MISP - Open Source Threat Intelligence Platform

Supporting Digital Forensic and Incident Response

CIRCL
Computer Incident
Response Center
Luxembourg

Team CIRCL *TLP:WHITE*

16th May 2019

Objectives

- This training is a first step to bring together **forensic analysis, information sharing and information exchange**.
- Your contribution is critical and will help to improve open source software such as MISP and the training materials at large for the LE community.
- **The session is interactive** and we will work together on solving cases, discovering new findings and techniques.

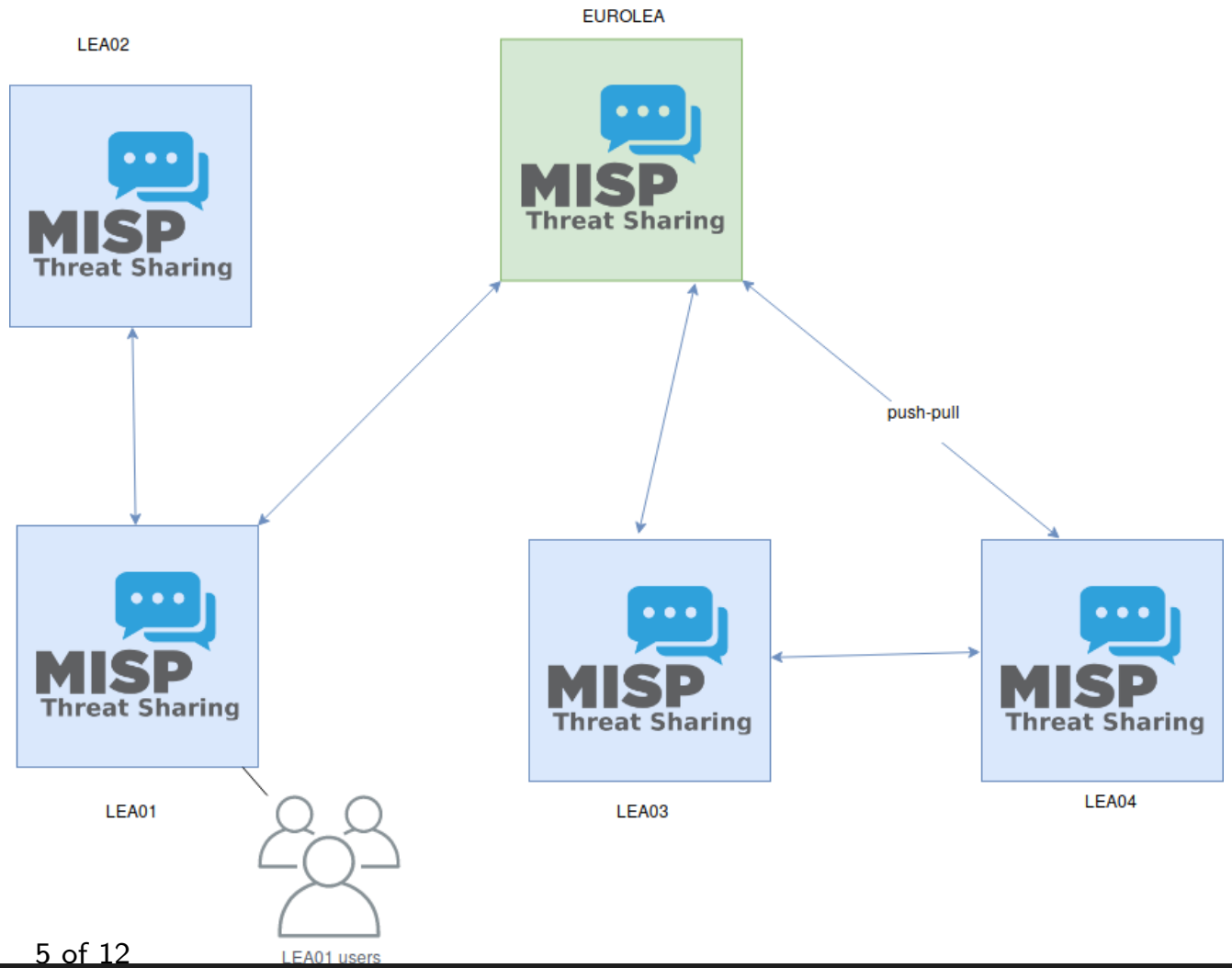
Session

- There are 5 teams (LEA01→LEA04 and EUROLEA).
- A team is composed of one or more analysts.
- Each team has their own MISP instance and each team member has a forensic workstation.
- During the 1 day 1/2 session, there are 3 cases (CASE01→CASE03) to investigate.
- Findings will be shared within a team as a first step and then at later stage between teams.

Agenda

- An introduction to MISP
- CASE 01 - "fake invoicing" Warming-up
- CASE 02 - "We all love ransomware"
- MISP synchronisation and exchange
- CASE 03 - "Something suspicious in the neighbourghood"

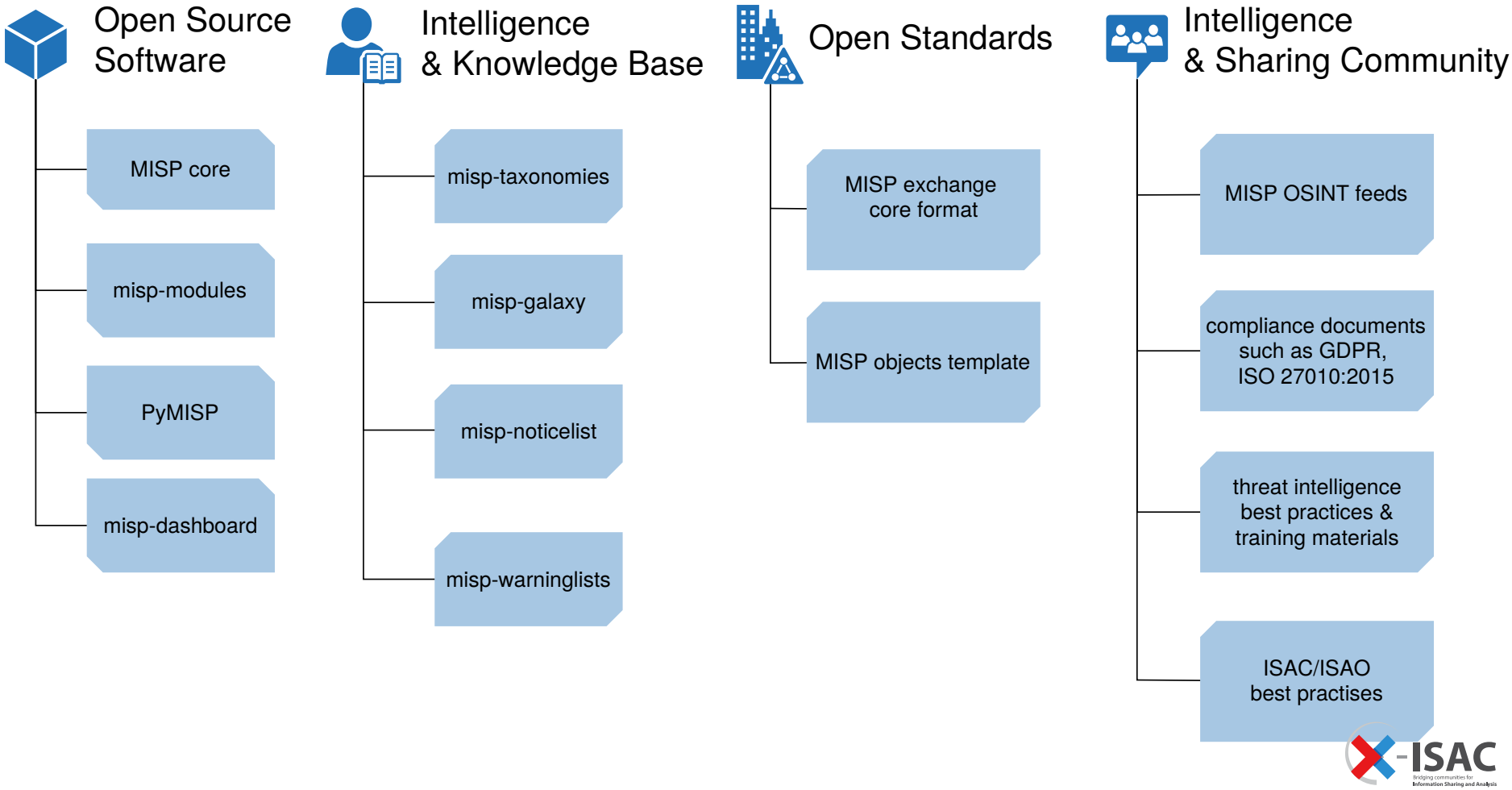
MISP Enforce training target setup



MISP - Open Source Threat Intelligence Platform

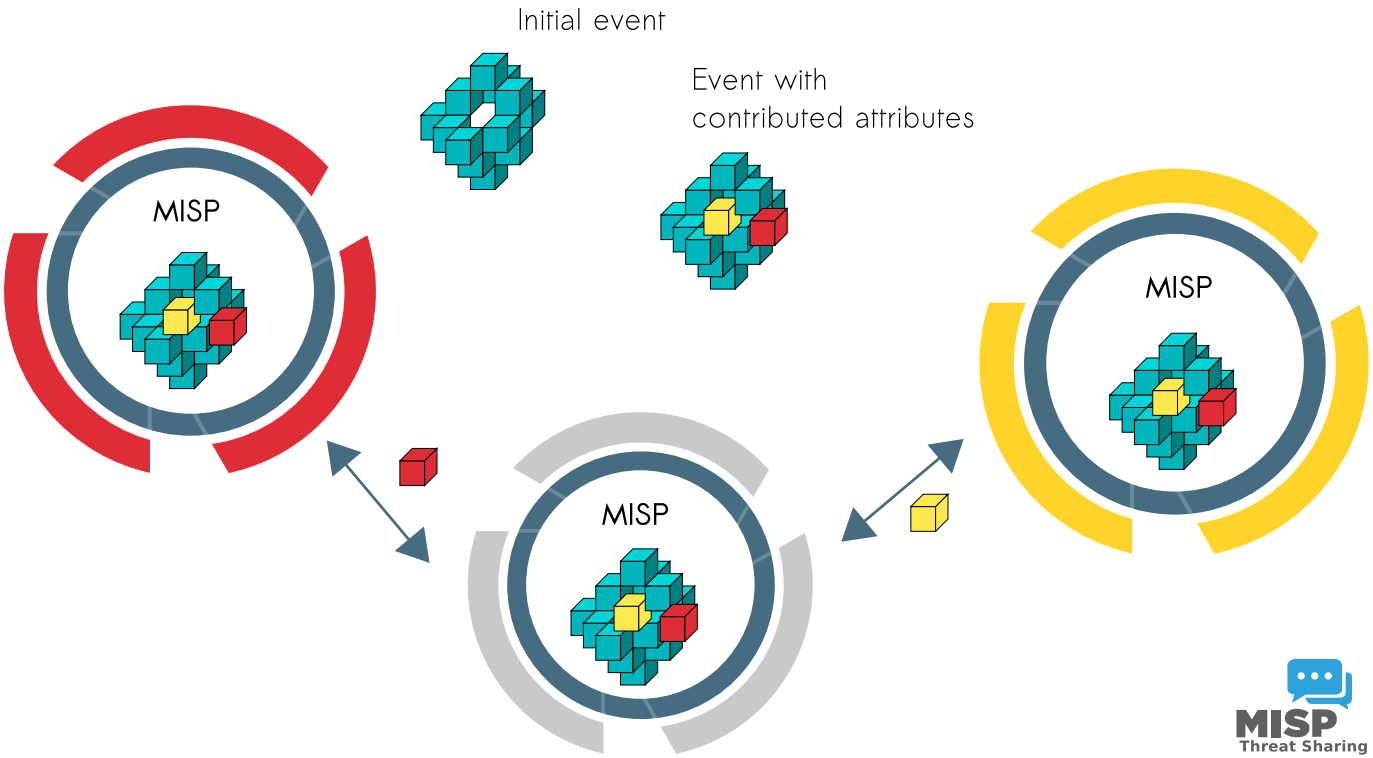
- MISP is an open source software (can be self-hosted or cloud-based) **information sharing and exchange platform**
- It enables analysts from different sectors/orgs to create, collaborate on and share information
- The information shared can then be used to find correlations as well as automatically 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



MISP core distributed sharing functionality

- MISP's 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.



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.

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 getting actionable information from CSIRTs/CERTs networks or security researchers.
- **Bridging LE communities with other communities**. Sharing groups can be created (and managed) between cross-sectors to support specific use-cases.
- **MISP standard format** is a flexible format which can be extended by the users who use the MISP platform. A MISP object template can be created in 30 minutes and directly share information with your model towards existing communities.

Future of Information Sharing

- MISP is a long-term project (started in 2012) and since **information sharing is becoming more essential** than ever to thwart threats, we have long-term plans for the project as the project is used in various critical information exchange communities.
- We hope to have the means to be the enablers and the interface for real cross-sectorial sharing and support the organisations facing hybrid threats.
- Tools, open standards and 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, don't hesitate to interact.

- Contact: info@circl.lu
- `https://www.circl.lu/`
- `https://www.misp-project.org/`
- `https://github.com/MISP` - `https://twitter.com/MISPProject`
- Don't hesitate to get in touch with us to access one of our sharing community or feedback to improve MISP.