MISP Project and ISACs

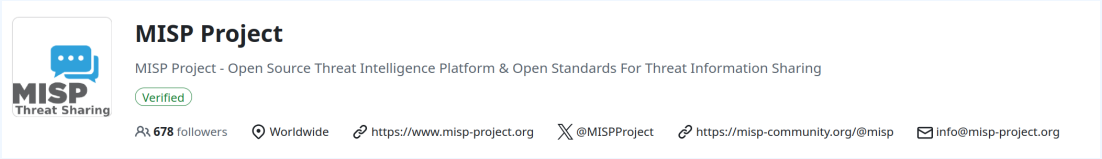
A Versatile Open Source Information Sharing Platform

Team CIRCL

TLP:WHITE

13th ENISA-EC3 Workshop

$whoarewe - MISP AND CIRCL



- CIRCL is mandated by the Ministry of Economy
- CIRCL leads the development of MISP.
- **CIRCL runs multiple large MISP communities performing active daily threat-intelligence sharing**.
- Funding is from LU, several EU programs and partnerships (EU/US) agreements.

Plan of this session

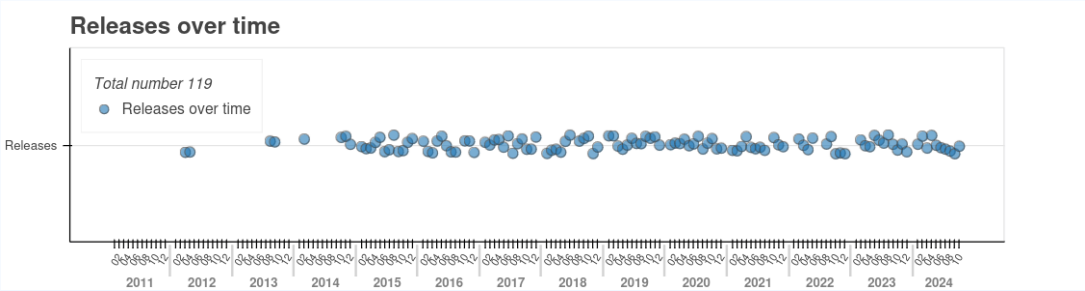
- MISP Intro: What it is, and what it can do
- Current state and Future of MISP
- How can MISP supports ISACs and its members

- Building an information sharing community, lessons learnt and best practices[1].

[1] We published the complete guidelines in https://www.x-isac.org/assets/images/guidelines_to_set-up_an_ISAC.pdf

What is MISP?

- MISP is a **threat information sharing platform** (**TISP**) that is free & open source software
- Mature project that was started in 2012, and since then, has been following a community-driven development



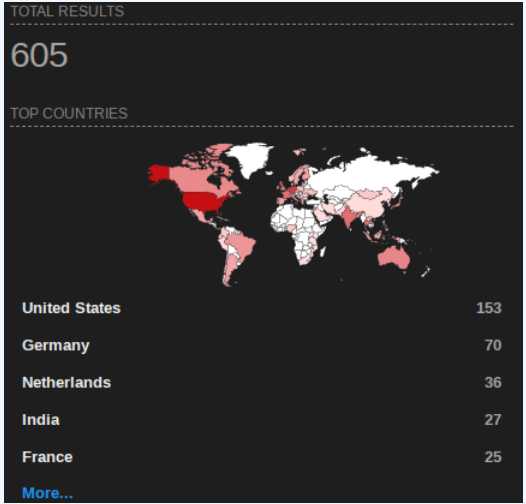
What is MISP?

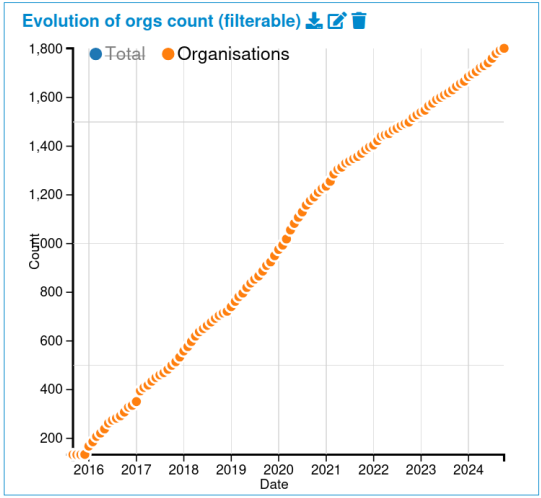
- Used worldwide to share threat-related information
- **Open-source commitment**: Users of MISP can rely on the tool never turning into closed source

What is MISP? (1)

- MISP is a **threat information sharing platform** (**TISP**) 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

Who is using MISP? (1)



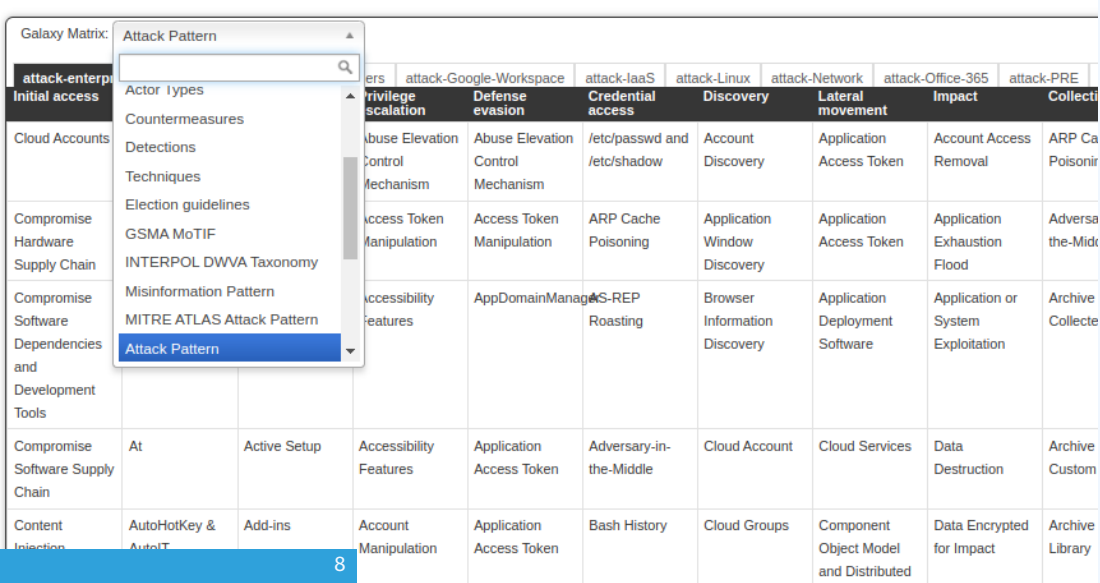


Who is using MISP? (2)

Communities: groups of users sharing within a set of common objectives/values.

- **Private sector** Financial, Manufacturing, Telecommunication
- **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)
- **ISACs** for many sectors (telecom, retail, aviations, ...) use MISP as a sharing mechanism
- **Trusted groups** running MISP communities in island mode (air gapped system) or partially connected mode.
- **LEA Agencies** EUROPOL, INTERPOL, MISP-LEA, · · ·
- **International groups** FIRST.org, MISP-Priv, · · ·

What is MISP? (2)

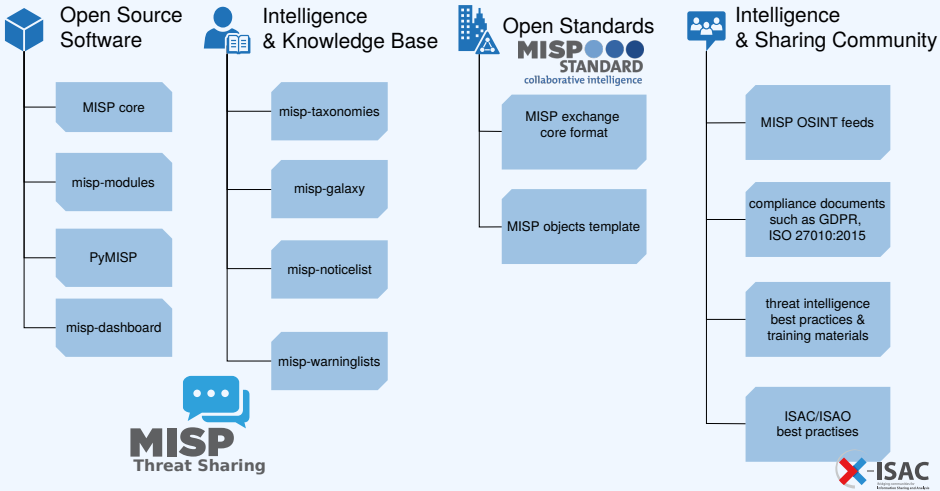


What is MISP? (2)

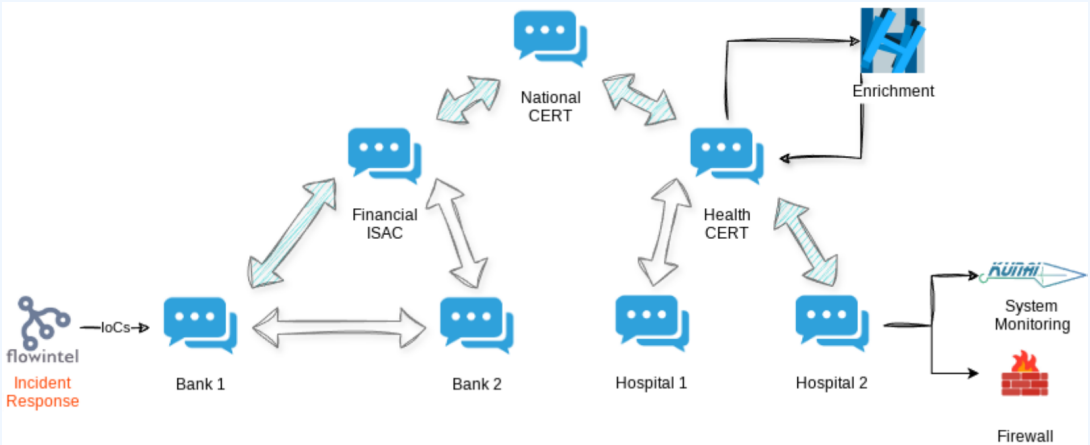
MISP is designed from the ground up to perform context-rich **threat intelligence**:

- **Enrich** information with context and metadata
- Maps **Threats and TTPs** (e.g MITRE ATT&CK)
- Supports many **standardized classification** marking
- Enables information **curation** through automated quality checks
- Offers visualisation of threat **relationships** and **technique** used
- Generates customizable **threat reports**
- Allows creation of **Dashboard** for trend analysis

MISP Project Overview



Sharing in MISP (1)



Sharing in MISP (2)

MISP offers a wide range of **strategy to share information**:

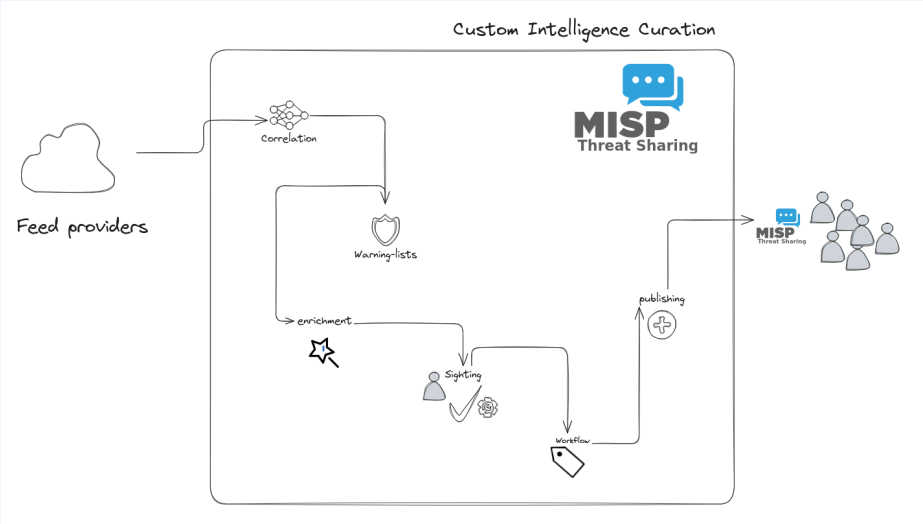
- Many **distribution level** offering granularity
- Sharing via distribution lists - **Sharing groups**
- Incremental Synchronisation & air-gapped sharing
- Feed system for ingestion & generation
- User defined **filtered sharing** for all the above mentioned methods
- Cross-instance information **caching** for quick lookups of large data-sets
- Support for multi-MISP **internal enclaves**

Information Quality Management

MISP has many features to help you manage and curate the data:

- **Correlating** data
- Feedback loop from detections via **Sightings**
- **False positive management** via the warninglist system
- **Enrichment system** via MISP-modules
- **Workflow** system to review and control information publication
- **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**
- **Jupyter Notebooks** supporting common use-cases

A Sample Curation Process in MISP

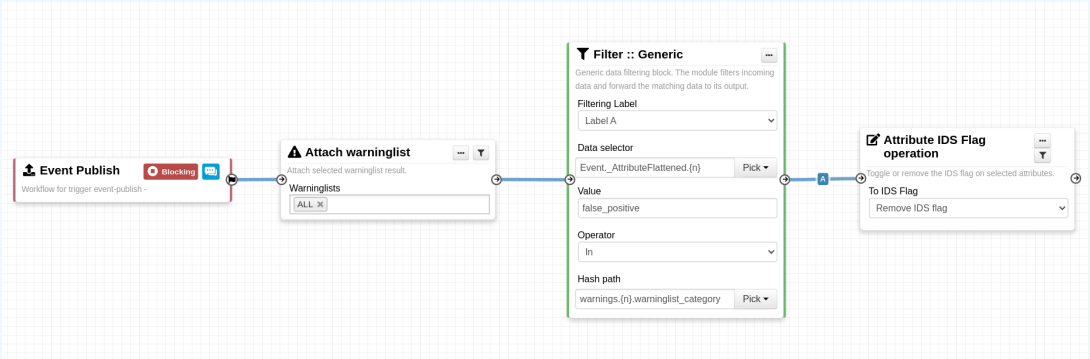


Integration and Automation ecosystem

MISP has many features to help you integrate various tools, processes and workflows:

- REST-full **API** & **PyMISP**
- **PubSub channels** (ZeroMQ & Kafka)
- **Enrichment** & **Import/Export** service through MISP-modules
- **Workflow system**: Quick and easy automation based on trigger/conditions/actions blocks

Information Quality Management



Blueprint library available on Github[2]

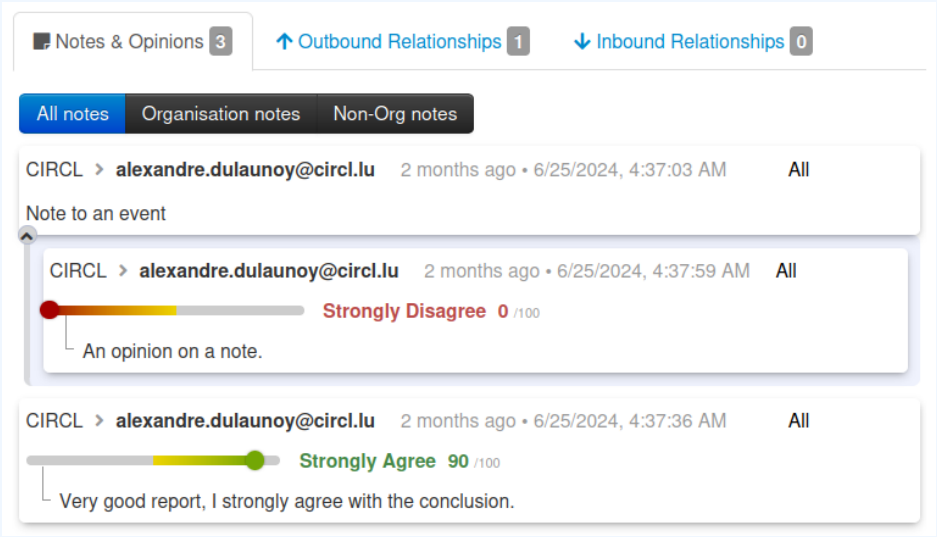
[2] https://github.com/MISP/misp-workflow-blueprints

Using the Power of the Community

MISP has many features to foster collaboration. To name a few:

- Proposals
- Analyst Data
- Delegation
- Sightings
- Extended Events
- Sharing-Groups
- . . .

Using the Power of the Community



Getting started: Joining/Running a sharing community using MISP

As a Member

- **Join** a "Hub" MISP instance
- **Host your own** MISP instance and connect to a "Hub"

As a ISAC

Plan ahead:

- Estimate community **requirements and objectives**
- Decide on **common vocabularies**
- **Offer services** to your members
  - Enrichment, Curation, ···

Success/Failure stories in MISP communities

TODO: To be added by alex

- CSSA
- Forced sharing as a requirement

Advantage of MISP being free and open-source

TODO: To be added by alex

Future of MISP: What's ongoing

Medium term:

- We just release a minor version 2.4
- Support 2.4 until 6 months after 2.5's release
- Full feature parity and compatibility
- In progress: Installation/update scripts for alternate distros

Long term: Major version 3.0

- Purge old/unused functionalities
- Port of the codebase to a new stack
- Rework DB updates
- Revamp front-end & aesthetics
- Analyst centric perspective
- Improved search and trend
- Improved performance

CIRCL's MISP Professional Services (MPS)

- We are confortably funded for the project to continue to prospere
- MPS offers professional services & supports the growth of the project

CIRCL's Offering:

- **Support Contract** - Prioritized resolution of issues and guidance
- **Training** - Adapted to the level of expertise of the participants
  - Free onboarding MISP training for ISACs and it's member
- **Hosting** - Hosted on our infrastructure (LU): Virtual or Dedicated
  - Maintenance of OS & MISP, Early patching for security issues

Conclusion

- MISP is just a tool. What matters is your **sharing practices**.
- MISP strives to meet any community's use-cases.
- MISP project combines **open source softwares**, **open standards & best practices** to make information sharing a reality.