Forensic support in MISP

Tools and visualization to support digital forensic

Team CIRCL

info@circl.lu

June 18, 2019
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 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.
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
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]

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