

# MISP PROJECT AND ISACs

A VERSATILE OPEN SOURCE INFORMATION SHARING PLATFORM

TEAM CIRCL  
*TLP:WHITE*

13TH ENISA-EC3 WORKSHOP





## MISP Project

MISP Project - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing

Verified

678 followers

Worldwide

<https://www.misp-project.org>

@MISPPProject

<https://misp-community.org/@misp>

[info@misp-project.org](mailto:info@misp-project.org)



**circl.lu**

Computer Incident  
Response Center  
LUXEMBOURG

- 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

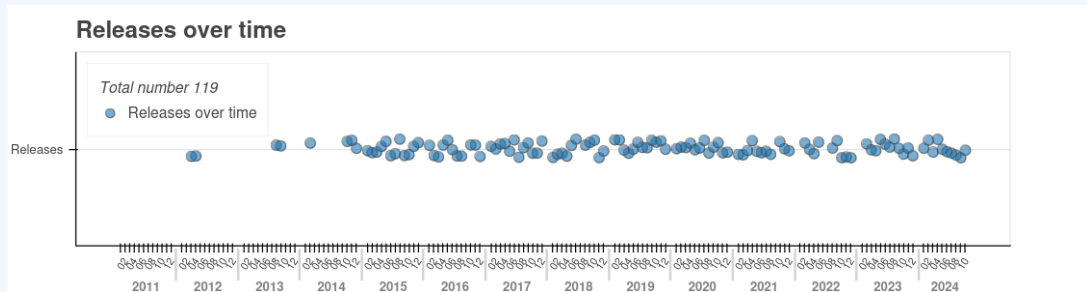
- MISP Intro: What it is, and what it can do
- Current state and Future of MISP
- How can MISP supports ISACs and its members
- Building an information sharing community, lessons learnt and best practices<sup>1</sup>.

---

<sup>1</sup>We published the complete guidelines in [https://www.x-isac.org/assets/images/guidelines\\_to\\_set-up\\_an\\_ISAC.pdf](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?

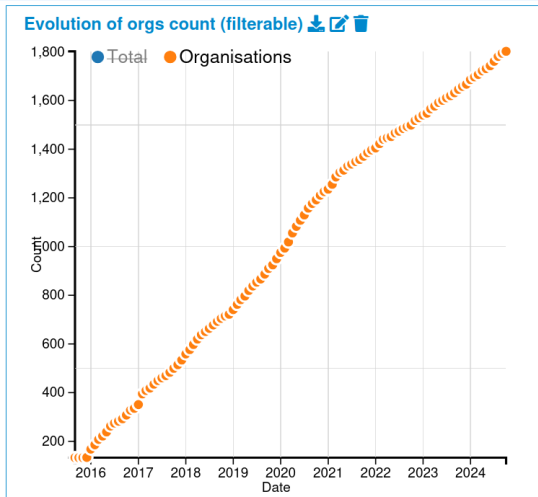
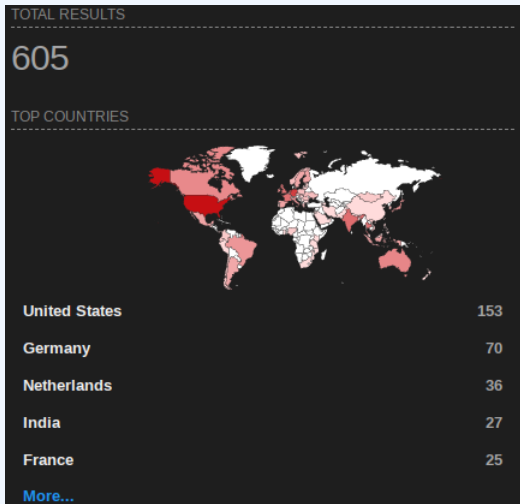
- Used worldwide to share threat-related information
- **Open-source commitment:** Users of MISP can rely on the tool never turning into closed source



# 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)

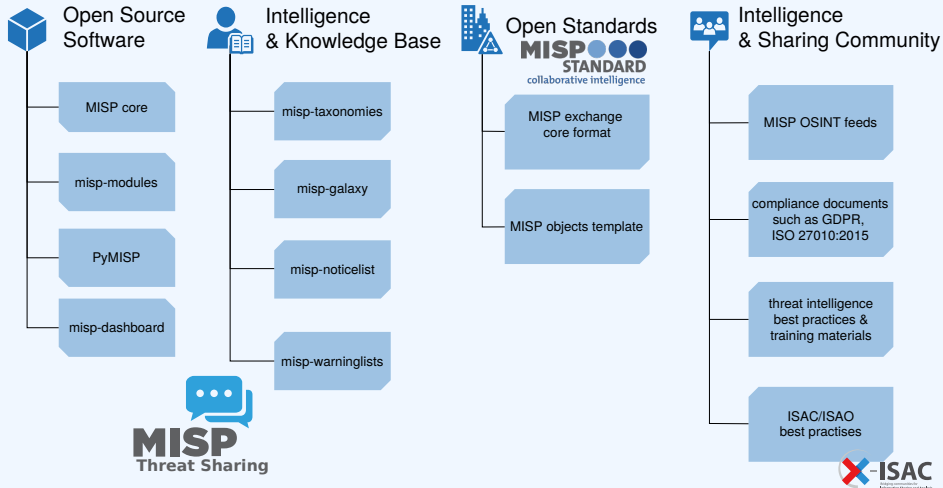
Galaxy Matrix:	Attack Pattern								
attack-enterprise									
Initial access	Actor Types		Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Impact	Collection
Cloud Accounts	Countermeasures		Abuse Elevation	Abuse Elevation	/etc/passwd and /etc/shadow	Account Discovery	Application Access Token	Account Access Removal	ARP Cache Poisoning
	Detections		Control Mechanism	Control Mechanism					
Compromise Hardware	Techniques		Access Token Manipulation	Access Token Manipulation	ARP Cache Poisoning	Application Window Discovery	Application Access Token	Application Exhaustion Flood	Adversary in-the-Middle
Supply Chain	Election guidelines								
	GSMA MoTIF								
Compromise Software	INTERPOL DWVA Taxonomy								
Dependencies and Development Tools	Misinformation Pattern		Accessibility Features	AppDomainManager	AS-REP Roasting	Browser Information Discovery	Application Deployment Software	Application or System Exploitation	Archive Collection
	MITRE ATLAS Attack Pattern								
	Attack Pattern								
Compromise Software Supply Chain	At	Active Setup	Accessibility Features	Application Access Token	Adversary-in-the-Middle	Cloud Account	Cloud Services	Data Destruction	Archive Custom
Content Injection	AutoHotKey & AutoIT	Add-ins	Account Manipulation	Application Access Token	Bash History	Cloud Groups	Component Object Model and Distributed	Data Encrypted for Impact	Archive Library

## WHAT IS MISP? (2)

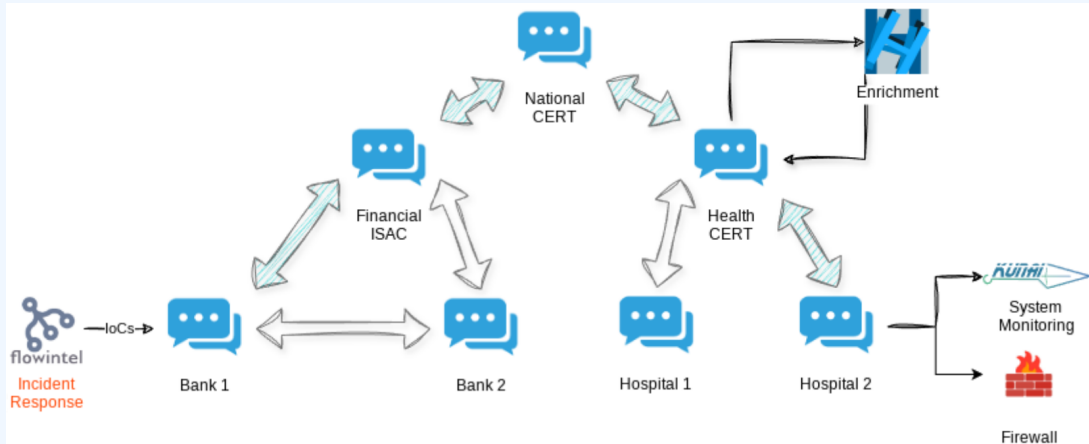
MISP is designed from the ground up to perform context-rich **threat intelligence**:

- **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)



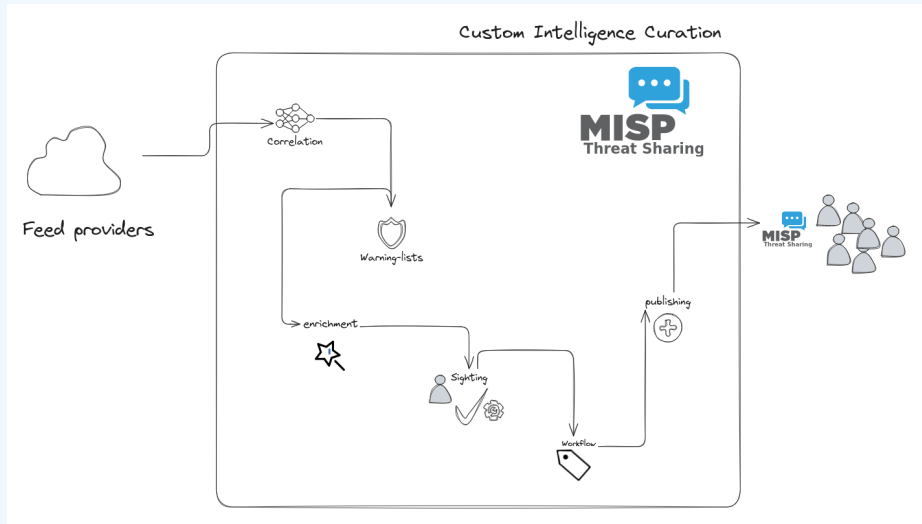
MISP offers a wide range of **strategy to share information**:

- 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**

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

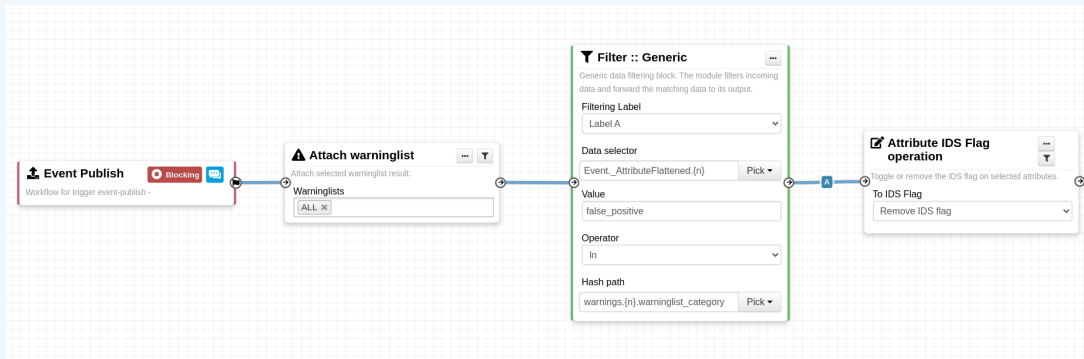


MISP has many features to help you integrate various tools, processes and workflows:

- 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<sup>2</sup>

<sup>2</sup><https://github.com/MISP/misp-workflow-blueprints>

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

Notes & Opinions 3

Outbound Relationships 1

Inbound Relationships 0

All notes

Organisation notes

Non-Org notes

CIRCL > alexandre.dulaunoy@circl.lu
2 months ago • 6/25/2024, 4:37:03 AM
All

Note to an event

CIRCL > alexandre.dulaunoy@circl.lu
2 months ago • 6/25/2024, 4:37:59 AM
All

Strongly Disagree 0 /100

An opinion on a note.

CIRCL > alexandre.dulaunoy@circl.lu
2 months ago • 6/25/2024, 4:37:36 AM
All

Strongly Agree 90 /100

Very good report, I strongly agree with the conclusion.

# 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, ...

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 comfortably funded for the project to continue to prosper
- 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 its member
- **Hosting** - Hosted on our infrastructure (LU): Virtual or Dedicated
  - ▶ Maintenance of OS & MISP, Early patching for security issues



- 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.