

# MISP-STIX PROJECT

PYTHON LIBRARY TO CONVERT MISP <-> STIX

MISP CORE TEAM

MISP PROJECT

<https://www.misp-project.org/>

JTAN HACKATHON - 2022/06/03



- **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

## ■ Feature limitations

- ▶ Supported versions
- ▶ Data type support

## ■ Practical limitations

- ▶ Export and import features only available via MISP rest client
- ▶ **Github:** STIX issues lost within the MISP core issues

- Revamp of the source code
- **Enable a standalone use of the python code**
  - ▶ MISP JSON format -> STIX
  - ▶ Pass files with MISP JSON format -> get file with the export results in STIX
- Possible integration within python code

- Choose the STIX version
  - ▶ **STIX 2.1 Support**
- Filter on the data to export
  - ▶ **Attributes collections**
- **Mapping documentation**
- Better exceptions handling

# 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

# WORK IN PROGRESS & NEXT IMPROVEMENTS

- **Implementing the import feature**
- Extending the test cases
- Improving the conversion mapping
- Support of existing STIX objects libraries<sup>1</sup>
- Support custom STIX format<sup>2</sup>
- Package on PyPI

---

<sup>1</sup><https://github.com/mitre/cti>

<sup>2</sup>Especially while importing STIX data, **and as long as we can implement support of well defined versions**

## 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](https://twitter.com/chrisred_68)