

MISP PROJECT AND ISACs

A VERSATILE OPEN SOURCE INFORMATION SHARING PLATFORM

TEAM CIRCL

TLP:CLEAR

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>

🐦 @MISPProject

🌐 <https://misp-community.org/@misp>

✉ info@misp-project.org



circl.lu

Computer Incident
Response Center
LUXEMBOURG

- CIRCL is mandated by the Ministry of the Economy (under NIS 2).
- CIRCL leads the development of MISP.
- **CIRCL manages multiple large MISP communities, enabling active daily threat intelligence sharing.**
- Funding comes from Luxembourg, various EU programs, and partnerships under EU/US agreements.

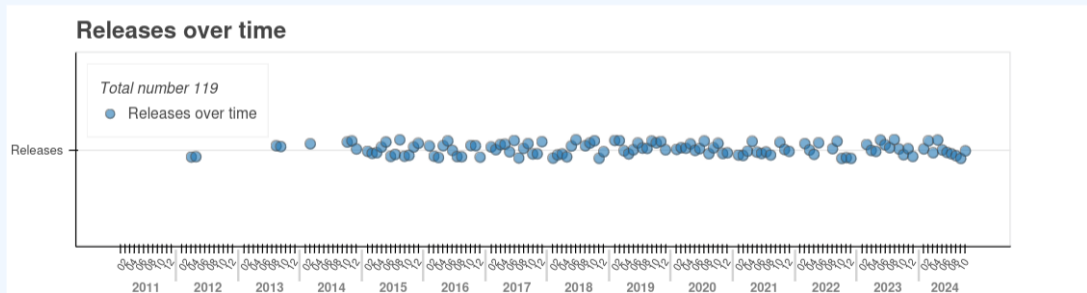
- MISP Intro: What it is, and what it can do
- Current state and Future of MISP
- How can MISP supports ISACs and its members

- Building an information sharing community, lessons learnt and best practices¹.

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

WHAT IS MISP?

- MISP² 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



²<https://www.misp-project.org/>

WHAT IS MISP?

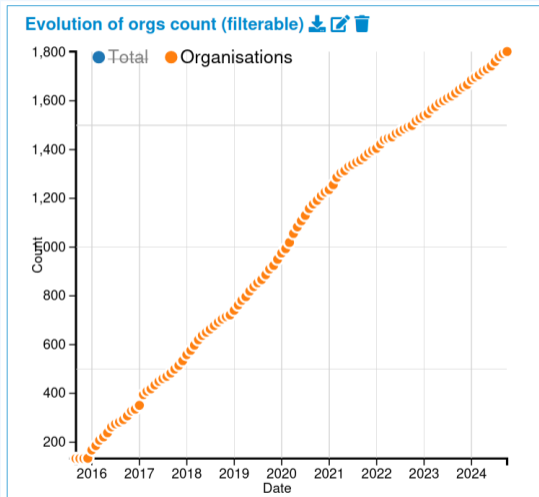
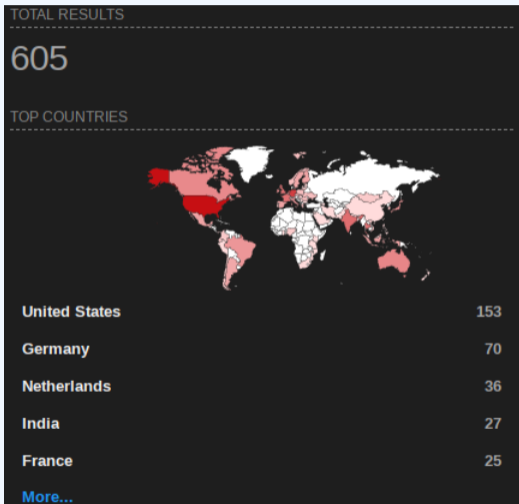
- Used worldwide to manage and share threat-related information and intelligence.
- **Open-Source Commitment:** Users of MISP can rely on the tool remaining open source and never becoming closed source (autonomy of the users).



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 and values.

- **Private Sector:** Financial, Manufacturing, Telecommunications.
- **Military and International Organizations:** NATO, military CSIRTs, national and governmental CERTs, etc.
- **Security Vendors:** Running their own communities or interfacing with MISP communities
- **Topical Communities:** Set up to tackle specific issues (e.g., COVID-19 MISP).
- **ISACs:** Serving various sectors such as Telecom, Retail, Aviation Traffic Control, etc.
- **Trusted Groups:** Operating MISP communities in island mode (air-gapped systems) or partially connected modes.
- **Law Enforcement Agencies (LEAs):** EUROPOL, INTERPOL, MISP-LEA, and more.
- **International Groups:** FIRST.org, MISP-Priv, and others.

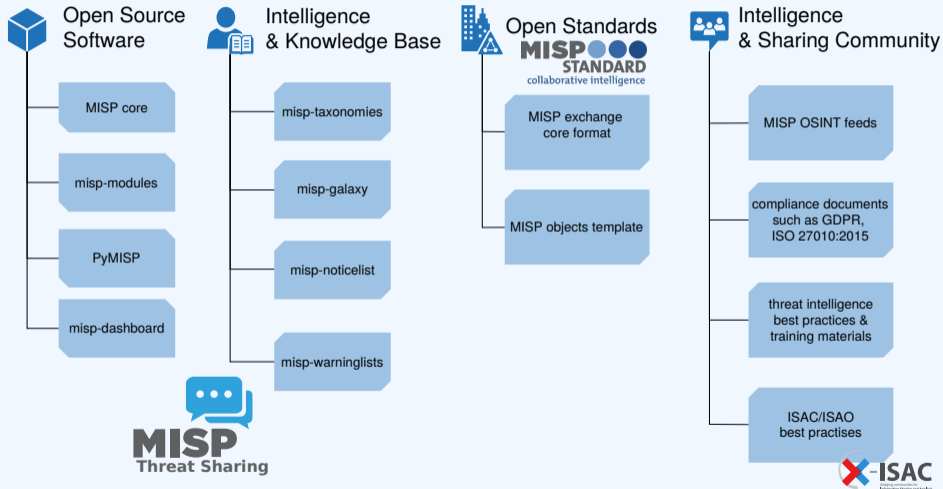
WHAT IS MISP? (2)

Galaxy Matrix:			ers	attack-Google-Workspace	attack-iaaS	attack-Linux	attack-Network	attack-Office-365	attack-PRE
Initial access	Actor types	Countermeasures	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Impact	Collection
Cloud Accounts	Detections	Techniques	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	/etc/passwd and /etc/shadow	Account Discovery	Application Access Token	Account Access Removal	ARP Cache Poisoning
Compromise Hardware Supply Chain	Election guidelines	GSMA MoTIF	Access Token Manipulation	Access Token Manipulation	ARP Cache Poisoning	Application Window Discovery	Application Access Token	Application Exhaustion Flood	Adversary-in-the-Middle
Compromise Software Dependencies and Development Tools	Misinformation Pattern	INTERPOL DWVA Taxonomy	Accessibility Features	AppDomainManager	AS-REP Roasting	Browser Information Discovery	Application Deployment Software	Application or System Exploitation	Archive Collection
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

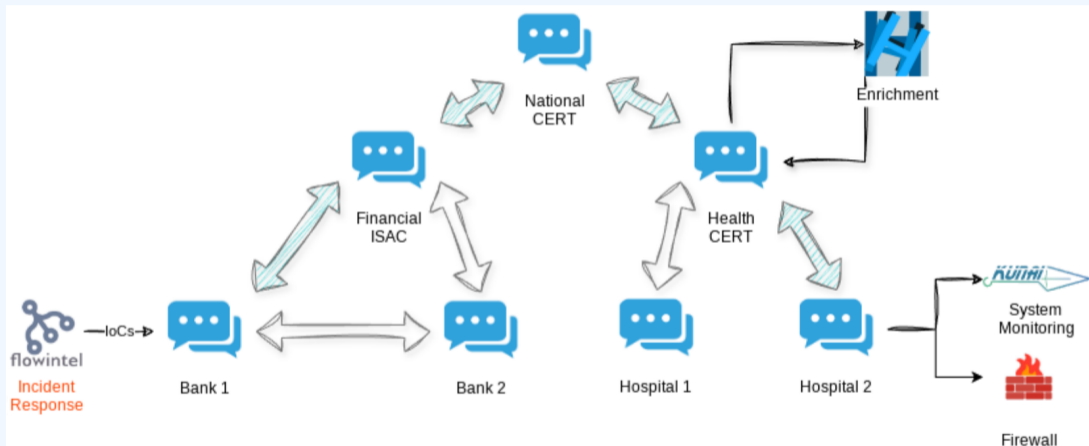
MISP is designed from the ground up to perform context-rich **threat intelligence**:

- **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)



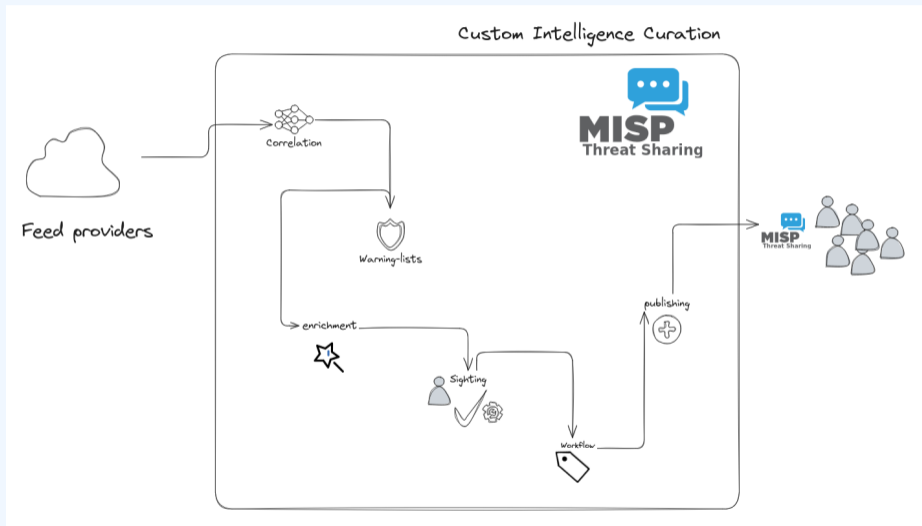
MISP offers a wide range of **strategy to share information**:

- 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

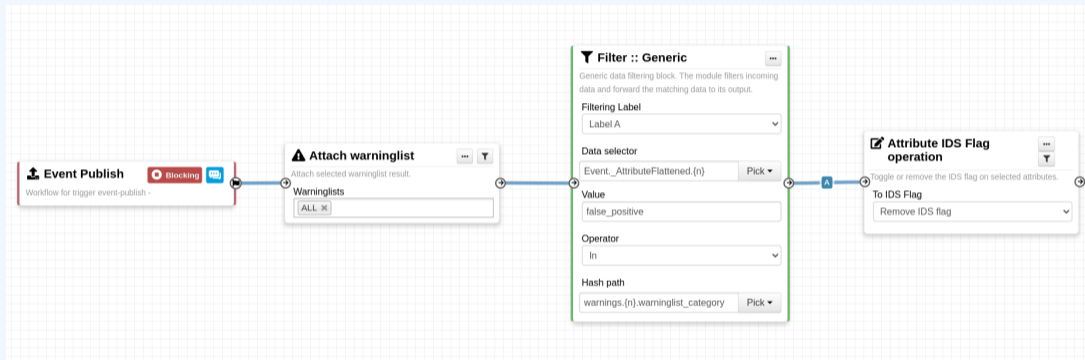
A SAMPLE CURATION PROCESS IN MISP



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 Github³

³<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

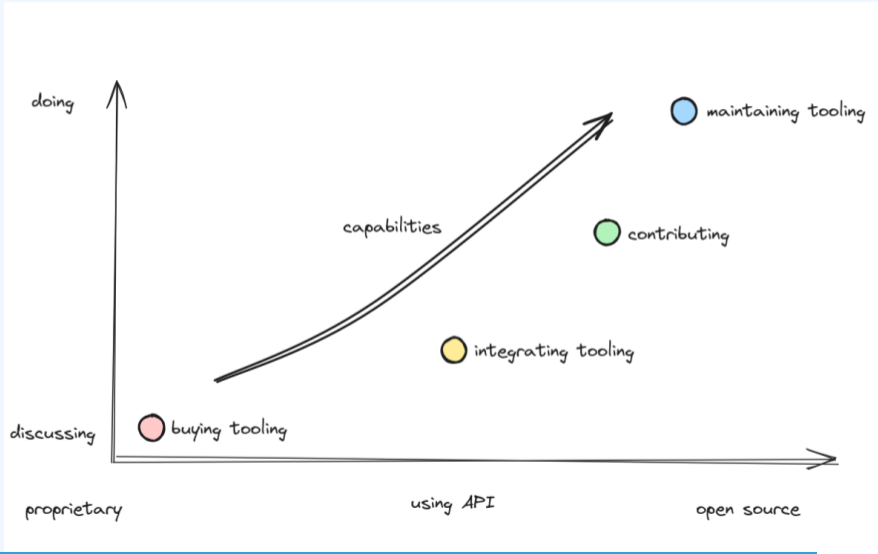
Plan ahead:

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

SUCCESS AND FAILURE STORIES IN MISP COMMUNITIES

- We have supported various ISACs and sharing communities over the past years.
- Success largely depends on **the dynamics** within the sharing community and how the rules are defined.
- Collaboration improves with **contextualization practices** and **well-established rules of operation**.
- Successful ISACs use MISP as a tool, customizing it to fit their specific needs.

INCENTIVES FOR USING OPEN SOURCE



Medium Term:

- We just released version 2.5.
- Support for 2.4 will continue until 6 months after 2.5's release.
- Full feature parity and compatibility between 2.4 and 2.5.

Long Term: Major Version 3.0

- Revamp front-end and aesthetics.
- Analyst-centric perspective.
- Improved search and analytics.
- Enhanced performance.

CIRCL'S MISP PROFESSIONAL SERVICES (MPS)

- We are comfortably funded to ensure the project's continued prosperity.
- MPS provides professional services and assists organizations seeking to secure support for MISP.

CIRCL's Offering:

- **Support Contract:** Prioritized issue resolution and expert guidance.
- **Training:** Tailored to the expertise level of participants.
 - ▶ Free onboarding MISP training for ISACs and their members.
- **Hosting:** Hosted on our infrastructure in Luxembourg (LU), available as virtual or dedicated instances.
 - ▶ OS and MISP maintenance, with early patching for security issues.

- MISP is just a tool—what truly matters are your **sharing and analysis practices**.
- MISP strives to meet the use cases of any community, from simple to complex ones.
- The MISP project combines **open-source software, open standards, and best practices** to make information sharing and analysis a reality.

- `info@circl.lu - info@misp-project.org`
- Open source software developed and used by CIRCL - <https://tinyurl.com/ISACTOOLING>