What's next?
MISP - Malware Information Sharing Platform & Threat Sharing

CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy
Andras Iklody
Raphaël Vinot

TLP:WHITE

http://www.misp-project.org/
Twitter: *@MISPProject*

MISP Training Luxembourg
20170320

What's cooking?

MISP next features and work in progress

Tagging improvements

- Attribute level tags
  - **Apply galaxy clusters to attributes (in addition to tags)**
  - Wide range of use-cases (TLP markings, Kill-chain phase, CSIRTs status on compromised infrastructure)
- Internal tags
  - Gives us much more granularity.
  - **Convenient way to add features** without a database change.
- Tags with a variable component
  - Tags would have a variable embedded.
  - These would be set on a per tag-instance basis.
  - Examples for uses:
    - **Expiration tags**
    - **Boolean tags**

Graphing improvements

- Highly used but a currently underdeveloped feature
- **Add tags and galaxies** to the correlation graph
- Open up the **correlation graph to the enrichment module functionality**
- Allow adding attributes directly from the correlation graph
- Allow tagging / attaching clusters directly from the correlation graph

MISP objects

- Objective: create a semi-dynamic data model.
- Using existing MISP attributes to build new objects.
- **Share the object designs within partners automatically along with the events shared** (e.g. allowing to share events with yet unknown objects).
- Have a community-driven set of default objects[1].
- Early work already accessible, it's also open source.

[1] `https://github.com/misp/misp-objects`

MISP galaxy 2.0

- Currently galaxy clusters are static and based on the shared repository / an out of bound created local repository
- 2.0 Will allow the interactive creation / editing of galaxies and clusters
- Sharing these across instances will happen purely in MISP instead of just sharing the tags

MISP Darwin

- MISP events are great for more technical analysts or staff familiar with MISP
- The goal is to consolidate the information and automatically **generate natural language reports out of these events**
- Upcoming new project on GitHub
- Python code for managing the creation based on triggers and conversion mechanisms
- Using a list of pre-defined strings from customiseable libraries
- Similar approach as warninglists, taxonomies or galaxies. Just create your own JSON

MISP Workbench

- Objective: Make it easy to use MISP data in other contexts.
- Export snapshot of MISP values into Redis.
- Easily **enrich MISP dataset** with other fields (specially PE indicators).
- Group events using galaxies.
- Full text indexing and lookups for external values.
- Fuzzy hashing (binaries and import tables).

MISP Hashstore

- Allow very **fast lookups** against big dataset.
- Only store hashed versions of the attributes.
- Can be used on untrusted or compromised systems (comparable to **bloom filter**).
- Hashstore can be used for forensic analysis (e.g. compare baseline
- Beta version available[2].

[2] https://github.com/MISP/misp-workbench/tree/master/hashstore

MISP privacy-aware exchange

- A privacy-aware exchange module to securely and privately share your indicators.
- The basic idea is to transform MISP attributes into something sharable which does not leak any information.
- A first prototype is accessible[3].

[3] https://github.com/MISP/misp-privacy-aware-exchange

MISP Gamification

- Goal is to encourage users to contribute by offering recognition for their efforts.
- Profiles with various metrics tracking contribution.
- Opt-in system since it requires a loss of anonymity.
- Gain points by
  - Entering events
  - Proposing changes (that have to be accepted to get credit)
  - Reviewing events and pointing out false positives

Conclusion

- **Information sharing practices come from usage** and by example (e.g. learning by imitation from the shared information).
- MISP is just a tool. What matters is your sharing practices. The tool should be as transparent as possible to support you.
- Enable users to customize MISP to meet their community's use-cases.
- MISP is evolving into a modular tool for information sharing and "CTI".
- **Contributions and ideas originate from the community of users**.
- Co-funding of new features or projects around MISP are welcome.

Q&A

- `https://github.com/MISP/MISP`
- `https://github.com/MISP/` for misp-modules, misp-objects, misp-taxonomies and misp-galaxy.
- Feel free to open an issue or make a pull-request on GitHub.