...: parser = ExternalSTIX2toMISPParser()
   ...: parser.parse_stix_content(
   ...:     'tmp/AA23-263A_#StopRansomware_Snatch_Ransomware.stix21.json'
   ...: )
   ...: event = misp.add_event(parser.misp_event)
   ...: event.id
Out[1]: 1424
```

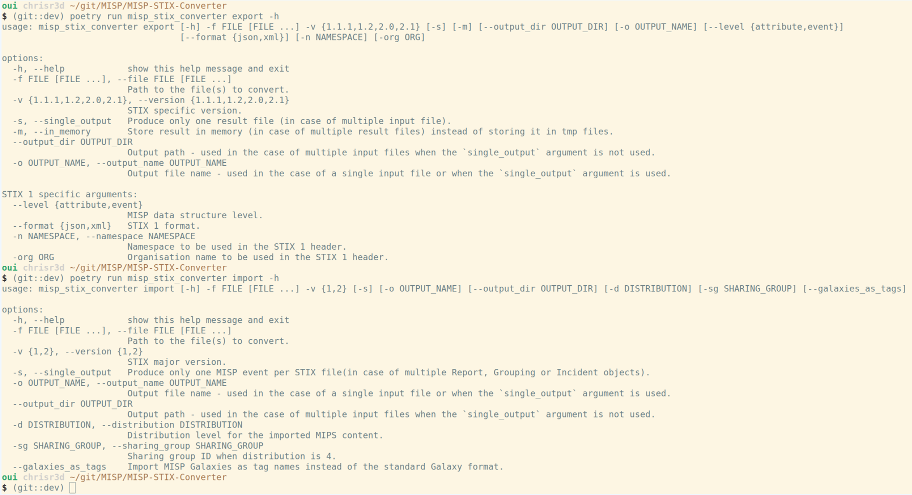
    - Using the API endpoint directly



```
In [2]: params = {'galaxies_as_tags': 0, 'debug': 1}
   ...: response = misp.upload_stix(
   ...:     'tmp/AA23-187A.stix21.json', kw_params=params
   ...: )
   ...: response.json()['Event']['id']
Out[2]: '1425'
```

Handling the conversion with a python library

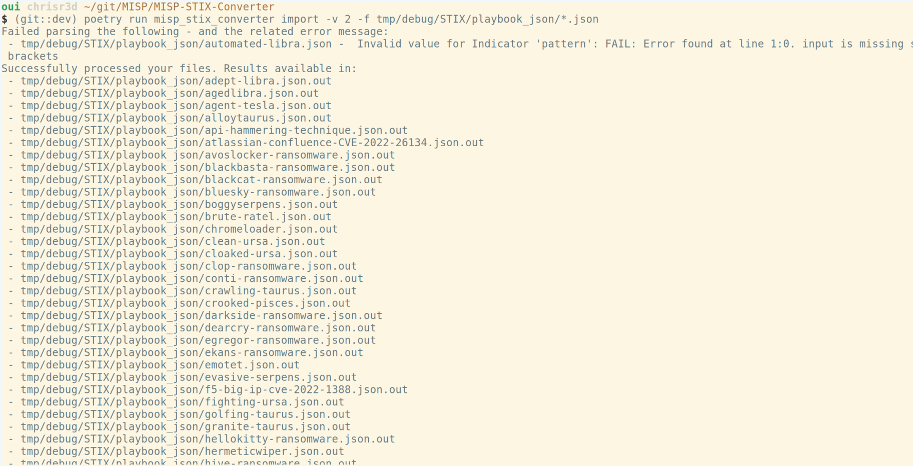
- Addressing the limitations of a MISP built-in integration
  - Export & import features available as a command-line application



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

options:
  -h, --help            show this help message and exit
  -f FILE [FILE ...], --file FILE [FILE ...]
                        Path to the file(s) to convert.
  -v {1.1.1,1.2,2.0,2.1}, --version {1.1.1,1.2,2.0,2.1}
                        STIX specific version.
  -s, --single_output   Produce only one result file (in case of multiple input file).
  -m, --in_memory       Store result in memory (in case of multiple result files) instead of storing it in tmp files.
  --output_dir OUTPUT_DIR
                        Output path - used in the case of multiple input files when the `single_output` argument is not used.
  -o OUTPUT_NAME, --output_name OUTPUT_NAME
                        Output file name - used in the case of a single input file or when the `single_output` argument is used.

STIX 1 specific arguments:
  --level {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.
  -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 import -h
usage: misp_stix_converter import [-h] -f FILE [FILE ...] -v {1,2} [-s] [-o OUTPUT_NAME] [--output_dir OUTPUT_DIR] [-d DISTRIBUTION] [-sg SHARING_GROUP] [--galaxies_as_tags]

options:
  -h, --help            show this help message and exit
  -f FILE [FILE ...], --file FILE [FILE ...]
                        Path to the file(s) to convert.
  -v {1,2}, --version {1,2}
                        STIX major version.
  -s, --single_output   Produce only one MISP event per STIX file(in case of multiple Report, Grouping or Incident objects).
  -o OUTPUT_NAME, --output_name OUTPUT_NAME
                        Output file name - used in the case of a single input file or when the `single_output` argument is used.
  --output_dir OUTPUT_DIR
                        Output path - used in the case of multiple input files when the `single_output` argument is not used.
  -d DISTRIBUTION, --distribution DISTRIBUTION
                        Distribution level for the imported MIPS content.
  -sg SHARING_GROUP, --sharing_group SHARING_GROUP
                        Sharing group ID when distribution is 4.
  --galaxies_as_tags    Import MISP Galaxies as tag names instead of the standard Galaxy format.
oui chrisr3d ~/git/MISP/MISP-STIX-Converter
$ (git::dev) 
```

Handling the conversion with a python library

- Addressing the limitations of a MISP built-in integration
  - Export & import features available as a command-line application



```
oui chrisr3d ~/git/MISP/MISP-STIX-Converter
$ (git::dev) poetry run misp_stix_converter import -v 2 -f tmp/debug/STIX/playbook_json/*.json
Failed parsing the following - and the related error message:
 - tmp/debug/STIX/playbook_json/automated-libra.json -  Invalid value for Indicator 'pattern': FAIL: Error found at line 1:0. input is missing s
 brackets
Successfully processed your files. Results available in:
 - tmp/debug/STIX/playbook_json/adept-libra.json.out
 - tmp/debug/STIX/playbook_json/agedlibra.json.out
 - tmp/debug/STIX/playbook_json/agent-tesla.json.out
 - tmp/debug/STIX/playbook_json/alloytaurus.json.out
 - tmp/debug/STIX/playbook_json/api-hammering-technique.json.out
 - tmp/debug/STIX/playbook_json/atlassian-confluence-CVE-2022-26134.json.out
 - tmp/debug/STIX/playbook_json/avoslocker-ransomware.json.out
 - tmp/debug/STIX/playbook_json/blackbasta-ransomware.json.out
 - tmp/debug/STIX/playbook_json/blackcat-ransomware.json.out
 - tmp/debug/STIX/playbook_json/bluesky-ransomware.json.out
 - tmp/debug/STIX/playbook_json/boggyserpens.json.out
 - tmp/debug/STIX/playbook_json/brute-ratel.json.out
 - tmp/debug/STIX/playbook_json/chromeloader.json.out
 - tmp/debug/STIX/playbook_json/clean-ursa.json.out
 - tmp/debug/STIX/playbook_json/cloaked-ursa.json.out
 - tmp/debug/STIX/playbook_json/clop-ransomware.json.out
 - tmp/debug/STIX/playbook_json/conti-ransomware.json.out
 - tmp/debug/STIX/playbook_json/crawling-taurus.json.out
 - tmp/debug/STIX/playbook_json/crooked-pisces.json.out
 - tmp/debug/STIX/playbook_json/darkside-ransomware.json.out
 - tmp/debug/STIX/playbook_json/dearcry-ransomware.json.out
 - tmp/debug/STIX/playbook_json/egregor-ransomware.json.out
 - tmp/debug/STIX/playbook_json/ekans-ransomware.json.out
 - tmp/debug/STIX/playbook_json/emotet.json.out
 - tmp/debug/STIX/playbook_json/evasive-serpens.json.out
 - tmp/debug/STIX/playbook_json/f5-big-ip-cve-2022-1388.json.out
 - tmp/debug/STIX/playbook_json/fighting-ursa.json.out
 - tmp/debug/STIX/playbook_json/golfing-taurus.json.out
 - tmp/debug/STIX/playbook_json/granite-taurus.json.out
 - tmp/debug/STIX/playbook_json/hellokitty-ransomware.json.out
 - tmp/debug/STIX/playbook_json/hermeticwiper.json.out
 - tmp/debug/STIX/playbook_json/hive-ransomware.json.out
```

Continuous Work in Progress & Improvement

- **Improve the import feature**
  - Handle different content design from different sources
  - Support of existing STIX objects libraries[3]
  - Support custom STIX format
  - **Handle validation issues**
- Continuous MISP ⟺ STIX mapping improvement
- More tests to avoid edge case issues

- Participating in Oasis CTI TC

[3] https://github.com/mitre/cti

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

To get in touch with us

- 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