Information Sharing and Taxonomies
Practical Classification of Threat Indicators using MISP

Alexandre Dulaunoy -
TLP:WHITE

January 26, 2016
Quick MISP introduction

• MISP\(^1\) is an IOC and threat indicators sharing software.
• MISP has **many functionalities** e.g. flexible sharing groups, automatic correlation, free-text import helper, event distribution and collaboration.
• CIRCL operates multiple MISP instances with a significant user base (around 300 organizations with 700 users).
• After some years of trial-and-error, we share in this presentation a specific **new MISP feature introduced in 2.4 called taxonomies**.

\(^1\)https://github.com/MISP/MISP
Sharing Difficulties

• Legal restriction
  ○ "Our legal framework doesn’t allow us to share information."
  ○ "Risk of information leak is too high and it’s too risky for our organization or partners."

• Practical restriction
  ○ "We don’t have information to share."
  ○ "We don’t have time to process or contribute indicators."
  ○ "Our model of classification doesn’t fit your model."
  ○ "Tools for sharing information are tied to a specific format, we use a different one."
From Tagging to Flexible Taxonomies

OSINT - Cyberthreats BlackEnergy2

- Tagging is a simple way to attach a classification to an event.
- In the early version of MISP, tagging was local to an instance.
- After evaluating different solutions of classification, we build a new scheme using the concept of machine tags.
Machine Tags

• Triple tag or machine tag was introduced in 2004 to extend geotagging on images.

```
admiralty-scale:source-reliability="c"
```

• A machine tag is just a tag expressed in way that allows systems to parse and interpret it.

• Still have a human-readable version:
  ○ `admiralty-scale:Source Reliability=""Fairly reliable""`
MISP Taxonomies

- Taxonomies are implemented in a simple JSON format.
- Anyone can create their own taxonomy or reuse an existing one.
- The taxonomies are in an independent git repository\(^2\).
- These can be freely reused and integrated in other threat intel tools.

\(^2\)https://www.github.com/MISP/misp-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**
Want to write your own taxonomy? 1/2

```json
{
    "namespace": "admiralty-scale",
    "description": "The Admiralty Scale (also called the NATO System) is used to rank the reliability of a source and the credibility of an information."
    "version": 1,
    "predicates": [
        {
            "value": "source-reliability",
            "expanded": "Source Reliability"
        },
        {
            "value": "information-credibility",
            "expanded": "Information Credibility"
        }
    ]
}....
```
Want to write your own taxonomy? 2/2

```json
{
    "values": [
        {
            "predicate": "source-reliability",
            "entry": [
                {
                    "value": "a",
                    "expanded": "Completely reliable"
                }
            ]
        }
    ]
}
```

- Publishing your taxonomy is as easy as a simple git pull request on misp-taxonomies³.

³[https://github.com/MISP/misp-taxonomies](https://github.com/MISP/misp-taxonomies)
How are taxonomies integrated in MISP?

- MISP administrator can just import (or even cherry pick) the namespace or predicates they want to use as tag.
- Tags can be exported to other instances.
- Tags are also accessible via the MISP REST API.
Filtering the distribution of events among MISP instances

- Applying rules for distribution based on tags:
Other use cases using MISP taxonomies

- Tags can be used to set events for further processing by external tools (e.g. VirusTotal auto-expansion using Viper).
- Ensuring a classification manager classifies the events before release (e.g. release of information from air-gapped/classified networks).
- Enriching IDS export with tags to fit your NIDS deployment.
Future functionalities related to MISP taxonomies

• Sighting support (thanks to NCSC-NL) will be integrated in MISP allowing to auto expire IOC based on user detection.
• Adjusting taxonomies (adding/removing tags) based on their score or visibility via sighting.
• Simple taxonomy editors to help non-technical users to create their taxonomies.
• More public taxonomies to be included.
Q&A

- https://github.com/MISP/MISP
- https://github.com/MISP/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