MISP-STIX Project

Python library to convert MISP <-> STIX

MISP core team

TLP:WHITE

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

MISP Training

2022-09-16

MISP-STIX Project

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

2022-09-16

MISP-STIX Project

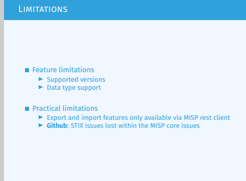
└MISP & STIX

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



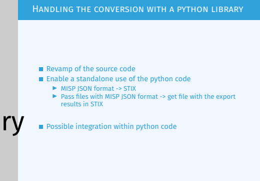
Limitations

- 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



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

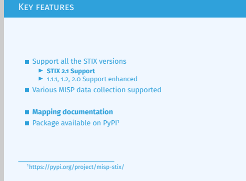
- **Mapping documentation**
- Package available on PyPI[1]

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

2022-09-16

MISP-STIX Project

└─Key features



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 PyPI[1]

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

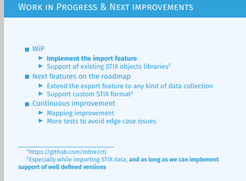
Work in Progress & Next improvements

- WiP
  - **Implement the import feature**
  - Support of existing STIX objects libraries[2]
- Next features on the roadmap
  - Extend the export feature to any kind of data collection
  - Support custom STIX format[3]
- Continuous improvement
  - Mapping improvement
  - More tests to avoid edge case issues

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

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

└Work in Progress & Next improvements



Work in Progress & Next improvements

- WiP
  - **Implement the import feature**
  - Support of existing STIX objects libraries[2]
- Next features on the roadmap
  - Extend the export feature to any kind of data collection
  - Support custom STIX format[3]
- Continuous improvement
  - Mapping improvement
  - More tests to avoid edge case issues

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

[3] Especially 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

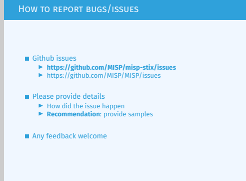
- Please provide details
  - How did the issue happen
  - **Recommendation**: provide samples

- Any feedback welcome

2022-09-16

MISP-STIX Project

└How to report bugs/issues



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

2022-09-16

MISP-STIX Project

└To get in touch with us

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