MISP new features and development evolution

MISP & Threat Sharing

CIRCL
Computer Incident
Response Center
Luxembourg

Andras Iklody - *TLP:WHITE*

MISP Summit II - 10/17/2016

2.4 development and release cycle

- Git tags are used for MISP point releases (2.4.x), each of which we consider to be a **stable release**.
- We generally recommend MISP administrators to always run the latest release version.
- Development version is on the git HEAD of the MISP project.
- Any new feature or functionality altering change at first ends up in a feature branch (such as feature/feeds)
- If several larger changes are to be added in an upcoming version, they are first merged into a testing pre-release branch (such as 2.4.51)

2.4 development and release cycle continued

- Once all of the new features are tested they are merged into the 2.4 branch
- Starting from 2.4, updates of the database schema are all done automatically at the first login.
- A MISP release[1] includes fixes, improvement and often new features (disabled by default if changing default MISP behavior).

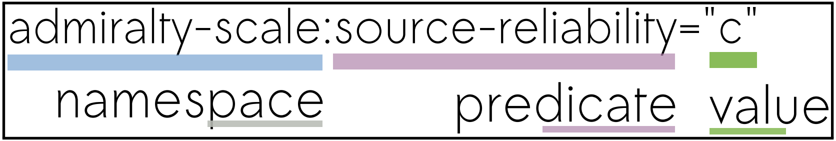
[1] http://www.misp-project.org/Changelog.txt

So what's new in MISP? (New features)

- The main mantra of the last year has been modulairty
  - We want to give the userbase to extend and customise MISP in various ways
  - We realised that in order to make this a reality, we need to remove a lot of functionality from the MISP core
  - The result was a series systems that are all being developed independently of the MISP core application
  - Each of them have their own github repository and have their own active communities
  - These can be freely reused and integrated in other threat intel tools

MISP Taxonomies

- Classify events using various known vocabularies, contextualise using threat intel related taxonomies, define how the contained indicators can be actioned on
- Triple tag format (namespace:predicate="value")



admiralty-scale:source-reliability="c"

namespace predicate value

- Simple JSON format, includes triple tag, colour, extended descriptions
- No programming knowledge required to create taxonomies

Existing Taxonomies

- NATO - **Admiralty Scale**
- CIRCL Taxonomy - **Schemes of Classification in Incident Response and Detection**
- eCSIRT and IntelMQ incident classification
- EUCI **EU classified information marking**
- Information Security Marking Metadata from DNI (Director of National Intelligence - US)
- NATO Classification Marking
- OSINT **Open Source Intelligence - Classification**
- TLP - **Traffic Light Protocol**
- Vocabulary for Event Recording and Incident Sharing - **VERIS**
- and many more like ENISA, Europol, or the draft FIRST SIG Information Exchange Policy.

MISP Warninglists

- Warn users about potential false positives
- Lists of values that will trigger on entry for certain or all attribute types
- String matches or cidr ranges
- Similar to Taxonomies in design
- Simple JSON format to describe a warninglist
- Trivial to develop, immediate impact in the application

MISP Modules

- Extend functionalities that were part of the MISP core before (import/export)
- Add a new enrichment system to MISP
- Web service running side by side with MISP based on Tornado
- Simple to write conversion modules, tied directly into the UI and soon the APIs
- All Python based
- No internal knowledge of MISP required, can reuse the freetext facilities of MISP

Example Modules

- Enrichment
  - PassiveTotal
  - CIRCL PassiveSSL/PassiveDNS
  - Virustotal
- Import
  - STIX
  - OCR
- Export
  - CEF

New features of the past few months

- Feed system
  - MISP feeds
  - Ingest external feeds (freetext, CSV)
  - Ability to leverage MISP as a feed provider
  - Avoiding air-gap issues
  - Cherry-picking data
  - Constant tuning of indicator detection

New features of the past few months

- Internal synchronisation
  - The advantages of running more than one MISP instances
  - The downsides of such as setup prior to internal sync
  - Exchange data between internal instances without any of the sync side effects
- Various new integration options
  - Bro export
  - Reworked STIX export
  - STIX - MISP converter
- Inline screenshots
- Shibboleth authentication
- Massive list of fixes, improvements

Upcoming features on the short term roadmap - 2.4.53/54

- 2.4.53
  - Multiple tags assigneable to a Feed
  - Internal taxonomy
  - Correlation only events (especially when used in junction with the feeds)
  - Improved tag searches
- 2.4.54
  - Import/export API rework
  - Unified APIs with a common set of filter options
  - Open up access to the import/export modules
  - Route feeds through the import/export modules

Upcoming features on the short term roadmap - 2.4.55

- 2.4.55
  - Rework of the scheduled tasks
  - Allow setting granular parameters for the scheduled tasks
  - Easy error recovery
  - Add/Remove/Edit granular tasks rapidly

Upcoming features on the short term roadmap - 2.4.56

- 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**

Mid term features

- MISP Galaxies
  - 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.
- Galaxy 1.0 implementation
  - Our answer to the threat intel requirements
  - Using the misp-galaxy project data
  - First implementation will allow the linking to static galaxies
  - Community driven repository

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

```
{
"name" : "threat actor",
"description": "threat actor cluster",
"version": 1,
"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"]
 }
```

Other mid term features

- Async modules
- Attribute overrides using proposals
- Various new Import/Export modules
- Rule based tag-translation system for the synchronisation/feeds
- Feed and module authentication systems
- User-settings

Longer term features - MISP objects

- Objective: create a semi-dynamic data model.
- Using existing MISP attributes to build new objects[2].
- **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.

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

Longer term features - other

- MISP Galaxies 2.0
- Gamification
- Role based views of the data (Analyst view, Manager view, Financial sector view, etc)
- Advanced correlations
- Opt-in MISP discovery mode
- Graph based enrichment

Q&A

- `https://github.com/MISP/MISP`
- `https://github.com/MISP/` for misp-modules, misp-objects and misp-taxonomies
- info@circl.lu (if you want to join one of the MISP community operated by CIRCL)
- PGP key fingerprint: CA57 2205 C002 4E06 BA70 BE89 EAAD CFFC 22BD 4CD5