Information Sharing and Taxonomies Practical Classification of Threat Indicators using MISP



Alexandre Dulaunoy - TLP:WHITE

March 24, 2016

From Tagging to Flexible Taxonomies

OSINT - Cyberthreats BlackEnergy2

Event ID	2910			
Uuid	568e7167-4e00-4654-b5f8-4b23950d210f			
Org	CIRCL			
Owner org	CIRCL			
Contributors				
Email	alexandre.dulaunoy@circl.lu			
Tags	tlp:white x Type:OSINT x +			
Date	2016-01-07			
Threat I evel	Medium			

- 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.

- A machine tag is just a tag expressed in way that allows systems to parse and interpret it.
- Still have a human-readable version:
 - o 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 repository¹.
- These can be freely reused and integrated in other threat intel tools.

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

```
"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.
4
5
    "predicates": [
6
7
8
9
         "value": "source-reliability",
         "expanded": "Source Reliability"
10
11
         "value": "information—credibility",
12
         "expanded": "Information Credibility"
13
14
15
```

Want to write your own taxonomy? 2/2

 Publishing your taxonomy is as easy as a simple git pull request on misp-taxonomies².

²https://github.com/MISP/misp-taxonomies

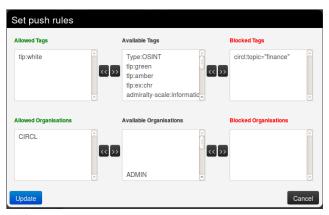
How are taxonomies integrated in MISP?

10	×	TO:HIDE		2	Ø.
9	×	TODO		8	Ø
11	×	TODO:VT-ENRICHMENT		9	Ø.
1	~	Type:OSINT		932	Ø.
18	•	admiralty-scale:information-credibility="1"	admiralty-scale	0	Ø
19	✓	admiralty-scale:information-credibility="2"	admiralty-scale	1	Ø
20	✓	admiralty-scale:information-credibility="3"	admiralty-scale	3	Ø
21	✓	admiralty-scale:information-credibility="4"	admiralty-scale	0	Ø
22	•	admiralty-scale:information-credibility="5"	admiralty-scale	1	Ø.
23	4	admiralty-scale:information-credibility="6"	admiralty-scale	2	G.

- 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:



9 of 12

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 classies 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