An Introduction to Cybersecurity Information Sharing

MISP - Malware Information Sharing Platform & Threat Sharing

CIRCL
Computer Incident
Response Center
Luxembourg

Team CIRCL

http://www.misp-project.org/
Twitter: *@MISPProject*

Univ. Lorraine
20181124

Agenda

- (09:00 - 13:00) Session threat intelligence

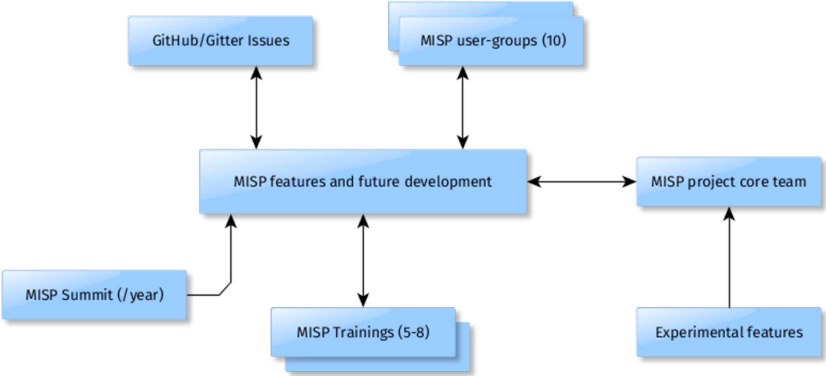
MISP and starting from a practical use-case

- During a malware analysis workgroup in 2012, we discovered that we worked on the analysis of the same malware.
- We wanted to share information in an easy and automated way **to avoid duplication of work**.
- Christophe Vandeplas (then working at the CERT for the Belgian MoD) showed us his work on a platform that later became MISP.
- A first version of the MISP Platform was used by the MALWG and **the increasing feedback of users** helped us to build an improved platform.
- MISP is now **a community-driven development**.

Development based on practical user feedback

- There are many different types of users of an information sharing platform like MISP:
    - **Malware reversers** willing to share indicators of analysis with respective colleagues.
    - **Security analysts** searching, validating and using indicators in operational security.
    - **Intelligence analysts** gathering information about specific adversary groups.
    - **Law-enforcement** relying on indicators to support or bootstrap their DFIR cases.
    - **Risk analysis teams** willing to know about the new threats, likelyhood and occurences.
    - **Fraud analysts** willing to share financial indicators to detect financial frauds.

MISP model of governance



GitHub/Gitter Issues

MISP user-groups (10)

MISP features and future development

MISP project core team

MISP Summit (/year)

MISP Trainings (5-8)

Experimental features

Many objectives from different user-groups

- Sharing indicators for a **detection** matter.
  - 'Do I have infected systems in my infrastructure or the ones I operate?'
- Sharing indicators to **block**.
  - 'I use these attributes to block, sinkhole or divert traffic.'
- Sharing indicators to **perform intelligence**.
  - 'Gathering information about campaigns and attacks. Are they related? Who is targeting me? Who are the adversaries?'
- → These objectives can be conflicting (e.g. False-positives have different impacts)

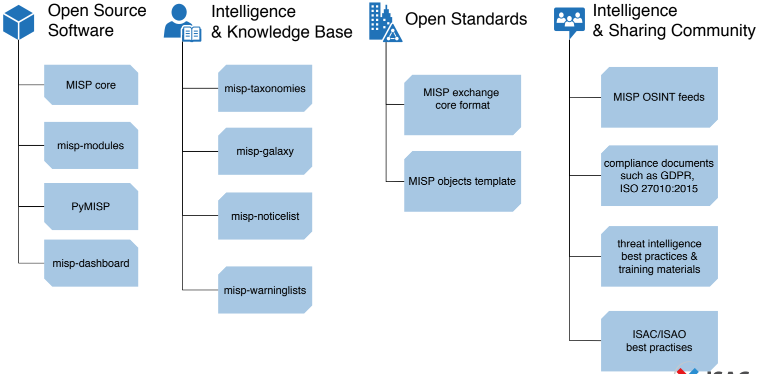
Sharing Difficulties

- Sharing difficulties are not really technical issues but often it's a matter of **social interactions** (e.g. **trust**).
- Legal restriction[1]
  - "Our legal framework doesn't allow us to share information."
  - "Risk of information-leak is too high and it's too risky for our organization or partners."
- Practical restriction
  - "We don't have information to share."
  - "We don't have time to process or contribute indicators."
  - "Our model of classification doesn't fit your model."
  - "Tools for sharing information are tied to a specific format, we use a different one."

[1] `https://www.misp-project.org/compliance/`

MISP Project Overview

MISP Project is a **completely open collaborative effort** to support analysts and organisations in all efforts related to **information sharing and threat intelligence**. The project includes a range of open source software, composed of a **threat intelligence platform** with sharing capabilities, expansion modules, advanced API capabilities and situational awareness tools. It also includes a comprehensive intelligence library and knowledge base acting as reference material for common taxonomies and classifications, threat-actors, complex intelligence models and common false-positive warning libraries. Furthermore, the project encompasses a set of **open standards**, of which the reference implementation is MISP itself, designed to be freely reused by communities developing their own software and tools. In addition, the MISP project releases a set of best practises that can be used as guidelines meant **to support closed, semi-open and open sharing communities**.



- Open Source Software
  - MISP core
  - misp-modules
  - PyMISP
  - misp-dashboard
- Intelligence & Knowledge Base
  - misp-taxonomies
  - misp-galaxy
  - misp-noticelist
  - misp-warninglists
- Open Standards
  - MISP exchange core format
  - MISP objects template
- Intelligence & Sharing Community
  - MISP OSINT feeds
  - compliance documents such as GDPR, ISO 27010:2015
  - threat intelligence best practices & training materials
  - ISAC/ISAO best practises

MISP features

- MISP[2] is a threat information sharing free & open source software.
- There is a possibility to run it as a self-hosted service, or to join community hosted instnaces
- It can be used in island mode, internal clusters or peer to peer connected
- MISP has **a host of functionalities** that assist users in creating, collaborating & sharing threat information - e.g. flexible sharing groups, **automatic correlation**, free-text import helper, event distribution & proposals.
- Many export formats which support IDSes / IPSes (e.g. Suricata, Bro, Snort), SIEMs (eg CEF), Host scanners (e.g. OpenIOC, STIX, CSV, yara), analysis tools (e.g. Maltego), DNS policies (e.g. RPZ).
- One of the key goals is modularity and customisations to make the tool fit your workflows

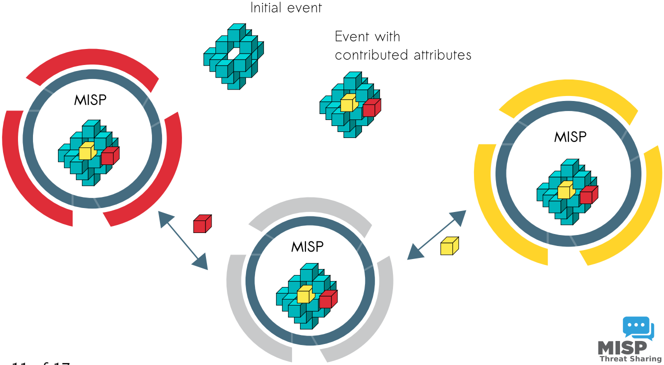
[2] https:/

Communities using MISP

- Communities are groups of users sharing within a set of common objectives/values.
- CIRCL operates multiple MISP instances with a significant user base (more than 950 organizations with more than 2400 users).
- **Trusted groups** running MISP communities in island mode (air gapped system) or partially connected mode.
- **Financial sector** (banks, ISACs, payment processing organizations) use MISP as a sharing mechanism.
- **Military and international organizations** (NATO, military CSIRTs, n/g CERTs,...).
- **Security vendors** running their own communities (e.g. Fidelis) or interfacing with MISP communities (e.g. OTX).

MISP core distributed sharing functionality

- MISPs' core functionality is sharing where everyone can be a consumer and/or a contributor/producer."
- Quick benefit without the obligation to contribute.
- Low barrier access to get acquainted to the system.



Helping Contributors in MISP

- Contributors can use the UI, API or using the freetext import to add events and attributes.
    - Modules existing in Viper (a binary framework for malware reverser) to populate and use MISP from the vty or via your IDA.
- Contribution can be direct by creating an event but **users can propose attributes updates** to the event owner.
- **Users should not be forced to use a single interface to contribute**.

Various ways of contextualising information

- Data is somewhat useful in itself, **context is what makes the data actionable** though
  - Who can we give the information to?
  - What can we do with the information?
  - Do we trust the source of the data and/or does the source have trust in the information?
  - What concerns is the information trying to address?
  - How can we make use of the information?
  - What sort of automatic actions should the publishing of the data trigger?
- **MISP includes several flexible systems to support these concerns** (tags, taxonomies, galaxies)

Dealing with various hurdles when sharing data in MISP

- Anonymised sharing via the delegation system
- Air-gapped connections / out of band sharing
- Granular sharing
    - Granular distribution system - mark distribution at any level
    - Sharing Group system to support recurring sharing topologies and ad hoc sharing scenarios
    - Filtered sharing to enable/disable sharing based on certain marking related criteria
- Feedback loop for the community via Sightings
- Collaborative information sharing (proposals vs extended events)

False positive handling

- Collaborative tools mentioned earlier (proposals, sightings)
- False-positive notification lists called warning lists
- Detection and alerting for certain potentially invalid data points (financial indicators predominantly)

Tools for building larger networked MISP ”clouds” internally

- Local sync option
- Various automated and manual **filtering** options
- **Orchestration** via APIs
- **Flexible data-model** (MISP objects) to map your legacy and internal systems or model

Conclusion

- **Information sharing practices come from usage** and by example (e.g. learning by imitation from the shared information).
- MISP is just a tool. What matters is your sharing practices. The tool should be as transparent as possible to support you.
- Enable users to customize MISP to meet their community's use-cases.