Forensic support in MISP

Tools and visualization to support digital

Team CIRCL

info@circl.lu

August 3, 2022

MISP Threat Sharing

2022-08-03

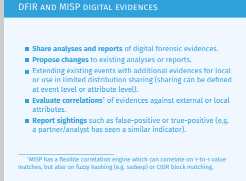
Forensic support in MISP

Forensic support in MISP
Tools and visualization to support digital
Team CIRCL
info@circl.lu
August 3, 2022
MISP Threat Sharing

DFIR and MISP digital evidences

- **Share analyses and reports** of digital forensic evidences.
- **Propose changes** to existing analyses or reports.
- Extending existing events with additional evidences for local or use in limited distribution sharing (sharing can be defined at event level or attribute level).
- **Evaluate correlations**[1] of evidences against external or local attributes.
- **Report sightings** such as false-positive or true-positive (e.g. a partner/analyst has seen a similar indicator).

[1] MISP has a flexible correlation engine which can correlate on 1-to-1 value matches, but also on fuzzy hashing (e.g. ssdeep) or CIDR block matching.



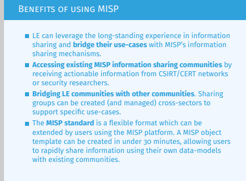
DFIR and MISP digital evidences

- **Share analyses and reports** of digital forensic evidences.
- **Propose changes** to existing analyses or reports.
- Extending existing events with additional evidences for local or use in limited distribution sharing (sharing can be defined at event level or attribute level).
- **Evaluate correlations**[1] of evidences against external or local attributes.
- **Report sightings** such as false-positive or true-positive (e.g. a partner/analyst has seen a similar indicator).

[1] MISP has a flexible correlation engine which can correlate on 1-to-1 value matches, but also on fuzzy hashing (e.g. ssdeep) or CIDR block matching.

Benefits of using MISP

- LE can leverage the long-standing experience in information sharing and **bridge their use-cases** with MISP's information sharing mechanisms.
- **Accessing existing MISP information sharing communities** by receiving actionable information from CSIRT/CERT networks or security researchers.
- **Bridging LE communities with other communities**. Sharing groups can be created (and managed) cross-sectors to support specific use-cases.
- The **MISP standard** is a flexible format which can be extended by users using the MISP platform. A MISP object template can be created in under 30 minutes, allowing users to rapidly share information using their own data-models with existing communities.

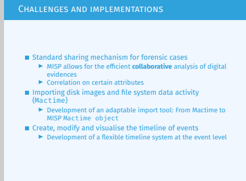


Benefits of using MISP

- LE can leverage the long-standing experience in information sharing and **bridge their use-cases** with MISP's information sharing mechanisms.
- **Accessing existing MISP information sharing communities** by receiving actionable information from CSIRT/CERT networks or security researchers.
- **Bridging LE communities with other communities**. Sharing groups can be created (and managed) cross-sectors to support specific use-cases.
- The **MISP standard** is a flexible format which can be extended by users using the MISP platform. A MISP object template can be created in under 30 minutes, allowing users to rapidly share information using their own data-models with existing communities.

Challenges and implementations

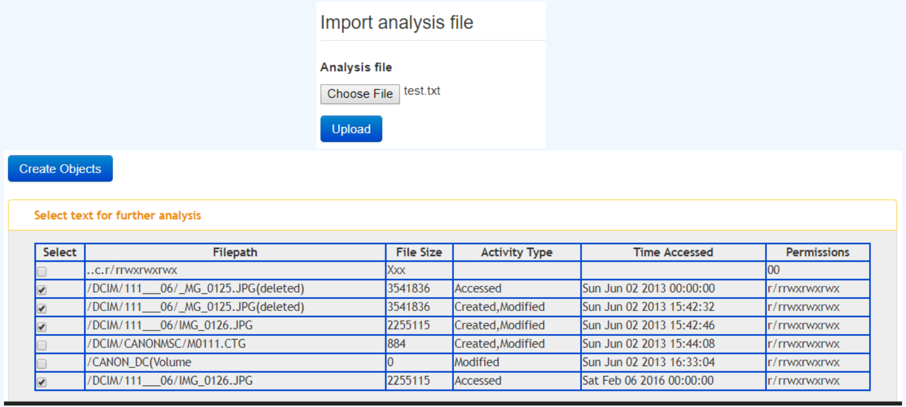
- Standard sharing mechanism for forensic cases
    - MISP allows for the efficient **collaborative** analysis of digital evidences
    - Correlation on certain attributes
- Importing disk images and file system data activity (`Mactime`)
    - Development of an adaptable import tool: From Mactime to MISP `Mactime object`
- Create, modify and visualise the timeline of events
    - Development of a flexible timeline system at the event level



Challenges and implementations

- Standard sharing mechanism for forensic cases
    - MISP allows for the efficient **collaborative** analysis of digital evidences
    - Correlation on certain attributes
- Importing disk images and file system data activity (`Mactime`)
    - Development of an adaptable import tool: From Mactime to MISP `Mactime object`
- Create, modify and visualise the timeline of events
    - Development of a flexible timeline system at the event level

Forensic import (MISP 2.4.98)



Import analysis file

Analysis file

test.txt

Select text for further analysis

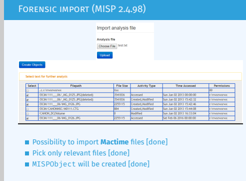
Select	Filepath	File Size	Activity Type	Time Accessed	Permissions
☐	..c.r/rrwxrwxrwx	Xxx			00
☑	/DCIM/111___06/_MG_0125.JPG(deleted)	3541836	Accessed	Sun Jun 02 2013 00:00:00	r/rrwxrwxrwx
☑	/DCIM/111___06/_MG_0125.JPG(deleted)	3541836	Created,Modified	Sun Jun 02 2013 15:42:32	r/rrwxrwxrwx
☑	/DCIM/111___06/IMG_0126.JPG	2255115	Created,Modified	Sun Jun 02 2013 15:42:46	r/rrwxrwxrwx
☐	/DCIM/CANONMSC/M0111.CTG	884	Created,Modified	Sun Jun 02 2013 15:44:08	r/rrwxrwxrwx
☐	/CANON_DC(Volume	0	Modified	Sun Jun 02 2013 16:33:04	r/rrwxrwxrwx
☑	/DCIM/111___06/IMG_0126.JPG	2255115	Accessed	Sat Feb 06 2016 00:00:00	r/rrwxrwxrwx

- Possibility to import **Mactime** files [done]
- Pick only relevant files [done]
- `MISPObject` will be created [done]

2022-08-03

Forensic support in MISP

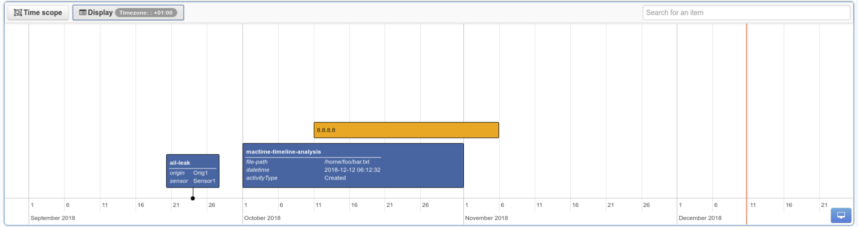
└Forensic import (MISP 2.4.98)



Forensic import (MISP 2.4.98)

- Possibility to import **Mactime** files [done]
- Pick only relevant files [done]
- `MISPObject` will be created [done]

DATA VISUALIZATION (MISP ZOIDBERG BRANCH)



ail-leak

origin	Orig1
sensor	Sensor1

mactime-timeline-analysis

file-path	/home/foo/bar.txt
datetime	2018-12-12 06:12:32
activityType	Created

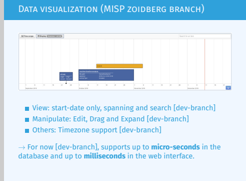
- View: start-date only, spanning and search [dev-branch]
- Manipulate: Edit, Drag and Expand [dev-branch]
- Others: Timezone support [dev-branch]

→ For now [dev-branch], supports up to **micro-seconds** in the database and up to **milliseconds** in the web interface.

2022-08-03

Forensic support in MISP

└Data visualization (MISP zoidberg branch)


DATA VISUALIZATION (MISP ZOIDBERG BRANCH)

- View: start-date only, spanning and search [dev-branch]
- Manipulate: Edit, Drag and Expand [dev-branch]
- Others: Timezone support [dev-branch]

→ For now [dev-branch], supports up to **micro-seconds** in the database and up to **milliseconds** in the web interface.