An Introduction to Cybersecurity Information Sharing

MISP - Threat Sharing

Alexandre Dulaunoy

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

University of Lorraine

MISP
Threat Sharing

- (09:00 - 10:30) Introduction to Information Sharing with MISP
- (10:45 - 12:30) Best practices in threat intelligence

- 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**.

The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents. CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg and is operated by securitymadein.lu g.i.e.

- CIRCL is mandated by the Ministry of Economy and acting as the Luxembourg National CERT for private sector.
- CIRCL leads the development of the Open Source MISP threat intelligence platform which is used by many military or intelligence communities, private companies, financial sector, National CERTs and LEAs globally.
- **CIRCL runs multiple large MISP communities performing active daily threat-intelligence sharing**.

Co-financed by the European Union
Connecting Europe Facility

- 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, likelihood and occurences.
  - ▶ **Fraud analysts** willing to share financial indicators to detect financial frauds.
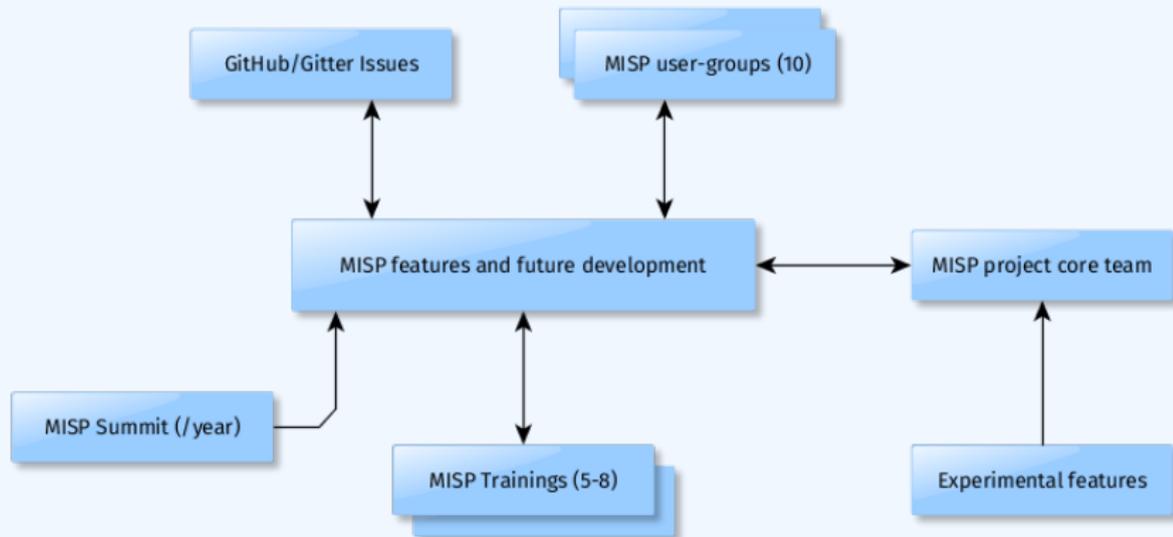
- Sharing indicators for a **detection** matter.
  - ▶ 'Do I have infected systems in my infrastructure or the ones I operate?'
- Sharing indicators to **block**.
  - ▶ 'I use these attributes to block, sinkhole or divert traffic.'
- Sharing indicators to **perform intelligence**.
  - ▶ 'Gathering information 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/`
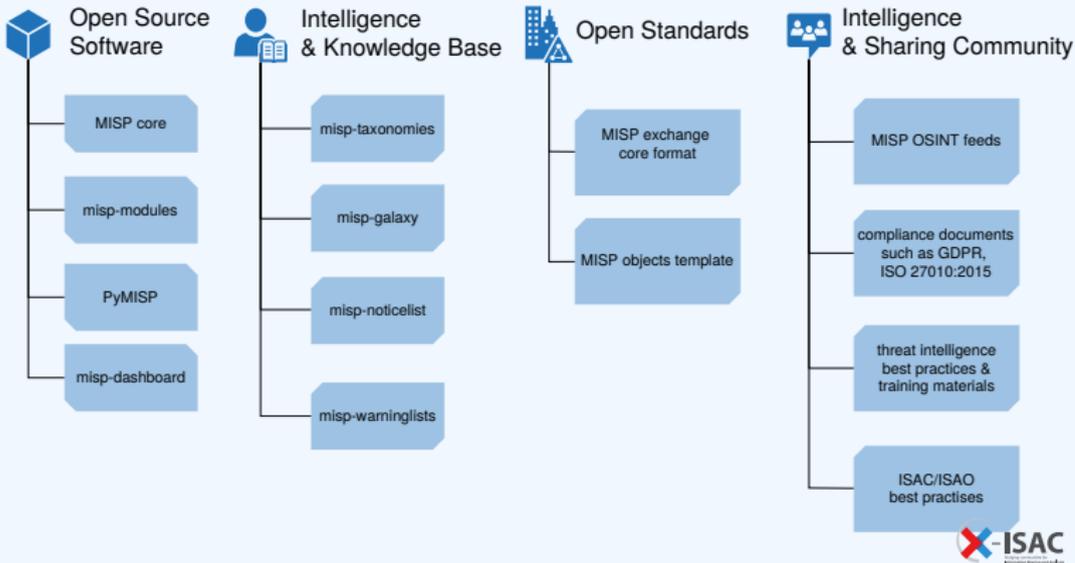
- MISP[2] is a threat information sharing free & open source software.
- MISP has **a host of functionalities** that assist users in creating, collaborating & sharing threat information - e.g. flexible sharing groups, **automatic correlation**, free-text import helper, event distribution & proposals.
- 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).
- A rich set of MISP modules[3] to add expansion, import and export functionalities.

---

[2]https://github.com/MISP/MISP
[3]https://www.github.com/MISP/misp-modules
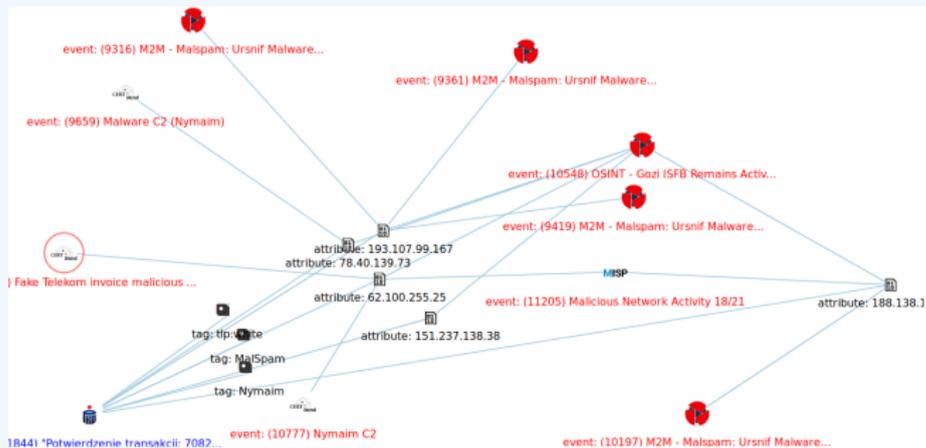
- To **corroborate a finding** (e.g. is this the same campaign?), **reinforce an analysis** (e.g. do other analysts have the same hypothesis?**), confirm a specific aspect** (e.g. are the sinkhole IP addresses used for one campaign?) or just find if this **threat is new or unknown in your community**.

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.
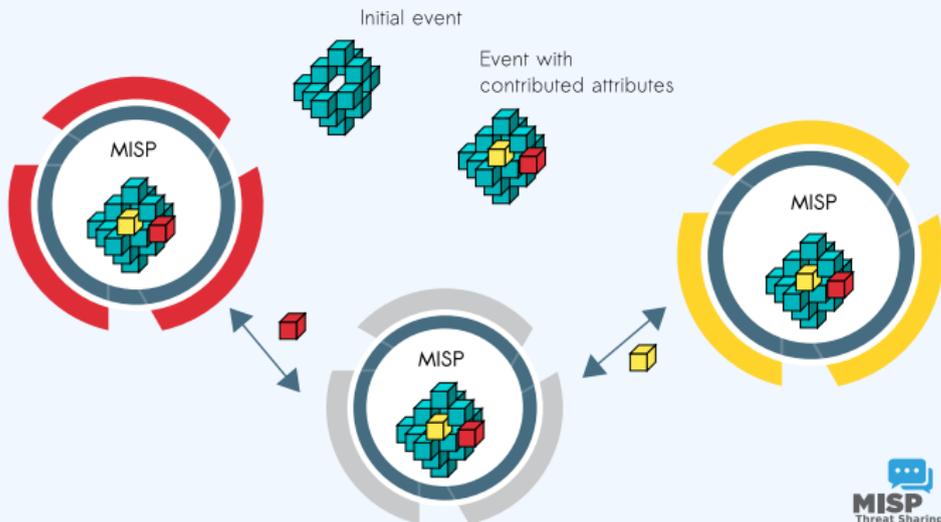
Events, Objects and Attributes in MISP

- MISP events are encapsulations for contextually linked information
- MISP attributes[4] initially started with a standard set of "cyber security" indicators.
- MISP attributes are purely **based on usage** (what people and organizations use daily).
- Evolution of MISP attributes is based on practical usage & users (e.g. the addition of **financial indicators** in 2.4).
- MISP objects are attribute compositions describing points of data using many facets, constructed along the lines of community and user defined templates.
- Galaxies granularly contextualise, classify & categorise data based on **threat actors**, **preventive measures**, tools used by adversaries.

[4]attributes can be anything that helps describe the intent of the event package from indicators, vulnerabilities or any relevant information

- Indicators[5]
  - ▶ Indicators contain a pattern that can be used to detect suspicious or malicious cyber activity.
- Attributes in MISP can be network indicators (e.g. IP address), system indicators (e.g. a string in memory) or even bank account details.
  - ▶ **A type (e.g. MD5, url) is how an attribute is described**.
  - ▶ An attribute is always in a category (e.g. Payload delivery) which puts it in a context.
    - **A category is what describes** an attribute.
  - ▶ An IDS flag on an attribute allows to determine if **an attribute can be automatically used for detection**.

---

[5]IoC (Indicator of Compromise) is a subset of indicators

- MISP integrates at event or attribute level MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK).

27

Supporting specific datamodel

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**.

Example: Freetext import in MISP

Supporting Classification

- Tagging is a simple way to attach a classification to an event or an attribute.
- **Classification must be globally used to be efficient**.
- MISP includes a flexible tagging scheme where users can select from more than 42 existing taxonomies or create their own taxonomy.

Supporting Sharing in MISP

- Delegate events publication to another organization (introduced in MISP 2.4.18).
  - ▶ The other organization can take over the ownership of an event and provide **pseudo-anonymity to initial organization**.
- Sharing groups allow custom sharing (introduced in MISP 2.4) per event or even at attribute level.
  - ▶ Sharing communities can be used locally or even cross MISP instances.
  - ▶ **Sharing groups** can be done at **event level or attributes level** (e.g. financial indicators shared to a financial sharing groups and cyber security indicators to CSIRT community).

- Sightings allow users to notify the community about the activities related to an indicator.
- In recent MISP versions, the sighting system supports negative sigthings (FP) and expiration sightings.
- Sightings can be performed via the API, and the UI, even including the import of STIX sighting documents.
- Many use-cases for scoring indicators based on users sighting.

IMPROVING INFORMATION SHARING IN MISP

- False-positives are a recurring challenge in information sharing.
- In MISP 2.4.39, we introduced the misp-warninglists[6] to help analysts in their day-to-day job.
- Predefined lists of well-known indicators which are often false-positives like RFC1918 networks, public DNS resolver are included by default.

---

[6]https://github.com/MISP/misp-warninglists

Improving support of sharing within and outside an organization

- Even in a single organization, multiple use-cases of MISP can appear (groups using it for dynamic malware analysis correlations, dispatching notification).
- In MISP 2.4.51, we introduced the ability to have **local MISP** servers connectivity to avoid changes in distribution level. This allows to have mixed synchronization setup within and outside an organization.
- Feed support was also introduced to support synchronization between untrusted and trusted networks.

Bootstrapping MISP with indicators

- We maintain the default CIRCL OSINT feeds (TLP:WHITE selected from our communities) in MISP to allow users to ease their bootstrapping.
- The format of the OSINT feed is based on standard MISP JSON output pulled from a remote TLS/HTTP server.
- Additional content providers can provide their own MISP feeds. (`https://botvrij.eu/`)
- Allows users to **test their MISP installations and synchronisation with a real dataset**.
- Opening contribution to other threat intel feeds but also allowing the analysis of overlapping data[7].

---

[7]A recurring challenge in information sharing

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.
- MISP project combines open source software, open standards, best practices and communities to make information sharing a reality.

MISP User Experience Survey

A researcher–Borce STOJKOVSKI–from University of Luxembourg (SnT) is conducting a survey about MISP UX.

- You may participate at the following location:
  `https://misp-project.org/ux-survey`
- on-voluntary basis: opt-out at any time,
- results will be communicated back to the community and used to improve MISP's User Interface,
- for any inquiries contact ux@misp-project.org