

What's next?

MISP - Malware Information Sharing Platform & Threat Sharing



CIRCL

Computer Incident
Response Center
Luxembourg

Team CIRCL

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

MISP Training @ Prague
20180917

What's cooking?

MISP next features and work in progress

Tagging improvements

- Generating related tags (to show and propose similar tags for similar values)
- Special local tags to tags non-owned events
- "Tag everything project"
 - Gives us much more granularity.
 - **Convenient way to add features** without a database change.
- Tags exclusivity as expressed in Taxonomy (e.g. TLP:AMBER and TLP:GREEN tags are exclusive to an attribute or event)

Unified API and modules interface

- **Single search API** / scope (events, objects, attributes)
- Return in **any format** supported by the internal converters and export module
- **Consistent filters** for all output formats
- Open up export modules for bulk exports (framing system)

Graphing improvements

- Highly used but a currently underdeveloped feature
- 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
- Advanced correlation where correlations are proposed based on fuzzy matching
- Persistent / shareable graphs (on correlation - already available in graph event)
- Gephi export/integration (on correlation - already available in graph event)

MISP objects improvements

- In application object template editor
- Object level tagging and galaxies
- **Share the object designs within partners on-demand** (e.g. remotely browse shared templates of a partner and import them).
- Closer integration of the objects into the various exports
- MISP-modules upgrade for tighter object integration

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 customisable libraries
- Similar approach as warninglists, taxonomies or galaxies. Just create your own JSON

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 available¹.

¹<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 accessible².

²<https://github.com/MISP/misp-privacy-aware-exchange>

MISP dashboard 2.0

- Tighter integration with MISP
- 2 way communication with MISP
- Authenticated / ACL enabled version

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
- Based on the existing work in misp-dashboard (MISP up vote on usefulness on information will be added).

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.