A brief demo of the improvements in MISP 2.4 and a glimpse into what to expect from future versions

by Andras Iklody

Improvements already in 2.3

- A total of 143 patches since 2.3
- Usual fixes for usability and security issues
- performance improvements
- Examples:
  - Correlation speed improvement
  - smart push synchronisation
  - API improvements (both in MISP and PyMISP)

New features already in 2.3

- Improved settings and diagnostics
- RPZ export
- ZeroMQ Pub/Sub
- New APIs (Upload / download samples, tagging)
- Event Blacklisting
- Usability tools for admins (customisable password reset messages, pgp key fetcher, various admin tools for maintenance)

New features already in 2.3

- Features contributed by 3rd parties
  - SSL Authentication by Guilherme Capilé from FIRST
  - Proxy config by Richard van den Berg from NCSC

New things in 2.4

- Work in progress, beta available on “2.4-beta” branch
- Main focus Releasability
  - Organisations
  - Create sharing communities (Sharing Groups)
  - Old releasability still intact
  - Sharing groups affect local and cross-instance access

New things in 2.4

- Synchronisation Filters
- Manual selective synchronisation
- Update mode for selective synchronisation

(Demo)

New things in 2.4

- Other improvements:
  - First iteration of the correlation graphing
  - Connection tests
  - Financial indicators
  - Host of new attribute types
    - 81 type
    - 186 category/type combinations

(Demo)

Future Roadmap – v2.5

- Sightings support for MISP (Project by NCSC-NL)
  - Allows users to provide feedback on indicators
  - Various settings for anonymity
  - Allows for temporal correlation of data
  - via TAXII Service (Using STIX sightings)
  - API (using MISP's own format)
  - First iteration of STIX import (very limited profile)

Future Roadmap – v2.5

- Modular import/export
- Integration with other tools (such as Cuckoo)
- Various smaller features (github release 2.5 tag)

Future Roadmap – v3.0

- Datamodel rework
  - Object relations
  - Mapping to STIX
  - STIX import/export
  - Standard agnostic, but aligned with bigger standards (mainly with STIX/CyBox)
  - Similar scope as MISP is today
- Automatic / interactive enrichment

Future Roadmap – v4.0

- Extended scope
  - Threat Intelligence structures ontop of current scope
  - Such as Threat actors, Campaigns, TTPs

Questions and practical information

- To get in touch with me: **mailto:andras.iklody.contractor@circl.lu**
- Contact the MISP Project: **info@misp-project.org**
- Website: **http://www.misp-project.org**
- Users list: **https://groups.google.com/forum/#!forum/misp-users**
- Developers list: **https://groups.google.com/forum/#!forum/misp-devel**
- Github: **http://github.com/MISP/MISP**
- Information and access request for the CIRCL MISP communities: **https://www.circl.lu/services/misp-malware-information-sharing-platform**