

BEST PRACTICES IN THREAT INTELLIGENCE

GATHER, DOCUMENT, ANALYSE AND CONTEXTUALISE IN-

CIRCL / TEAM MISP PROJECT

MISP PROJECT

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

CIISI-IE DUBLIN 2024



2024-07-08

Best Practices in Threat Intelligence

BEST PRACTICES IN THREAT INTELLIGENCE

GATHER, DOCUMENT, ANALYSE AND CONTEXTUALISE IN-

CIRCL / TEAM MISP PROJECT

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

CIISI-IE DUBLIN 2024



- Learn how to use MISP to support common OSINT gathering use-cases often used by SOC, CSIRTs and CERTs
 - ▶ Use practical exercise examples¹
 - ▶ The exercises are based on **practical recent cases to model and structure intelligence** using the MISP standard
- Improve the data models available in MISP by exchanging live improvements and ideas
- Be able to share the results to the community at the end of this session

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

Objectives

- Learn how to use MISP to support common OSINT gathering use-cases often used by SOC, CSIRTs and CERTs
 - ▶ Use practical exercise examples¹
 - ▶ The exercises are based on **practical recent cases to model and structure intelligence** using the MISP standard
- Improve the data models available in MISP by exchanging live improvements and ideas
- Be able to share the results to the community at the end of this session

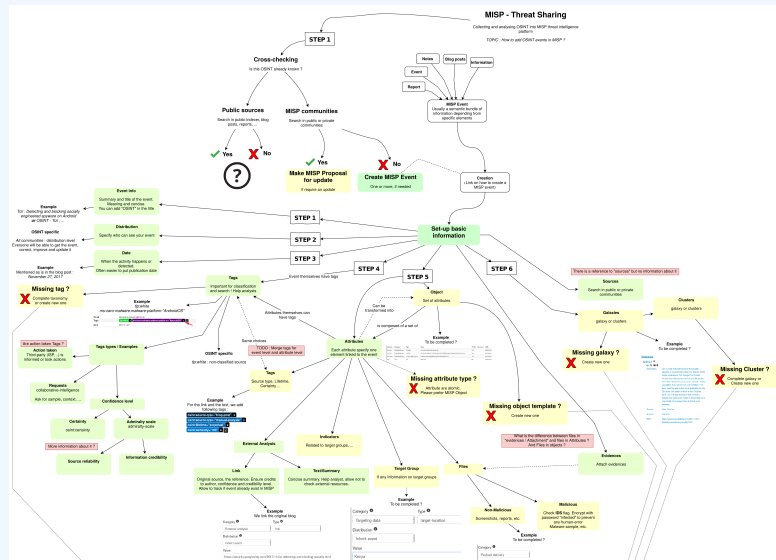
¹<https://gist.github.com/adulau/8c1de48060e259799d3397b83b0eec4f>

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

└─(Threat) Intelligence

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

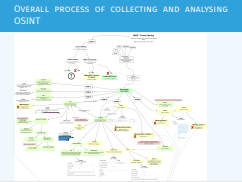
OVERALL PROCESS OF COLLECTING AND ANALYSING OSINT



2024-07-08

Best Practices in Threat Intelligence

Overall process of collecting and analysing OSINT



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

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

└─ Meta information and contextualisation 1/2

- Quality of indicators/attributes are important but **tagging and classification are also critical to ensure actionable information**
- Organizing intelligence is done in MISP by using tags, which often originate from MISP taxonomy libraries
- The scope can be classification (*tlp*, *PAP*), type (*osint*, *type*, *veris*), state (*workflow*), collaboration (*collaborative-intelligence*), or many other fields
- MISP taxonomy documentation is readily 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 use Galaxies
- **Galaxies** contain a huge set of common libraries³ such as threat actors, malicious tools, tactics, target information, mitigations, and more
- When tagging or adding a Galaxy cluster, tagging at the event level is for the whole event (including attributes and objects). Tagging at the attribute level is for a more specific context

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

└─ Meta information and contextualisation 2/2

- When information cannot be expressed in triple tags format (*namespace:predicate=value*), MISP use Galaxies
- **Galaxies** contain a huge set of common libraries³ such as threat actors, malicious tools, tactics, target information, mitigations, and more
- When tagging or adding a Galaxy cluster, tagging at the event level is for the whole event (including attributes and objects). Tagging at the attribute level is for a more specific context

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

- **Words of Estimative Probability**⁴ propose clear wording while estimating probability of occurrence from an event
- A MISP taxonomy called **estimative-language**⁵ proposes an applied model to tag information in accordance with the concepts of Estimative Probability

⁴[https:](https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/sherman-kent-and-the-board-of-national-estimates-collected-essays-6words.html)

[//www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/sherman-kent-and-the-board-of-national-estimates-collected-essays-6words.html](https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/sherman-kent-and-the-board-of-national-estimates-collected-essays-6words.html)

⁵<https://www.misp-project.org/taxonomies.html>

└ Estimative Probability

- **Words of Estimative Probability**⁴ propose clear wording while estimating probability of occurrence from an event
- A MISP taxonomy called **estimative-language**⁵ proposes an applied model to tag information in accordance with the concepts of Estimative Probability

⁴<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/sherman-kent-and-the-board-of-national-estimates-collected-essays-6words.html>

⁵<https://www.misp-project.org/taxonomies.html>

- The **Admiralty Scale**⁶ (also called the **NATO System**) is used to rank the reliability of a source and the credibility of information
- A MISP taxonomy called admiralty-scale⁷ is available
- US DoD **JP 2-0, Joint Intelligence**⁸ includes an appendix to express confidence in analytic judgments
- A MISP predicate in estimative-language called confidence-in-analytic-judgment⁹ is available

⁶<https://www.ijlter.org/index.php/ijlter/article/download/494/234>,
US Army Field Manual 2-22.3, 2006

⁷<https://www.misp-project.org/taxonomies.html>

⁸http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_o.pdf,
page 114

⁹<https://www.misp-project.org/taxonomies.html>

└ Reliability, credibility, and confidence

- The **Admiralty Scale**⁶ (also called the **NATO System**) is used to rank the reliability of a source and the credibility of information
- A MISP taxonomy called admiralty-scale⁷ is available
- US DoD **JP 2-0, Joint Intelligence**⁸ includes an appendix to express confidence in analytic judgments
- A MISP predicate in estimative-language called confidence-in-analytic-judgment⁹ is available

⁶<https://www.ijlter.org/index.php/ijlter/article/download/494/234>,
US Army Field Manual 2-22.3, 2006
⁷<https://www.misp-project.org/taxonomies.html>
⁸http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_o.pdf,
page 114
⁹<https://www.misp-project.org/taxonomies.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, but *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

└ Adding attributes/objects to an event

- 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, but *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

There are more than 150 MISP object¹⁰ 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*.

¹⁰<https://www.misp-project.org/objects.html>

└─ How to select the right object?

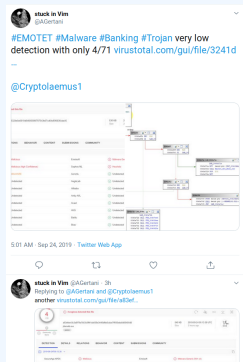
There are more than 150 MISP object¹⁰ templates.
As an example, at CIRCL, we regularly use the following object templates *file*, *microblog*, *domain-ip*, *ip-port*, *coin-address*, *virustotal-report*, *paste*, *person*, *ail-leak*, *pe*, *pe-section*, *registry-key*.

¹⁰<https://www.misp-project.org/objects.html>

MICROBLOG OBJECT

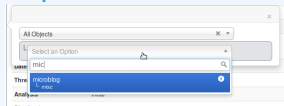
Use case

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



Object to use

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



Best Practices in Threat Intelligence

└ microblog object

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



Object to use
The microblog object can be used for Tweets or any microblog post (e.g. Facebook). The object can be linked using *followed-by* to describe a series 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	<input type="text"/>

└ file object

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	<input type="text"/>

- 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>

References

- 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>