MISP-STIX Project

Python library to convert MISP <-> STIX

MISP core team

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

MISP Summit 0x06 - 21st October 2021

MISP & STIX so far

- **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

Limitations

- 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

Handling the conversion with a python library

- 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

New features

- Choose the STIX version
  - **STIX 2.1 Support**
- **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
  - **Recommandation**: provide samples
- Any feedback welcome

Next improvements

- **Implement the import feature**
- Extend the export feature to any kind of data collection
- Support of existing STIX objects libraries[1]

- Support custom STIX format[2]
- More tests to avoid edge case issues

- Package on PyPI

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

[2] 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