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
- 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

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
- Package available on PyPI¹

+

¹https://pypi.org/project/misp-stix/

WORK IN PROGRESS & NEXT IMPROVEMENTS

- WiP
 - ► Implement the import feature
 - Support of existing STIX objects libraries²
- Next features on the roadmap
 - Extend the export feature to any kind of data collection
 - ► Support custom STIX format³
- Continuous improvement
 - Mapping improvement
 - More tests to avoid edge case issues

²https://github.com/mitre/cti

³Especially while importing STIX data, and as long as we can implement support of well defined versions

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