Forensic support in MISP

FORENSIC SUPPORT IN MISP TOOLS AND VISUALIZATION TO SUPPORT DIGITAL TAM GRCL HITO@CRICLU

hreat Sharing

OCTOBER 2, 2024

FORENSIC SUPPORT IN MISP

TOOLS AND VISUALIZATION TO SUPPORT DIGITAL

TEAM CIRCL

INFO@CIRCL.LU

OCTOBER 2, 2024



DFIR AND MISP DIGITAL EVIDENCES

2024-10-0

└─DFIR and MISP digital evidences

Forensic support in MISP

Share analyses and reports of digital forensic evidences.
Propose changes to existing analyses or reports.
Extending existing events with additional evidences for loca

- or use in limited distribution sharing (sharing can be defined at event level or attribute level).
- Evaluate correlations¹ 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).

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

- 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).

¹MISP 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.

Forensic support in MISP

2024-7

Benefits of using MISP

BENEFITS OF USING M

- ELE 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 floxible 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

Forensic support in MISP

3

2024-

L-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
- Importing disk images and me system data activity (Mactime)
- Development of an adaptable import tool: From Mactime to MISP Mactime object
- Create, modify and visualise the timeline of events

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 Choose File test txt Upload

Create Objects

Select text for further analysis

Select	Filepath	File Size	Activity Type	Time Accessed	Permissions
	c.r/rrwxrwxrwx	Ххх			00
e	/DCIM/11106/_MG_0125.JPG(deleted)	3541836	Accessed	Sun Jun 02 2013 00:00:00	r/rrwxrwxrwx
e	/DCIM/11106/_MG_0125.JPG(deleted)	3541836	Created,Modified	Sun Jun 02 2013 15:42:32	r/rrwxrwxrwx
e	/DCIM/11106/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/mwxrwxrwx
•	/DCIM/11106/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]

Forensic support in MISP

2024-10-02

└─Forensic import (MISP 2.4.98)

		noort analysis	Sie		
		ndonin Tie			
		Danafia waw			
nate De	en el				
	_				
	ic to forther andust				
3 I B	chi futba antun	100.000	hint for	Textinent	1 Marcine
	A To Tother watch	7 th Tar	Addres Tage	Treduced	Personal
1-1-1 1 -1-1-1	Next to further annual Press to a function of the function of	Sec.	humpi	Inche D 2012 N.M.M.	ale and a second
1-1-1 1 -1-1-1	A To Tother watch				ale and a second
1-1-1 1 -1-1-1	A to former annual a r tomore annual Information and a call of a strength Information and a call of a strength Information and a call of a strength Information and a	Sec.	Normal Country Normal	An to 2 21 20 30 40	in the second se
1-1-1 1 -1-1-1	A to further annuals A Construment (Construment)	1400 1400	homai Codel, he Bhat Chates, he Bhat Chates, he Bhat	lan her 2010 2010 2018 No. her 2010 1010 2010 No. her 2010 1010 1010 No. her 2010 1010 4010	
1 - 1 - 1 - 1 - 1 - 1 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2	A to former annual a r tomore annual Information and a call of a strength Information and a call of a strength Information and a call of a strength Information and a	1-110 1-110 1-110	Normal Country Normal	An to 2 21 20 30 40	Frendrich B Viersenere Viersenere Viersenere Viersenere Viersenere Viersenere

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

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]

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

Forensic support in MISP

2024-10-02

└─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.