Practical Information Sharing between Law Enforcement and CSIRT communities using MISP

E.101

CIRCL Computer Incident Response Center Luxembourg

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

October 27, 2022 - v0.7

Objectives

- The 2-day session objective is to show and practice **structured information-exchange** and sharing among team members, SOCs, CSIRT and LEA partners.
- The main objective is to be able to map real cases (based on practices from the previous modules) into structured and shareable information.
- The session will be interactive and access will be given to a MISP training instance.
- At the end of the 2-day module, you will be able to use MISP and **better undertand sharing practices** among different actors.

Objectives
- The 2-day session objective is to show and practice **structured information-exchange** and sharing among team members, SOCs, CSIRT and LEA partners.
- The main objective is to be able to map real cases (based on practices from the previous modules) into structured and shareable information.
- The session will be interactive and access will be given to a MISP training instance.
- At the end of the 2-day module, you will be able to use MISP and **better undertand sharing practices** among different actors.

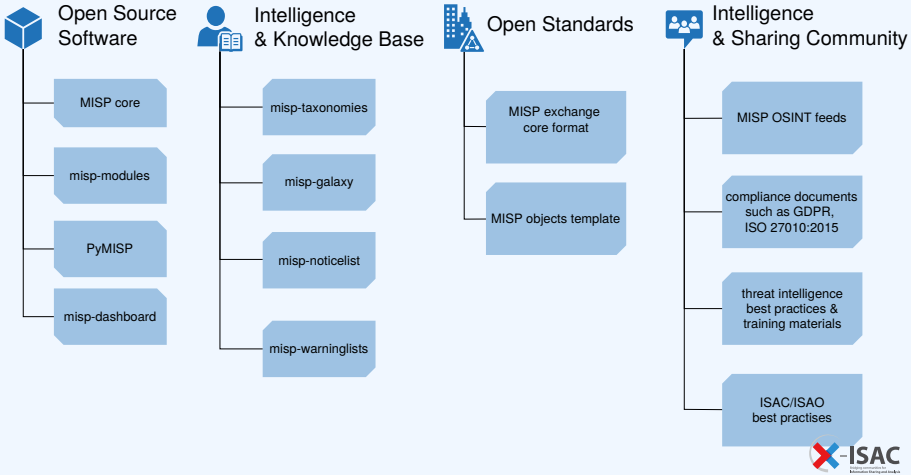
1. The goal is not to go for full technical session (even if there are some interesting labs) but the focus is the ability to describe cases into structured intelligence to server sharing. Sharing aspect is not only with third parties or partners but it's also within a team or a joint investigation team. This module is also the opportunity to setup and share the access to the MISP training instance which will be used for the 2-day session.

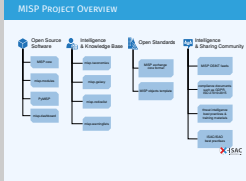
MISP - Open Source Threat Intelligence Platform

- MISP is an open source software (can be self-hosted or cloud-based) **information sharing and exchange platform**
- It enables analysts from different sectors/orgs to create, collaborate on and share information
- The information shared can then be used to find correlations as well as automatically be fed into **protective tools or processes**
- The software is widely used by CERTs, ISACs, Intelligence Community, military organisations, private sector organisations and researchers since 2012
- CIRCL is both the main driving force behind the tool's **development** as well as some of the largest information **sharing communities** worldwide

MISP - Open Source Threat Intelligence Platform
- MISP is an open source software (can be self-hosted or cloud-based) information sharing and exchange platform
- It enables analysts from different sectors/orgs to create, collaborate on and share information
- The information shared can then be used to find correlations as well as automatically be fed into protective tools or processes
- The software is widely used by CERTs, ISACs, Intelligence Community, military organisations, private sector organisations and researchers since 2012
- CIRCL is both the main driving force behind the tool's development as well as some of the largest information sharing communities worldwide

MISP Project Overview

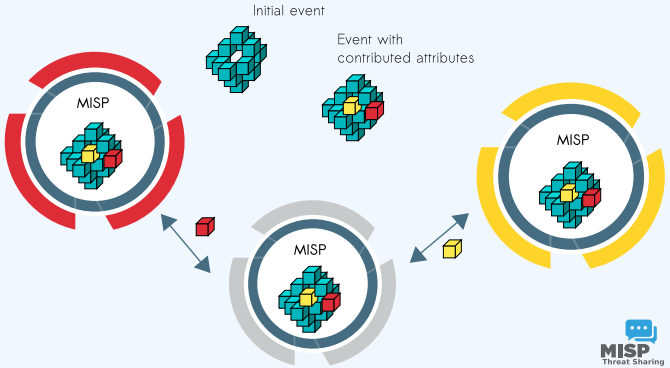


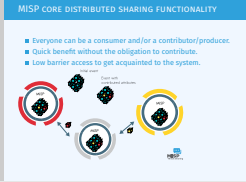


1. The MISP project includes:
2. Software (the MISP core software itself along with supporting libraries such as PyMISP)
3. Contextualisation libraries (to further elaborate on data's relevance, distribution rules, prevention methods, objectives, etc)
4. Best practice guidance (to ensure cohesion within communities and common understanding of the information shared)
5. Compliance guidance (to go into details about how information sharing fits into the various legal frameworks)

MISP CORE DISTRIBUTED SHARING FUNCTIONALITY

- 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.





1. It is important to emphasise the ability and expectations that come with MISP being a sharing platform rather than a feed ingestion platform
2. Whilst sharing is by no means a requirement in most MISP communities, it is a powerful tool to get sector / region specific information out in the community - especially when it leads to comments, improvements and competitve analyses
3. Having a natural growth in usage patterns is expected, getting started is as easy as logging onto a hosted instance and users can scale out to running their own communities and interconnecting with others organically

DFIR and MISP digital evidences

- **Share analysis and report** of digital forensic evidences.
- **Propose changes** to existing analysis or report.
- Extending existing event with additional evidences for local or limited use (sharing can be defined at event level or attribute level).
- **Evaluate correlations**[1] of evidences against external or existing attributes.
- **Report sighting** 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 but also fuzzy hashing (e.g. ssdeep) or CIDR block matching.

DFIR and MISP digital evidences
- **Share analysis and report** of digital forensic evidences.
- **Propose changes** to existing analysis or report.
- Extending existing event with additional evidences for local or limited use (sharing can be defined at event level or attribute level).
- **Evaluate correlations**[1] of evidences against external or existing attributes.
- **Report sighting** 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 but also fuzzy hashing (e.g. ssdeep) or CIDR block matching.

1. Modelling data correctly is essential for finding links to existing data, being able to feed other tools and to have a common understanding of what is meant.

LEA benefits of using MISP

- Leverage the long-standing experience in information sharing
- **Bridge their use-cases** with MISP's information sharing mechanisms
- **Accessing existing MISP information sharing communities** by getting actionable information from CSIRTs/CERTs networks or security researchers.
  - Access to **actionable intelligence** by CSIRT networks
  - Data-sets can be used to support forensic cases
- **Bridging** LE communities with other communities
  - Use **sharing groups** to manage distribution across the communities
  - Safety nets via **synchronisation filters**
  - Possibility to use certain communities as **correlation sources** only

LEA benefits of using MISP
- Leverage the long-standing experience in information sharing
- Bridge their use-cases with MISP's information sharing mechanisms
- Accessing existing MISP information sharing communities by getting actionable information from CSIRTs/CERTs networks or security researchers.
  - Access to actionable intelligence by CSIRT networks
  - Data-sets can be used to support forensic cases
- Bridging LE communities with other communities
  - Use sharing groups to manage distribution across the communities
  - Safety nets via synchronisation filters
  - Possibility to use certain communities as correlation sources only

1. Explain the advantages of receiving and interacting with the data shared in CSIRT networks
2. Cross correlating data can save time at the initial stages of an investigation
3. For forensics cases, determining if a system was compromised before gather evidences is crucial
4. Sharing can be a vehicle for collaboration, asking for support
5. It is easily possible to only exchange the none sensitive, technical subset of the data when engaging CSIRTs

LEA benefits of using MISP

- MISP handles a host of additional tasks around the data received and shared by LEAs:
  - **Normalisation** to ensure reusability
  - **Enrichment** using other services
  - **Correlation** of own cases against community data
  - Conversion to **other formats**
- The **MISP standard format** is extremely flexible
  - Create a new **object template** in under 30 minutes
  - Shared data using custom templates immediately understood by other communities
  - Tight **validation** and **conversions** for building blocks of the custom templates

LEA benefits of using MISP
- MISP handles a host of additional tasks around the data received and shared by LEAs:
  - Normalisation to ensure reusability
  - Enrichment using other services
  - Correlation of own cases against community data
  - Conversion to other formats
- The MISP standard format is extremely flexible
  - Create a new object template in under 30 minutes
  - Shared data using custom templates immediately understood by other communities
  - Tight validation and conversions for building blocks of the custom templates

1. Modelling data correctly is essential for finding links to existing data, being able to feed other tools and to have a common understanding of what is meant.
2. Information in general always evolves over time, be it from new findings, other parties observing similar cases or simply by lookup services offering more relevant information over time.
3. New attack techniques often require new ways of modelling information. The time spent waiting for support in tools for new data models is time lost in effectively sharing the information, custom templating is meant to address this.

Future of Information Sharing

- MISP is a long-term project (started in 2012)
- **Information sharing is becoming more essential** than ever to thwart threats
- Heavy focus on cross-sectorial sharing
- Support emerging threats, such as hybrid threats
- Open tools and standards along with interoperable software (e.g. DFIR tools) are driving forces behind resilient information exchange communities
- Getting ideas and practical **use-cases from LE community** is vital
- Reach out to influence how it evolves!

Future of Information Sharing
- MISP is a long-term project (started in 2012)
- Information sharing is becoming more essential than ever to thwart threats
- Heavy focus on cross-sectorial sharing
- Support emerging threats, such as hybrid threats
- Open tools and standards along with interoperable software (e.g. DFIR tools) are driving forces behind resilient information exchange communities
- Getting ideas and practical use-cases from LE community is vital
- Reach out to influence how it evolves!

1. Something to emphasise here is the emergence of threats spanning multiple disciplines (election interference, fraud involving crypto currencies, etc)
2. Interoperability between organisations and tools if becoming more crucial the more interconnected we are
3. Mention the need for experts to give feedback and input on better modelling strategies, emerging new threats or new classification systems to ensure community cohesion