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/

March 25, 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.

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

Open Source Software

- MISP core
- misp-modules
- PyMISP
- misp-dashboard

Intelligence & Knowledge Base

- misp-taxonomies
- misp-galaxy
- misp-noticelist
- misp-warninglists

Open Standards

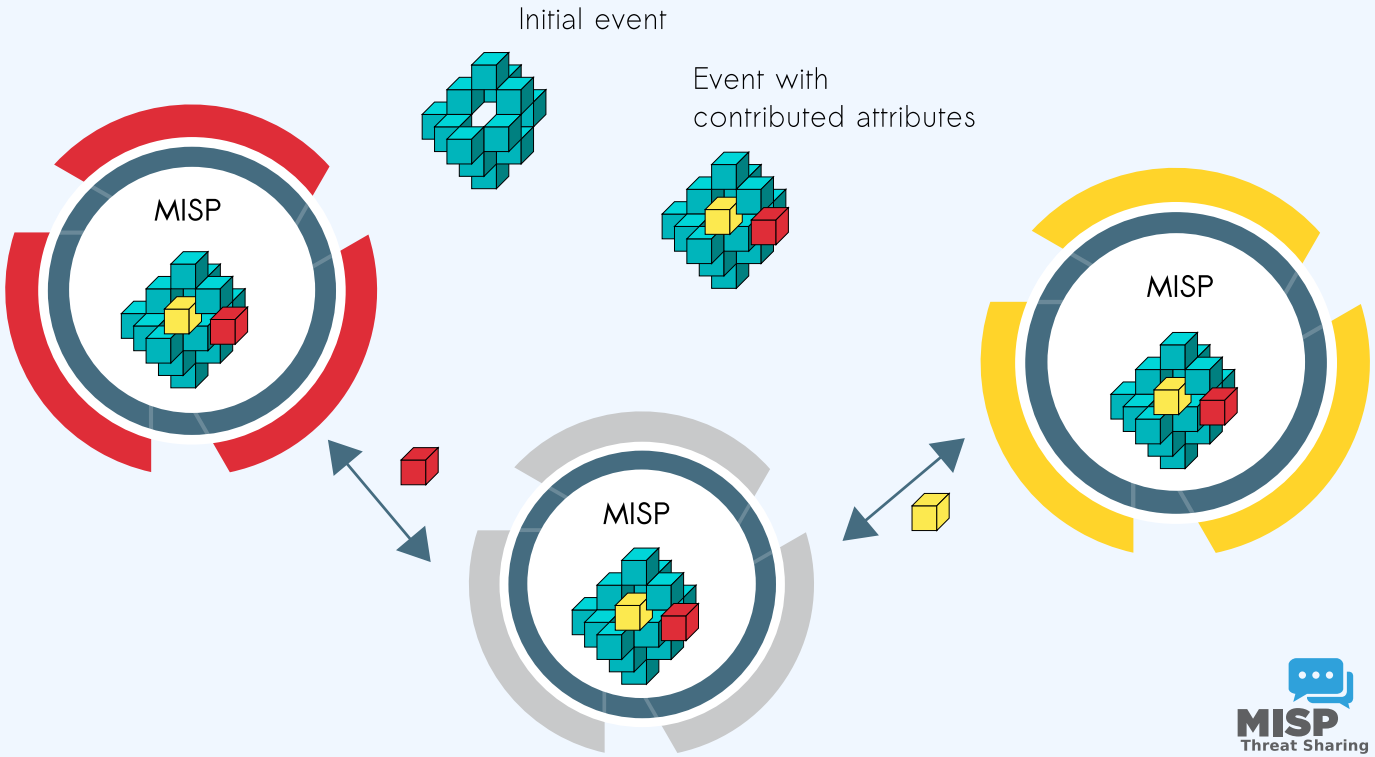
- MISP exchange core format
- MISP objects template

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 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.



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.

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

- 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

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!