Developing in STIX and TAXII 2

June 2018

Learning Objectives

- Dive in to the OASIS Open Python libraries for STIX and TAXII 2
  - *By the end of the session:* you should know what the libraries do, how to find them, and where to go for help.

- Survey of other open source tooling for STIX and TAXII 2
  - *By the end of the session:* you should know broadly what STIX/TAXII 2 tooling is available and how to find it.

Please ask questions! We can click the links and dig in.

A note about interoperability

None of the tooling, applications, or content in these slides has been tested using the Interoperability Specification.

STIX and TAXII in Python

So you're using the One True Programming Language...

OASIS Open Python Libraries and Capabilities

- Basic capabilities
  - Parse and write STIX 2
  - Management of data sources and sinks, including TAXII 2
  - Vanilla TAXII 2 client

- Making it easy
  - Environment layer to wrap sources, sinks, and defaults
  - Workbench layer to provide a default environment and more helper functions

```
pip install stix2 taxii2client
```

stix2.readthedocs.io

github.com/oasis-open/cti-python-stix2 and github.com/oasis-open/cti-taxii-client

OASIS Open Repositories

Work organized by the TC

Python Tooling

TAXII Libraries

taxii-server (medallion) - A (very) basic TAXII 2.0 server in Flask

STIX 2.0 Patterning

pattern-matcher - Match patterns against observed data

pattern-validator - Validate a pattern string against the specification

STIX 1.x Compatibility

stix-elevator - Convert STIX 1.x to STIX 2.0

stix-slider - Convert STIX 2.0 to STIX 1.x

Working with STIX

stix-validator - Validate STIX 2.0 content against the schemas

stix-visualization - Visualize the domain objects and relationships

Other Resources

Schemas

stix2-json-schemas - JSON schemas for STIX 2.0 (will do STIX 2.1 CSDs)

Documentation

documentation - Documentation available on cti-tc.github.io

training - These training materials (to be posted)

Other Open Source Tooling

Other people are doing this too!

Libraries (similar to python-stix2)

STIX 2

libstix2 - Go libraries to work with STIX objects

scalastix - Scala libraries to work with STIX objects

stix2patterns_translator - Translate STIX Patterns to Splunk and Elastic queries

StixConvert - Scala tool to convert STIX 2 into GraphML or GEXF

StixToNeoDB - Scala tool to load STIX 2 into Neo4J

TAXII 2

freetaxii-server - A Go server for TAXII 2.0 and 2.1 (prerelease)

Taxii2LibScala - Scala server for TAXII 2.0

taxii2lib - A Javascript client library for TAXII 2.0

Tools and Applications

Cyberstation - A STIX and TAXII 2 GUI

MISP - An open source information sharing application with support for STIX and TAXII 1, STIX 2 (not TAXII 2).

Unfetter - An application to understand your security posture using MITRE's ATT&CK framework, based on STIX and TAXII 2.

Data Sources

They do exist!

OSINT STIX and TAXII Data Sources

FreeTAXII - https://test.freetaxii.com:8000/taxii2/

TAXII 2.1 preview server hosting collections including ZeuS, Feodo, Ransomware, EmergingThreats, Threatexpert.com

UberTAXII - https://ubertaxii.com/taxii/

TAXII 2.0 server hosting collections including CIRCL, AIS, ATT&CK, Perch Security, Interop Test Data

Other data sources (including vendor-provided and open source communities) available at the TC Wiki Front Page.

https://wiki.oasis-open.org/cti/#STIX2_data_sources

Thank You