Best Practices in Threat Intelligence

Gather, document, analyse and contextualise intelligence using MISP

Team CIRCL

MISP Project
`https://www.misp-project.org/`

MISP Training @ CIRCL
20190923

Objectives

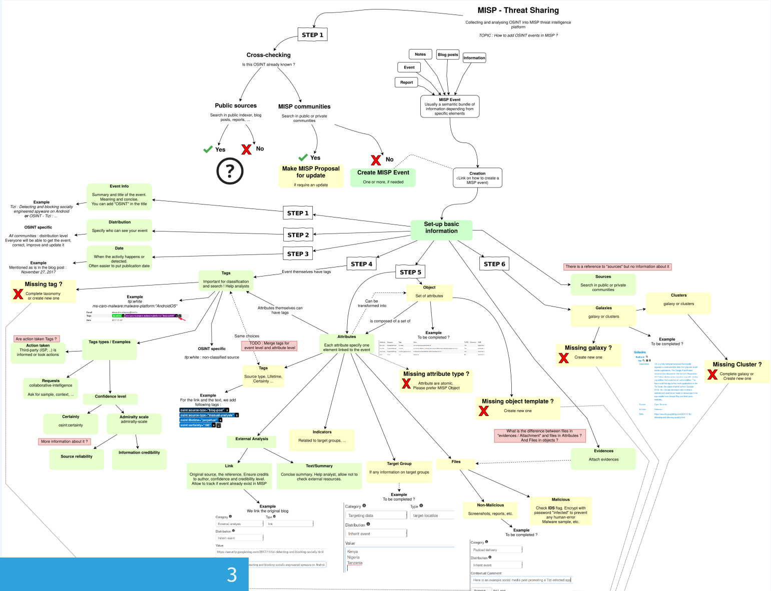
- Learning how to use MISP to support common OSINT gathering use-cases as often used by SOC, CSIRTs and CERTs
- By using a list of practical exercise[1]
- The exercises are **practical recent cases to model and structure intelligence** using the MISP standard
- Improving the data models available in 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

(Threat) Intelligence

- **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



MISP - Threat Sharing

Collecting and analysing OSINT into MISP threat intelligence platform

TOPIC : How to add OSINT events in MISP ?

STEP 1

Cross-checking
Is this OSINT already known ?

Public sources
Search in public indexer, blog posts, reports, ...
✓ Yes
☒ No
?

MISP communities
Search in public or private communities
✓ Yes — **Make MISP Proposal for update**: if require an update
☒ No — **Create MISP Event**: One or more, if needed

Notes
Blog posts
Information
Event
Report

MISP Event
Usually a semantic bundle of information depending from specific elements

Creation
<Link on how to create a MISP event)

Set-up basic information

STEP 1

Event Info
Summary and title of the event.
Meaning and concise.
You can add "OSINT" in the title

Example
Tizi : Detecting and blocking socially engineered spyware on Android
or *OSINT - Tizi : ...*

STEP 2

Distribution
Specify who can see your event

OSINT specific
All communities : distribution level
Everyone will be able to get the event, correct, improve and update it

STEP 3

Date
When the activity happens or detected.
Often easier to put publication date

Example
Mentioned as is in the blog post :
November 27, 2017

STEP 4

Event themselves have tags

Tags
Important for classification and search ! Help analysts

Missing tag ?
☒ Complete taxonomy or create new one

Example
tlp:white
ms-caro-malware:malware-platform:"AndroidOS"

Are action taken Tags ?

Action taken
Third-party (ISP, ..) is informed or took actions

Tags types / Examples

Requests
collaborative-intelligence

Ask for sample, context, ...

Confidence level

Certainty
osint:certainty

Admiralty scale
admiralty-scale

More information about it ?

Source reliability

Information credibility

OSINT specific
tlp:white : non-classified source

Same choices

TODO : Merge tags for event level and attribute level

Attributes themselves can have tags

Tags
Source type, Lifetime, Certainty ...

Example
For the link and the text, we add following tags :
osint:source-type="blog-post"
osint:source-type="manual-analysis"
osint:lifetime="perpetual"
osint:certainty="100"

STEP 5

Object
Set of attributes

Can be transformed into

is composed of a set of

Example
To be completed ?

Attributes
Each attribute specify one element linked to the event

Missing attribute type ?
☒ Attribute are atomic.
Please prefer MISP Object

Missing object template ?
☒ Create new one

External Analysis

Link
Original source, the reference. Ensure credits to author, confidence and credibility level.
Allow to track if event already exist in MISP

Example
We link the original blog

Category: External analysis
Type: link
Distribution: Inherit event
Value: https://security.googleblog.com/2017/11/tizi-detecting-and-blocking-socially.html

Text/Summary
Concise summary. Help analyst, allow not to check external resources.

Indicators
Related to target groups, ...

Target Group
If any information on target groups

Example
To be completed ?

Category: Targeting data
Type: target-location
Distribution: Inherit event
Value:
Kenya
Nigeria
Tanzania

Files

Non-Malicious
Screenshots, reports, etc.

Example
To be completed ?

Category: Payload delivery
Distribution: Inherit event
Contextual Comment: Here is an example social media post promoting a Tizi-infected app

Malicious
Check **IDS** flag. Encrypt with password "infected" to prevent any human-error
Malware sample, etc.

What is the difference between files in "evidences / Attachment" and files in Attributes ?
And Files in objects ?

Evidences
Attach evidences

STEP 6

There is a reference to "sources" but no information about it

Sources
Search in public or private communities

Galaxies
galaxy or clusters

Clusters
galaxy or clusters

Missing galaxy ?
☒ Create new one

Example
To be completed ?

Galaxies
Android
- Tizi

Missing Cluster ?
☒ Complete galaxy or Create new one

Meta information and contextualisation 1/2

- 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 available[2]
- **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 2/2

- **When information cannot be expressed in triple tags format** (*namespace:predicate=value*), MISP provides the galaxies
- Galaxies contain a huge set of common libraries[3] 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

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. When you are in doubt, don't set the IDS flag
- If the information is **composite** (ip/port, filename/hash, bank account/BIC), using a object is strongly recommended

How to select the right object?

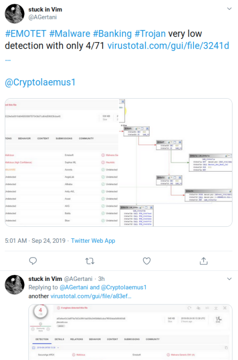
There are more than 150 MISP objects[4] templates.
As an example, at CIRCL, we regularly use the following object templates *file*, *microblog*, *domain-ip*, *ip-port*, *coin-address*, *virustotal-report*, *paste*, *person*, *ail-leak*, *pe*, *pe-section*, *registry-key*.

[4] https://www.misp-project.org/objects.html

MICROBLOG OBJECT

Use case

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



stuck in Vim
@AGertani

#EMOTET #Malware #Banking #Trojan very low detection with only 4/71 virustotal.com/gui/file/3241d …

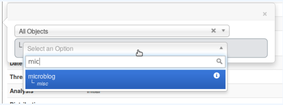
@Cryptolaemus1

5:01 AM · Sep 24, 2019 · Twitter Web App

stuck in Vim @AGertani · 3h
Replying to @AGertani and @Cryptolaemus1
another virustotal.com/gui/file/a83ef...

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.



All Objects

Select an Option

mic

microblog
└ misc

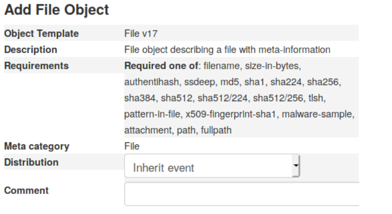
FILE OBJECT

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, authentihash, 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	

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