

Best Practices in Threat Intelligence

Gather, document, analyse and contextualise intelligence using MISP

Team CIRCL

MISP Project

<https://www.misp-project.org/>

MISP Training @ UNIV-LORRAINE
20191108



MISP
Threat Sharing

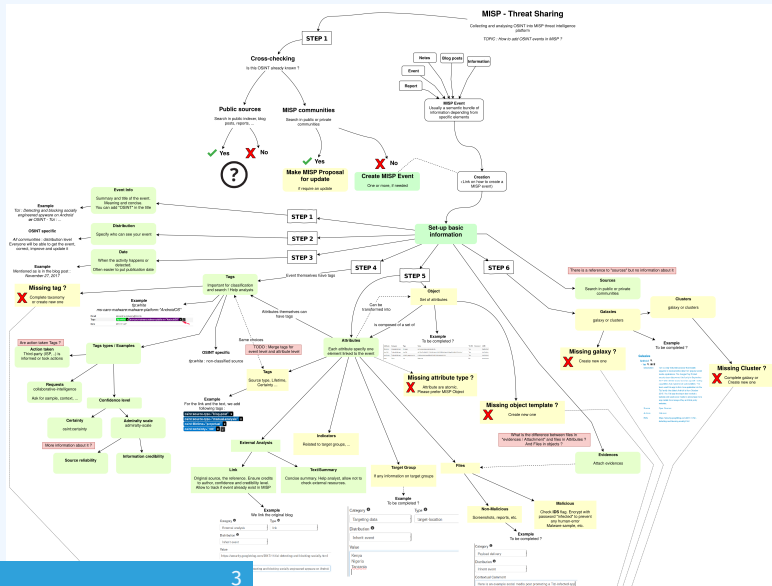
OBJECTIVES

- Learning how to use MISP to support common OSINT gathering use-cases as often used by SOC, CSIRTs and CERTs
- By using a list of practical exercise¹
- The exercises are **practical recent cases to model and structure intelligence** using the MISP standard
- Improving the data models available in MISP by exchanging live improvements and ideas
- Being able to share the results to the community at the end of this session

¹<https://gist.github.com/adulau/8c1de48060e259799d3397b83b0eec4f>

- **Cyber threat intelligence (CTI) is a vast concept** which includes different fields such as intelligence as defined in the military community or in the financial sector or the intelligence community
- **MISP project doesn't want to lock an organisation or an user into a specific model.** Each model is useful depending of the objectives from an organisation
- A set of pre-defined knowledge base or data-models are available and organisation can select (or create) what they need
- During this session, an overview of the most used taxonomies, galaxies and objects will be described

OVERALL PROCESS OF COLLECTING AND ANALYSING OSINT



- Quality of indicators/attributes are important but **tagging and classification are also critical to ensure actionable information**
- Tagging intelligence is done by using tags in MISP which are often originating from MISP taxonomy libraries
- The scope can be classification (*tlp, PAP*), type (*osint, type, veris*), state (*workflow*), collaboration (*collaborative-intelligence*) and many other fields
- MISP taxonomies documentation is available²
- **Review existing practices of tagging in your sharing community, reuse practices and improve context**

²<https://www.misp-project.org/taxonomies.html>

- **When information cannot be expressed in triple tags format** (*namespace:predicate=value*), MISP provides the galaxies
- Galaxies contain a huge set of common libraries³ such as threat actors, malicious tools, RAT, Ransomware, target information and many more
- When tagging or adding a galaxy cluster, don't forget that tagging at event level is for the whole event (including attributes and objects). While tagging at attribute level, it's often a more specific context

³<https://www.misp-project.org/galaxy.html>

- If the information is a **single atomic element**, using a single attribute is preferred
 - ▶ Choosing an attribute type is critical as this defines the automation/export rule (e.g. url versus link or ip-src/ip-dst?)
 - ▶ Enabling the IDS (automation) flag is also important. When you are in doubt, don't set the IDS flag
- If the information is **composite** (ip/port, filename/hash, bank account/BIC), using an object is strongly recommended

HOW TO SELECT THE RIGHT OBJECT?

There are more than 150 MISP objects⁴ templates.

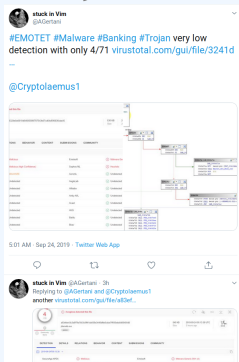
As an example, at CIRCL, we regularly use the following object templates *file*, *microblog*, *domain-ip*, *ip-port*, *coin-address*, *virustotal-report*, *paste*, *person*, *ail-leak*, *pe*, *pe-section*, *registry-key*.

⁴<https://www.misp-project.org/objects.html>

MICROBLOG OBJECT

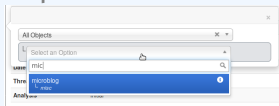
Use case

A series of OSINT tweets from a security researcher. To structure the thread, the information and keep an history.



Object to use

The microblog object can be used for Tweet or any microblog post (e.g. Facebook). Then object can be linked using *followed-by* to describe a serie of post.



Use case

- A file sample was received by email or extracted from VirusTotal.
- A list of file hashes were included in a report.
- A hash value was mentioned in a blog post.

Object to use

The file object can be used to describe file. It's usual to have partial meta information such as a single hash and a filename.

Add File Object

Object Template	File v17
Description	File object describing a file with meta-information
Requirements	Required one of: filename, size-in-bytes, authentichash, ssdeep, md5, sha1, sha224, sha256, sha384, sha512, sha512/224, sha512/256, tlsh, pattern-in-file, x509-fingerprint-sha1, malware-sample, attachment, path, fullpath
Meta category	File
Distribution	Inherit event
Comment	

- Graphical overview of OSINT collection using MISP <https://github.com/adulau/misp-osint-collection>
- MISP objects documentation
<https://www.misp-project.org/objects.html>
- MISP taxonomies documentation
<https://www.misp-project.org/taxonomies.html>
- MISP galaxy documentation
<https://www.misp-project.org/galaxy.html>