What's next?

MISP - Malware Information Sharing Platform & Threat Sharing

CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy -
Andras Iklody - *TLP:WHITE*

MISP Training - 20160905

What's cooking?

MISP next features and work in progress

Tagging improvements

- Attribute level tags
  - **Apply tags to attributes**
  - 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**

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.
- Early work already accessible, it's also open source.

MISP galaxy

- MISP galaxy is a simple method to express a large object called cluster that can be attached to MISP events or attributes.
- A cluster can be composed of one or more elements. Elements are expressed as key-values.
- Existing clusters and elements like threat actors, adversary groups, attacker tools, campaigns are available.
- There are default elements available in MISP galaxy but those can be overwritten, replaced or updated as you wish.

MISP galaxy - elements of threat actors

- An element list of threat actors included by default.

```
{
 "synonyms": [
   "PLA Unit 61486",
   "APT 2",
   "Group 36",
   "APT-2",
   "MSUpdater",
   "4HCrew",
   "SULPHUR"
 ],
 "country": "CN",
 "refs": [
   "http://cdn0.vox-cdn.com/assets/4589853/
    crowdstrike-intelligence-report-putter-
       panda.original.pdf"
 ],
 "description": "The CrowdStrike
    Intelligence team has been
 tracking this particular unit since 2012,
 under the codename PUTTER PANDA, and has
    documented activity
 dating back to 2007. The report identifies
 Chen Ping, aka cpyy, and the primary
    location of Unit 61486. ",
 "group": "Putter Panda"
}
```

MISP galaxy - elements of threat actors tools

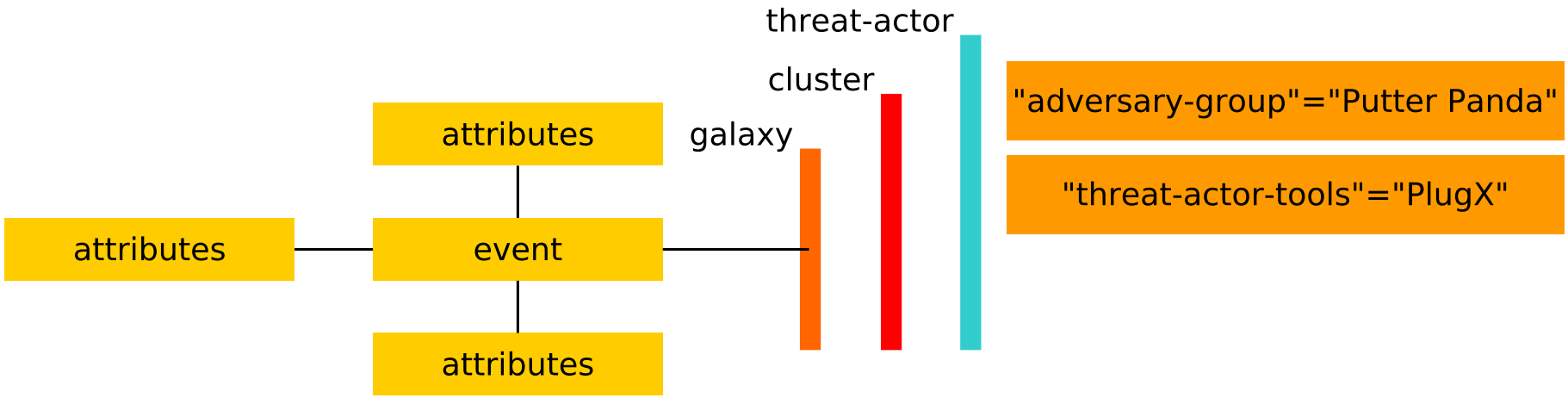
- An element list of tools used by various threat actors.
- The key-values can be freely combined.

```
            {
              "value": "MSUpdater"
            },
            {
              "value": "Poison Ivy",
              "description": "Poison Ivy is a RAT which
                  was freely available and first
                  released in 2005.",
              "refs": ["https://www.fireeye.com/content/
                  dam/fireeye-www/global/en/current-
                  threats/pdfs/rpt-poison-ivy.pdf"]
            },
            {
              "value": "Torn RAT"
            },
            {
              "value": "ZeGhost"
            },
            {
              "value": "Elise Backdoor",
              "synonyms": ["Elise"]
            }
```

MISP galaxy - A cluster is composed of various elements

```
1        {
2        "name" : "threat actor",
3        "description": "threat actor cluster",
4        "version": 1,
5        "elementOneOf": ["adversary-groups", "threat-
             actor-intended-effect-vocabulary", "planning
             -and-operational-support-vocabulary", "
             threat-actor-motivation-vocabulary", "threat
             -actor-type-vocabulary", "threat-actor-
             sophistication-vocabulary", "certainty-level
             ", "threat-actor-tools"]
6         }
```

MISP galaxy - how will it be integrated?



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[1].

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

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**.

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.