An Introduction to Cybersecurity Information Sharing

MISP - Threat Sharing

CIRCL / Team MISP Project

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

MISP Project

An Introduction to Cybersecurity Information Sharing
MISP - Threat Sharing
CIRCL / Team MISP Project
MISP Project
https://www.misp-project.org/
MISP Project
MISP
Threat Sharing

Agenda

- Agenda and details available
  https://www.foo.be/cours/dess-20232024/

Agenda
Agenda and details available
https://www.foo.be/cours/dess-20232024/

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**.

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**.

ABOUT CIRCL

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.

ABOUT CIRCL
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.

MISP and CIRCL

- 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

MISP and CIRCL
- 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

What is MISP?

- MISP is a **threat information sharing** platform that is free & open source software
- A tool that **collects** information from partners, your analysts, your tools, feeds
- Normalises, **correlates**, **enriches** the data
- Allows teams and communities to **collaborate**
- **Feeds** automated protective tools and analyst tools with the output

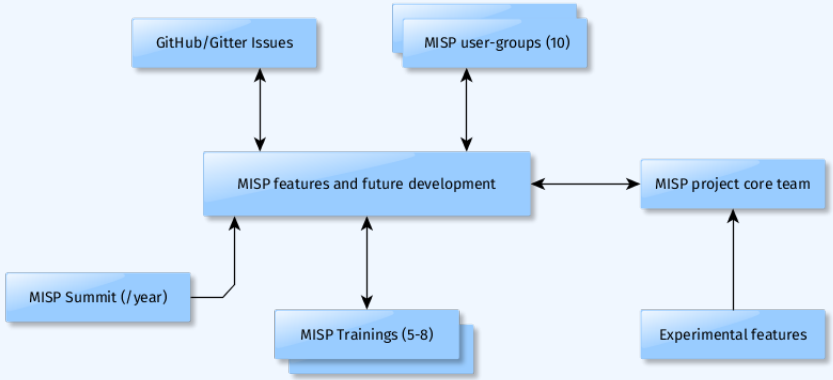
What is MISP?
- MISP is a **threat information sharing** platform that is free & open source software
- A tool that **collects** information from partners, your analysts, your tools, feeds
- Normalises, **correlates**, **enriches** the data
- Allows teams and communities to **collaborate**
- **Feeds** automated protective tools and analyst tools with the output

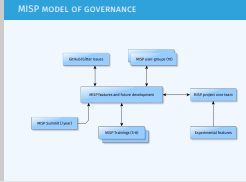
Development based on practical user feedback

- 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.

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)

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)

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 1200 organizations with more than 4000 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).
- **Topical communities** set up to tackle individual specific issues (COVID-19 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 1200 organizations with more than 4000 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).
- **Topical communities** set up to tackle individual specific issues (COVID-19 MISP)

Sharing Difficulties

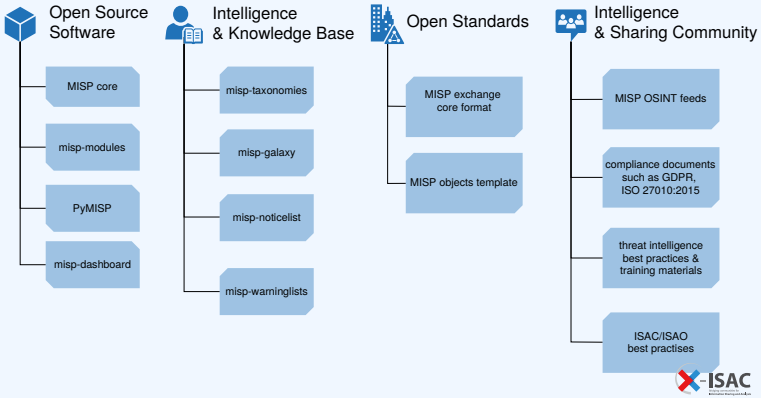
- Sharing difficulties are not really technical issues but often it's a matter of **social interactions** (e.g. **trust**).
- Legal restriction[1]
  - "Our legal framework doesn't allow us to share information."
  - "Risk of information-leak is too high and it's too risky for our organization or partners."
- 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/

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/

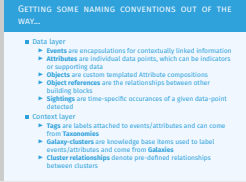
MISP Project Overview



MISP Project Overview

Getting some naming conventions out of the way...

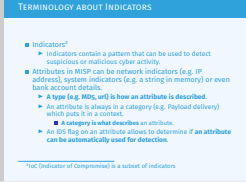
- Data layer
  - **Events** are encapsulations for contextually linked information
  - **Attributes** are individual data points, which can be indicators or supporting data
  - **Objects** are custom templated Attribute compositions
  - **Object references** are the relationships between other building blocks
  - **Sightings** are time-specific occurances of a given data-point detected
- Context layer
  - **Tags** are labels attached to events/attributes and can come from **Taxonomies**
  - **Galaxy-clusters** are knowledge base items used to label events/attributes and come from **Galaxies**
  - **Cluster relationships** denote pre-defined relationships between clusters



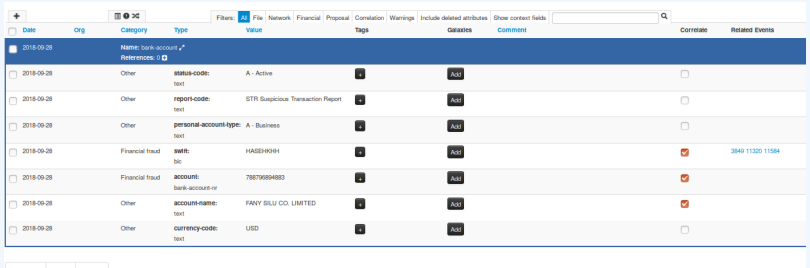
Terminology about Indicators

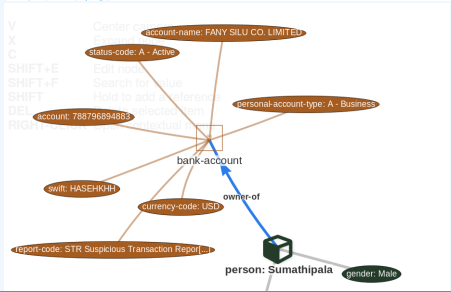
- Indicators[2]
  - Indicators contain a pattern that can be used to detect suspicious or malicious cyber activity.
- Attributes in MISP can be network indicators (e.g. IP address), system indicators (e.g. a string in memory) or even bank account details.
  - **A type (e.g. MD5, url) is how an attribute 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**.

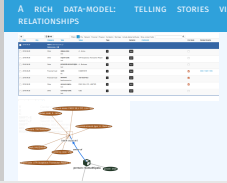
[2] IoC (Indicator of Compromise) is a subset of indicators



A RICH DATA-MODEL: TELLING STORIES VIA RELATIONSHIPS

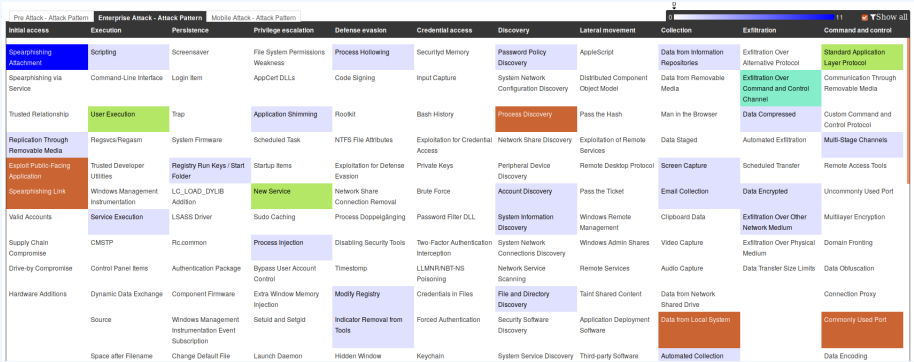


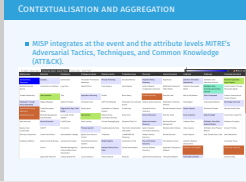




Contextualisation and aggregation

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





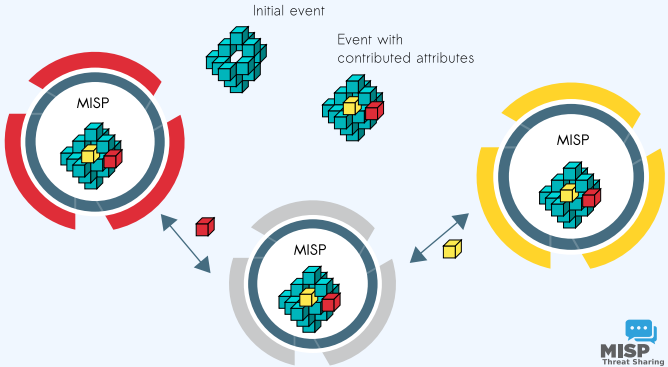
Sharing in MISP

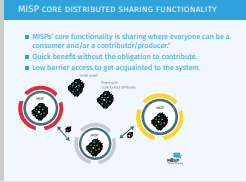
- Sharing via distribution lists - **Sharing groups**
- **Delegation** for pseudo-anonymised information sharing
- **Proposals** and **Extended events** for collaborated information sharing
- Synchronisation, Feed system, air-gapped sharing
- User defined **filtered sharing** for all the above mentioned methods
- Cross-instance information **caching** for quick lookups of large data-sets
- Support for multi-MISP internal enclaves

Sharing in MISP
- Sharing via distribution lists - **Sharing groups**
- **Delegation** for pseudo-anonymised information sharing
- **Proposals** and **Extended events** for collaborated information sharing
- Synchronisation, Feed system, air-gapped sharing
- User defined **filtered sharing** for all the above mentioned methods
- Cross-instance information **caching** for quick lookups of large data-sets
- Support for multi-MISP internal enclaves

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.



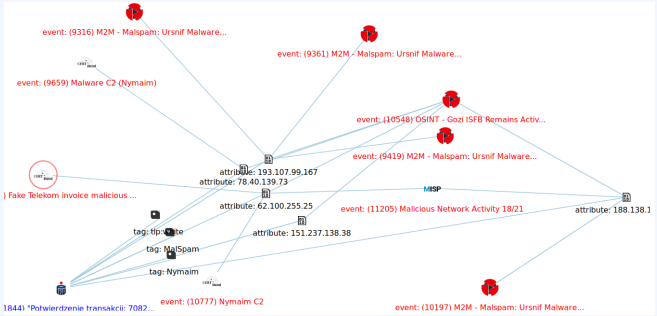


Information quality management

- Correlating data
- Feedback loop from detections via **Sightings**
- **False positive management** via the warninglist system
- **Enrichment system** via MISP-modules
- **Integrations** with a plethora of tools and formats
- Flexible **API** and support **libraries** such as PyMISP to ease integration
- **Timelines** and giving information a temporal context
- Full chain for **indicator life-cycle management**

Information quality management
- Correlating data
- Feedback loop from detections via **Sightings**
- **False positive management** via the warninglist system
- **Enrichment system** via MISP-modules
- **Integrations** with a plethora of tools and formats
- Flexible **API** and support **libraries** such as PyMISP to ease integration
- **Timelines** and giving information a temporal context
- Full chain for **indicator life-cycle management**

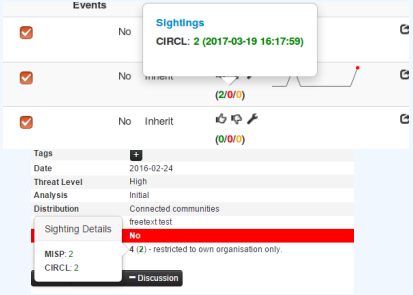
Correlation features: a tool for analysts



- 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**.

Correlation features: a tool for analysts
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.

Sightings support

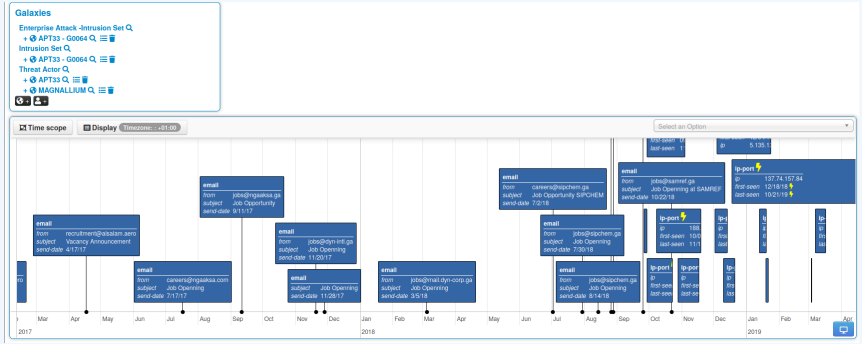


- Has a data-point been **sighted** by me or the community before?
- Additionally, the sighting system supports negative sigthings (FP) and expiration sightings.
- Sightings can be performed via the API or the UI.
- Many use-cases for **scoring indicators** based on users sighting.
- For large quantities of data, **SightingDB** by Devo

Sightings support
- Has a data-point been **sighted** by me or the community before?
- Additionally, the sighting system supports negative sigthings (FP) and expiration sightings.
- Sightings can be performed via the API or the UI.
- Many use-cases for **scoring indicators** based on users sighting.
- For large quantities of data, **SightingDB** by Devo

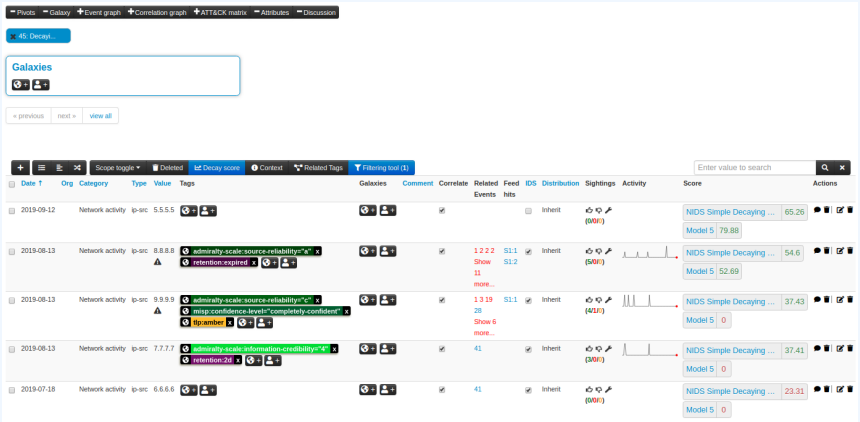
Timelines and giving information a temporal context

- Recently introduced **`first_seen`** and **`last_seen`** data points
- All data-points can be placed in time
- Enables the **visualisation** and **adjustment** of indicators timeframes

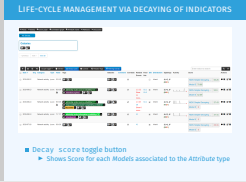


Timelines and giving information a temporal context
Recently introduced first_seen and last_seen data points
All data-points can be placed in time
Enables the visualisation and adjustment of indicators timeframes

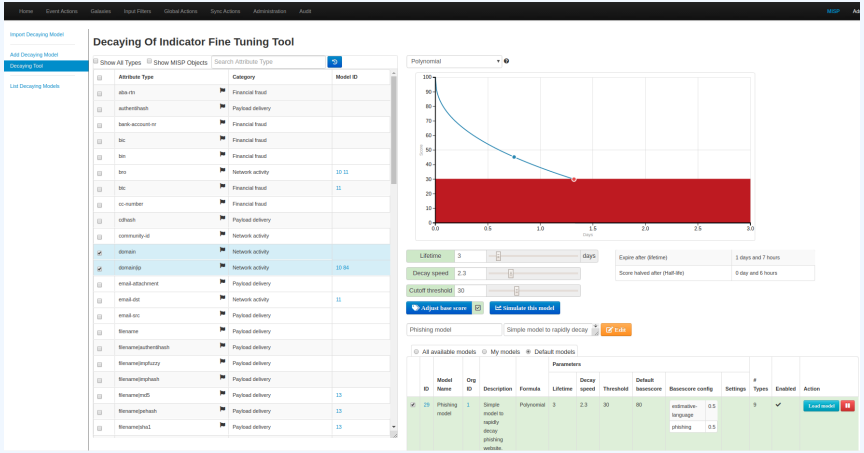
Life-cycle management via decaying of indicators



- Decay score toggle button
  - Shows Score for each *Models* associated to the *Attribute* type



Decaying of indicators: Fine tuning tool

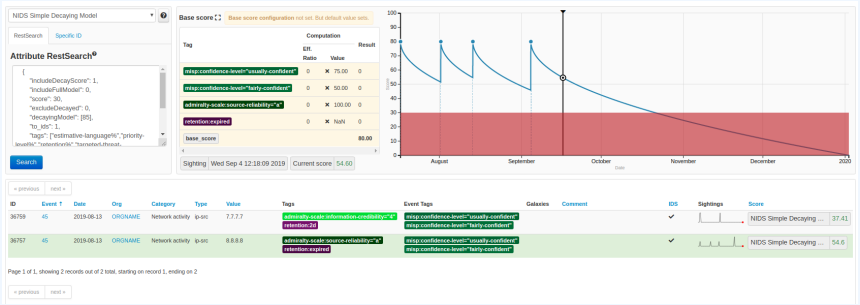


Create, modify, visualise, perform mapping

Decaying of indicators: Fine tuning tool

Create, modify, visualise, perform mapping

Decaying of indicators: simulation tool



Simulate *Attributes* with different *Models*

Decaying of indicators: simulation tool

Simulate Attributes with different Models

Bootstrapping your MISP with data

- 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[3].

[3] A recurring challenge in information sharing

Bootstrapping your MISP with data
- 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[3].
[3] 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.

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.