

# MISP OPEN SOURCE THREAT INTELLIGENCE AND SHARING PLATFORM

MILITARY USE CASES

ALEXANDRE DULAUNOY

MISP PROJECT

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

20240507



**MISP**  
Threat Sharing

- In 2012, during a malware analysis workgroup, we realized that multiple analysts were working independently on the same malware.
- To streamline our efforts and avoid redundancy, we sought a **method for easy and automated information sharing**.
- Christophe Vandeplass, then employed at the Belgian Ministry of Defense, presented his preliminary work on what would eventually evolve into the MISP platform.
- An initial version of the MISP platform was adopted by the MALWG, and the valuable feedback from users fueled further development and enhancements.
- Today, MISP has grown into a platform driven by **community development**.

The Computer Incident Response Center Luxembourg (CIRCL)<sup>1</sup> 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 Luxembourg House of Cybersecurity (LHC) g.i.e.

---

<sup>1</sup><https://www.circl.lu/>

- CIRCL is mandated by the Ministry of Economy and acting as the Luxembourg National CERT for private sector (under the NIS directive).
- 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.**



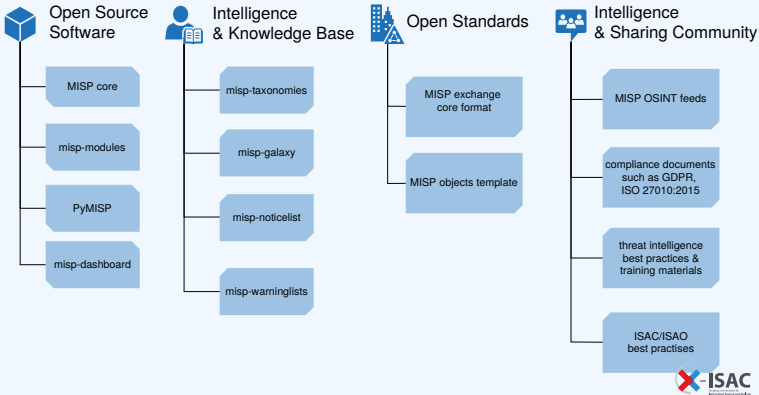
**Co-financed by the European Union**

Connecting Europe Facility

## WHAT IS MISP? (CORE SOFTWARE)

- 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

# MISP PROJECT OVERVIEW



- 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, likelihood and occurrences.
  - ▶ **Fraud analysts** willing to share financial indicators to detect financial frauds.

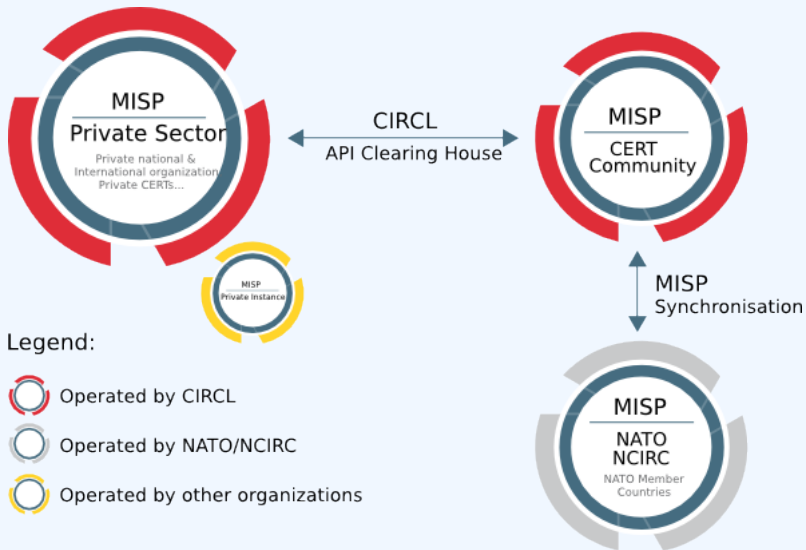
- Sharing indicators/selectors for a **detection** matter.
  - ▶ 'Do I have infected systems in my infrastructure or the ones I operate?'
- Sharing indicators to **block**.
  - ▶ 'I use these attributes to block, sinkhole or divert traffic.'
- Sharing indicators to **perform intelligence**.
  - ▶ 'Gathering 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)

# NATO AND MISP COMMUNITIES



- MISP's versatile standard<sup>2</sup> seamlessly integrates with military protocols, enhancing interoperability.
- Supports diverse intelligence inputs, including **HUMINT** (Human Intelligence), **SIGINT** (Signals Intelligence), and **OSINT** (Open Source Intelligence), within the MISP framework.

---

<sup>2</sup><https://www.misp-standard.org/>

- MISP has added support for the Signal Metadata Format Specification (SigMF)<sup>3</sup>, used widely in **software-defined radio and signal processing**.
- New SigMF-related object templates introduced:
  - ▶ SigMF Recording
  - ▶ SigMF Archive
  - ▶ SigMF Expanded Recording
- Enrichment features in MISP allow expansion of SigMF recordings, aiding in data analysis and integration of signal metadata into MISP attributes.
- This integration facilitates improved search capabilities and data analysis within MISP.


---

<sup>3</sup>[https://www.misp-project.org/2023/08/23/MISP\\_now\\_supports\\_Signal\\_Metadata\\_Format\\_Specification\\_SigMF.html/](https://www.misp-project.org/2023/08/23/MISP_now_supports_Signal_Metadata_Format_Specification_SigMF.html/)

# SIGINT - MISP INTEGRATION WITH SIGMF

2023-07-12 Object name: sigmf-expanded-recording [↗]

Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API

<input type="checkbox"/>	2023-07-12	Other	<b>datatype:</b> text	cf32_le	+ + + +
<input type="checkbox"/>	2023-07-12	Other	<b>license:</b> text	https://creativecommons.org/licenses/by/4.0/	+ + + +
<input type="checkbox"/>	2023-07-12	Other	<b>recorder:</b> text	GNU Radio 3.8.2	+ + + +
<input type="checkbox"/>	2023-07-12	Other	<b>sample_rate:</b> float	480000	+ + + +
<input type="checkbox"/>	2023-07-12	Other	<b>sha512:</b> text	bb2f1f9222b172373e81d333a11a866d56611308fd481c79c2462e50fec62da1bdd93a94cd9b3e00dcaa6ba4ffe4546022aa50385bc582fc8dd7426740b564	+ + + +
<input type="checkbox"/>	2023-07-12	Other	<b>version:</b> text	0.0.2	+ + + +
<input type="checkbox"/>	2023-07-12	External analysis	<b>waterfall-plot:</b> attachment		+ + + +

2023-07-12 Object name: sigmf-recording [↗]  
References: 0 [↗]  
Referenced by: 1 [↗]


<input type="checkbox"/>	2023-07-12	External analysis	<b>SigMF-data:</b> attachment	<a href="#">gw8.sigmf-data</a>	+ + + +
<input type="checkbox"/>	2023-07-12	External analysis	<b>SigMF-meta:</b> attachment	<a href="#">gw8.sigmf-meta</a>	+ + + +

- The MISP standard is extensible; objects can be easily created to cover specific use cases.
- Military organizations often have their own unique data models.
- The MISP standard includes 344<sup>4</sup> default object templates, many of which are applicable to HUMINT.

---

<sup>4</sup><https://www.misp-project.org/objects.html>

# HUMINT - MISP VERSATILE OBJECTS

2023-01-27 662...655		Object name: person	References: 9	Referenced by: 1				
<input type="checkbox"/>	2023-01-27 3f3...7ab	Other	<b>function:</b> text	Cyber Operator				
<input type="checkbox"/>	2023-01-27 1ac...bca	Person	<b>last-name:</b> last-name	Serebriakov				
<input type="checkbox"/>	2023-01-27 175...dd4	Person	<b>full-name:</b> full-name	Evengil Mikhaylovich Serebriakov				
<input type="checkbox"/>	2023-01-27 18e...5a3	Person	<b>middle-name:</b> middle-name	Mikhaylovich				
<input type="checkbox"/>	2023-01-27 e3a...068	Person	<b>first-name:</b> first-name	Evengil				
<input type="checkbox"/>	2023-01-27 a7f...bc9	Other	<b>alias:</b> text	Serebryakov				
<input type="checkbox"/>	2023-01-27 5fe...14b	External analysis	<b>portrait:</b> attachment					
<input type="checkbox"/>	2023-01-27 7f2...f97	Other	<b>occupation:</b> text	Cyber operator				
<input type="checkbox"/>	2023-01-27 f98...f48	Person	<b>place-of-birth:</b> place-of-birth	Kursk				
<input type="checkbox"/>	2023-01-27 ca1...e3b	Other	<b>role:</b> text	Suspect				
<input type="checkbox"/>	2023-01-27 015...73a	Person	<b>passport-expiration:</b> passport-expiration	17-04-2022				
<input type="checkbox"/>	2023-01-27 cf6...d6e	Person	<b>date-of-birth:</b> date-of-birth	26-07-1981				

- MISP includes a default knowledge base known as MISP Galaxies<sup>5</sup>,
- For instance, the Threat Actor galaxy contains an officially maintained list of Threat Actors.
- Military organizations often have their own methods of attribution or adaptations from existing models.
- MISP allows users to fork and maintain their own perspectives on threat actors.

---

<sup>5</sup><https://www.misp-galaxy.org/>



- 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

- 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**

- **Information sharing practices come from usage** and by example (e.g. learning by imitation from the shared information).
- MISIP 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 MISIP to meet their community's use-cases.
- MISIP project combines open source software, open standards, best practices and communities to make information sharing a reality.