An Introduction to Cybersecurity Information Sharing
MISP - Threat Intelligence Sharing Platform

Alexandre Dulaunoy
TLP: WHITE

http://www.misp-project.org/
Twitter: @MISPProject

CENTR 11th CENTR R&D workshop
20171016
MISP and starting from a practical use-case

- 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.
Development based on practical user feedback

- 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 occurrences.
  - **Fraud analysts** willing to share financial indicators to detect financial frauds.
MISP model of governance
Many objectives from different user-groups

- 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
  - "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."
MISP Project Overview

- The **core project** (PHP/Python) supports the backend, API and UI.
- Modules (Python) to expand MISP functionalities.
- Taxonomies (JSON) to add categories and global tagging.
- Warning-lists (JSON) to help analysts to detect potential false-positives.
- Galaxy (JSON) to add threat-actors, tools or "intelligence".
- Objects (JSON) to allow for templated composition of security related atomic points of information.

\[^a\]
MISP features

- MISP\(^1\) is an IOC and threat information sharing free and open source software.
- MISP has many functionalities e.g. flexible sharing groups, automatic correlation, free-text import helper, event distribution and collaboration.
- 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)
- After some years of trial-and-error, we explain the background behind current and new MISP features.

\(^{1}\) https://github.com/MISP/MISP
Communities using MISP

- Communities are group of users sharing within a set of common objectives/values.
- CIRCL operates multiple MISP instances with a significant user base (more than 700 organizations with more than 1600 users).
- **Trusted groups** running MISP communities in island mode 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

- 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.
Events and Attributes in MISP

- MISP attributes 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 and users (e.g. recent addition of the financial indicators in 2.4).
- MISP galaxy recently introduced to support additional descriptions like threat actors, preventive measures or tools used by adversaries.
- MISP objects added to give the freedom to the community to create new and combined attributes and share them.

\(^2\)attributes can be anything that helps describe the intent of the event package from indicators, vulnerabilities or any relevant information
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 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 support

- Sightings allow users to notify the community about the activities related to an indicator.
- In recent MISP version, sighting supports negative sighting (FP) and expiration sighting.
- Sightings can be performed via API, and UI including import of STIX sighting documents.
- Many use-cases opportunities in scoring indicators based on users sighting.
Improving Information Sharing in MISP

• False-positive is a recurring challenge in information sharing.
• In MISP 2.4.39, we introduced the misp-warninglists\(^3\) 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.

\(^3\)https://github.com/MISP/misp-warninglists
Feeds and comparing overlap

• MISP feeds (from remote url or file) have been completely rewritten to allow **caching of feeds** without importing these into MISP.

• So you can browse, cache and correlate information from feeds directly in your MISP instances. A feed overlap matrix feature is also available to compare the feeds in MISP.
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 (e.g. domain-abuse taxonomy).