MISP - Open Source Threat Intelligence Platform
Supporting Digital Forensic, Incident Response and Information Exchange

Team CIRCL  TLP:WHITE

2nd April 2019
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 practices
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

• Customs administration 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 Customs/border control 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.
Functionalities in MISP for customs and border control

- **Information sharing of travel documents** / biometric information between border control agencies. Exchange structured information on any Natural person of interest with border control agents.
- MISP includes **pre-defined types such PNR** (passenger name record) as used by the DHS/TSA.
- Sharing of information / involving experts for the identification of smuggled goods (e.g. **cultural goods or specific goods where expertise is required**).
- Anonymised lookups against exported data sets of the above information (e.g. offline border control check).
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 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 border control community is vital, don’t hesitate to contact us.
• 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.