An Introduction to Cybersecurity Information Sharing

MISP - Malware Information Sharing Platform & Threat Sharing

CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy
Andras Iklody
Raphaël Vinot

TLP:WHITE

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

January 12, 2018

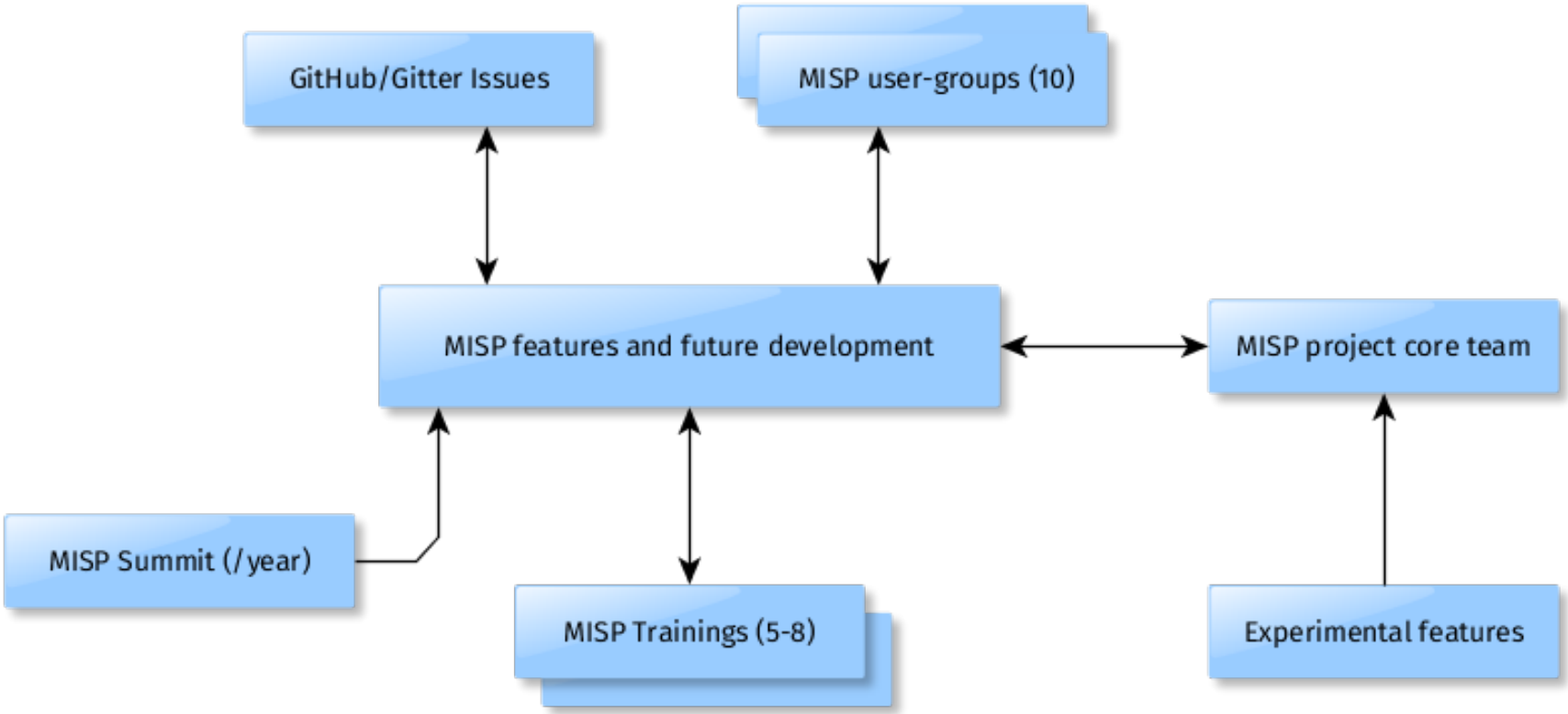
MISP and starting from a practical use-case

- 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, likelyhood and occurences.
  - **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?'
- $\rightarrow$ 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

Galaxy

warning-lists

Taxonomies

modules (import, export, enrichment)

- The **core project**[a] (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.

MISP features

- MISP[1] is a threat information sharing free and open source software.
- MISP has **a host of functionalities** that assist users in creating, collaborating and sharing threat information - e.g. flexible sharing groups, **automatic correlation**, free-text import helper, event distribution and 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)
- After some years of trial-and-error, we explain the background behind current and new **MISP features**.

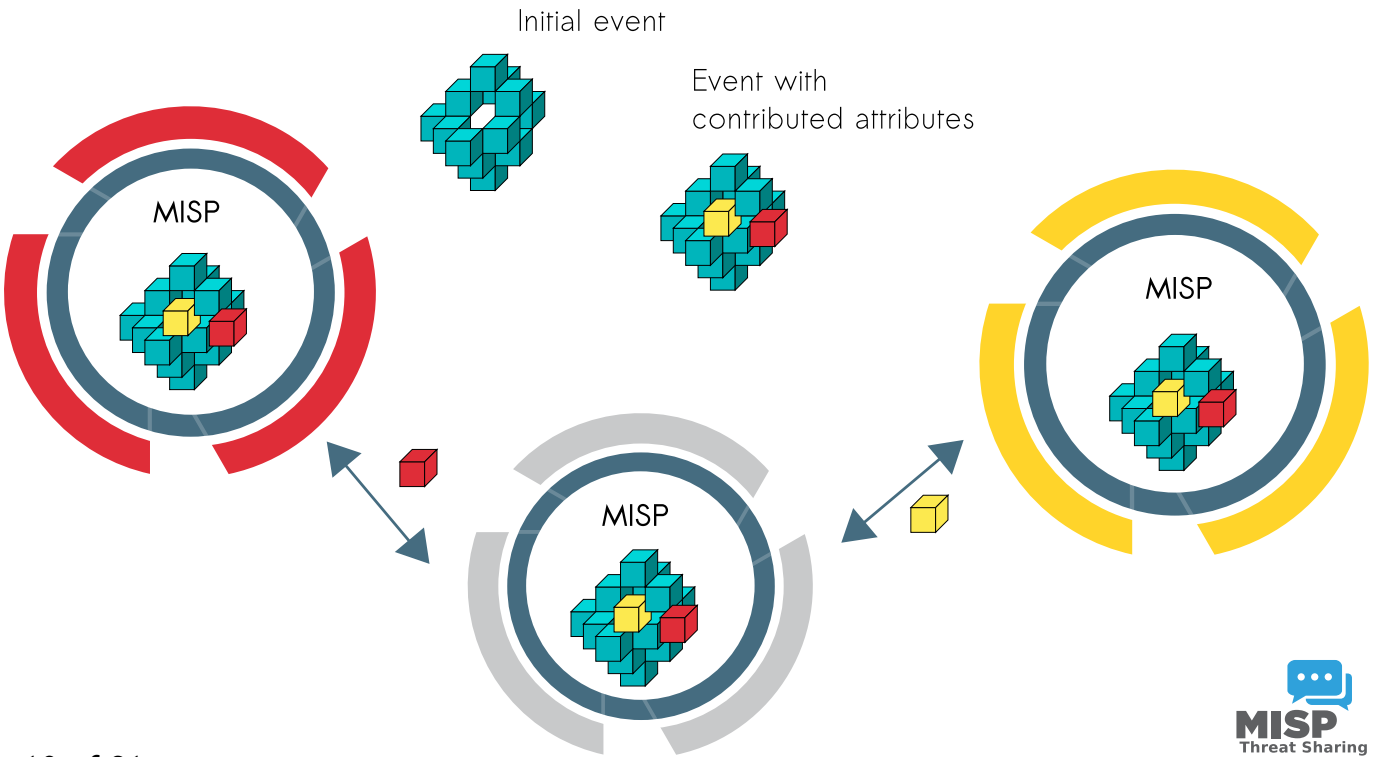
[1] https://github.com/MISP/MISP

Communities using MISP

- Communities are groups of users sharing within a set of common objectives/values.
- CIRCL operates multiple MISP instances with a significant user base (more than 800 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, Objects and Attributes in MISP

- MISP events are encapsulations for contextually linked information
- MISP attributes[2] 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 objects are attribute compositions describing points of data using many facets, constructed along the lines of community and user defined templates
- MISP galaxies granularly contextualise, classify and categorise data based on **threat actors**, **preventive measures** or tools used by adversaries.

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

Terminology about Indicators

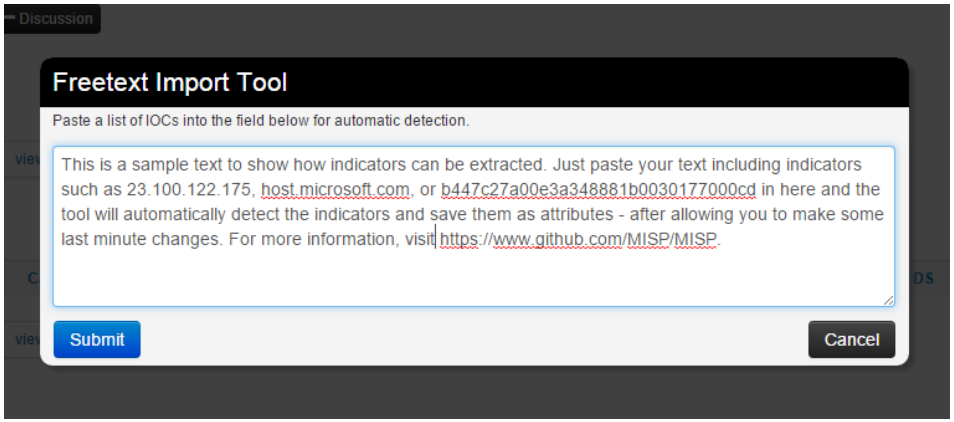
- Indicators[3]
  - Indicators contain a pattern that can be used to detect suspicious or malicious cyber activity.
- Attributes in MISP can be network indicators (e.g. IP address), system indicators (e.g. a string in memory) or even bank account details.
  - **A type (e.g. MD5, url) is how an attribute 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**.

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

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



Freetext Import Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic resolution.

Value	Category	Type	IDS	Comment	Actions
23.100.122.175	Network activity	ip-dst	☑	Imported via the freetext import.	✖
host.microsoft.com	Network activity	hostname	☑	Imported via the freetext import.	✖
b447c27a00e3a348881b0030177000cd	Payload delivery	md5	☑	Imported via the freetext import.	✖
https://www.github.com/MISP/MISP	Network activity	url	☑	Imported via the freetext import.	✖

Submit

ip-dst → ip-src Change all

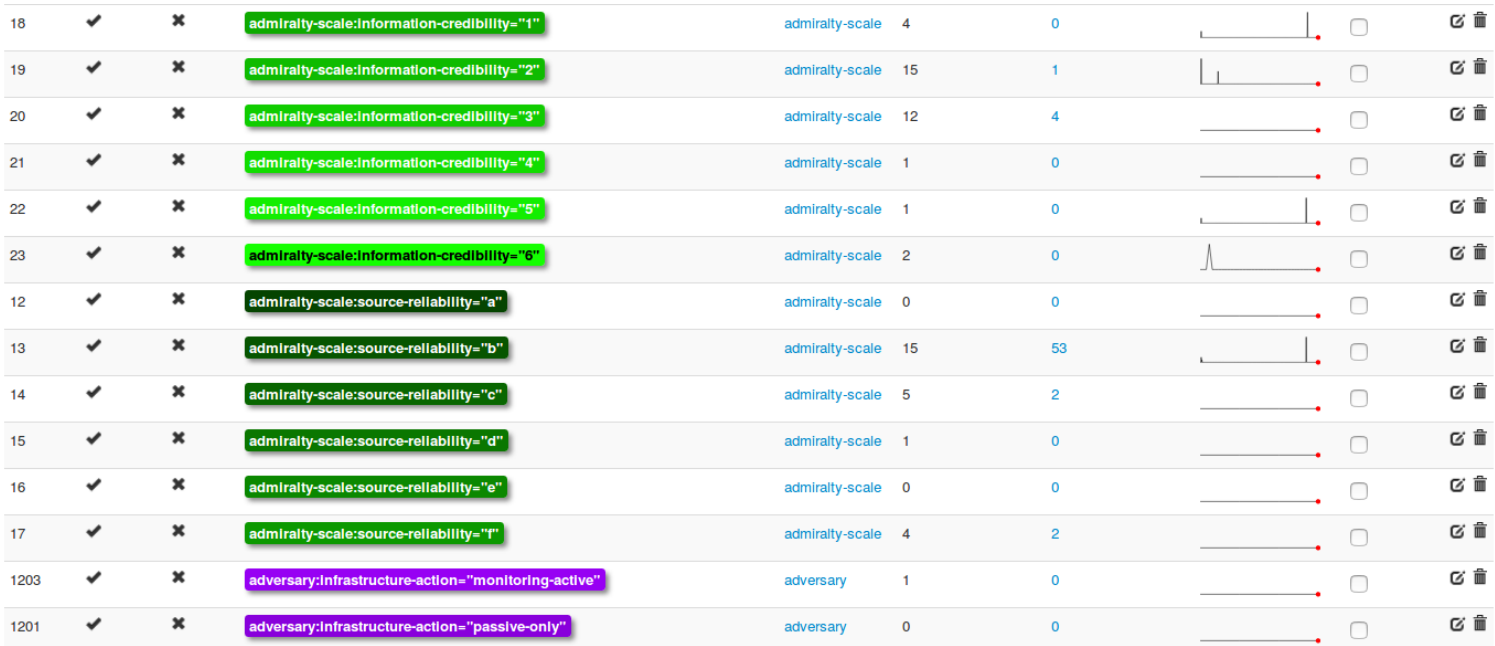
Update all comment fields Change all

Filters: All File Network Financial Proposal Correlation

Date	Org	Category	Type	Value	Comment	Related Events	IDS	Distribution	Actions
2016-02-24		Network activity	hostname	host.microsoft.com	Imported via the freetext import.		Yes	Inherit	
2016-02-24		Network activity	ip-dst	23.100.122.175	Imported via the freetext import.	298	Yes	Inherit	
2016-02-24		Network activity	url	https://www.github.com/MISP/MISP	Imported via the freetext import.		Yes	Inherit	
2016-02-24		Payload delivery	md5	b447c27a00e3a348881b0030177000cd	Imported via the freetext import.		Yes	Inherit	

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.

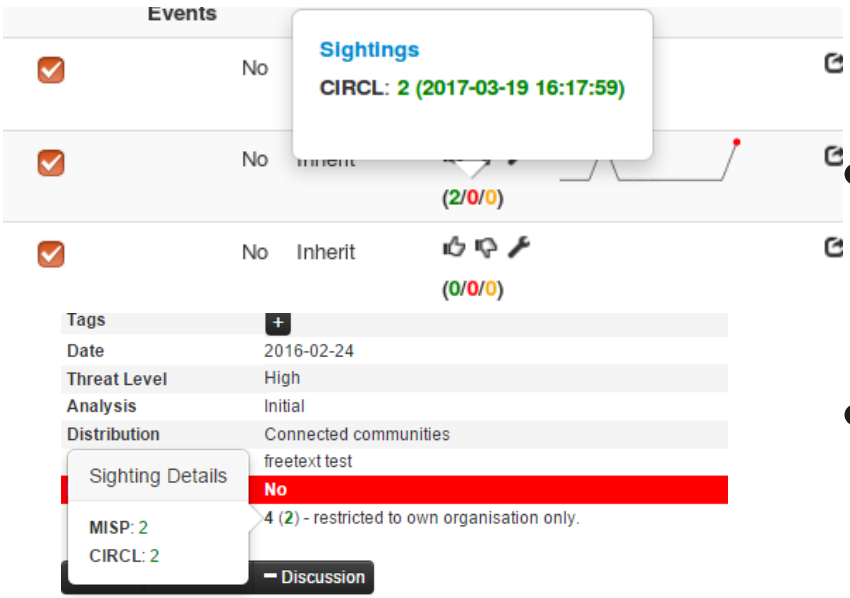


18	✔	✖	admiralty-scale:information-credibility="1"	admiralty-scale	4	0		
19	✔	✖	admiralty-scale:information-credibility="2"	admiralty-scale	15	1		
20	✔	✖	admiralty-scale:information-credibility="3"	admiralty-scale	12	4		
21	✔	✖	admiralty-scale:information-credibility="4"	admiralty-scale	1	0		
22	✔	✖	admiralty-scale:information-credibility="5"	admiralty-scale	1	0		
23	✔	✖	admiralty-scale:information-credibility="6"	admiralty-scale	2	0		
12	✔	✖	admiralty-scale:source-reliability="a"	admiralty-scale	0	0		
13	✔	✖	admiralty-scale:source-reliability="b"	admiralty-scale	15	53		
14	✔	✖	admiralty-scale:source-reliability="c"	admiralty-scale	5	2		
15	✔	✖	admiralty-scale:source-reliability="d"	admiralty-scale	1	0		
16	✔	✖	admiralty-scale:source-reliability="e"	admiralty-scale	0	0		
17	✔	✖	admiralty-scale:source-reliability="f"	admiralty-scale	4	2		
1203	✔	✖	adversary:Infrastructure-action="monitoring-active"	adversary	1	0		
1201	✔	✖	adversary:Infrastructure-action="passive-only"	adversary	0	0		

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 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[4] 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.

[4] 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[5].

[5] 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.