MISP Open Source Threat Intelligence and Sharing Plaform

Military Use Cases

Alexandre Dulaunoy

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

20240507

MISP
Threat Sharing

MISP and Starting from a Practical Use-Case

- 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 Vandeplas, 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**.

ABOUT CIRCL

The Computer Incident Response Center Luxembourg (CIRCL)[1] 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.

[1] https://www.circl.lu/

MISP and CIRCL

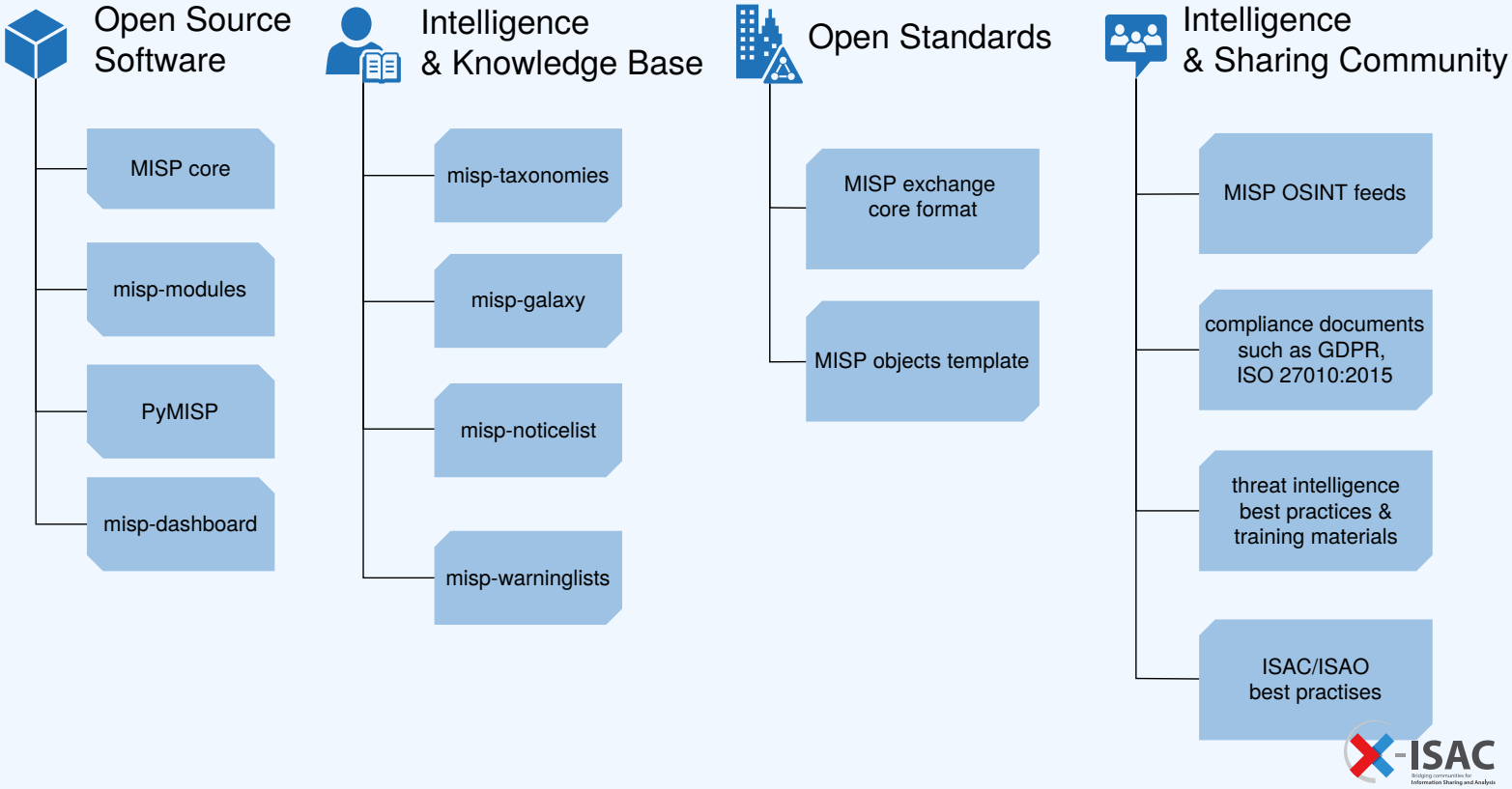
- CIRCL is mandated by the Ministry of Economy and acting as the Luxembourg National CERT for private sector (under the NIS directive).
- CIRCL leads the development of the Open Source MISP threat intelligence platform which is used by many military or intelligence communities, private companies, financial 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



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.

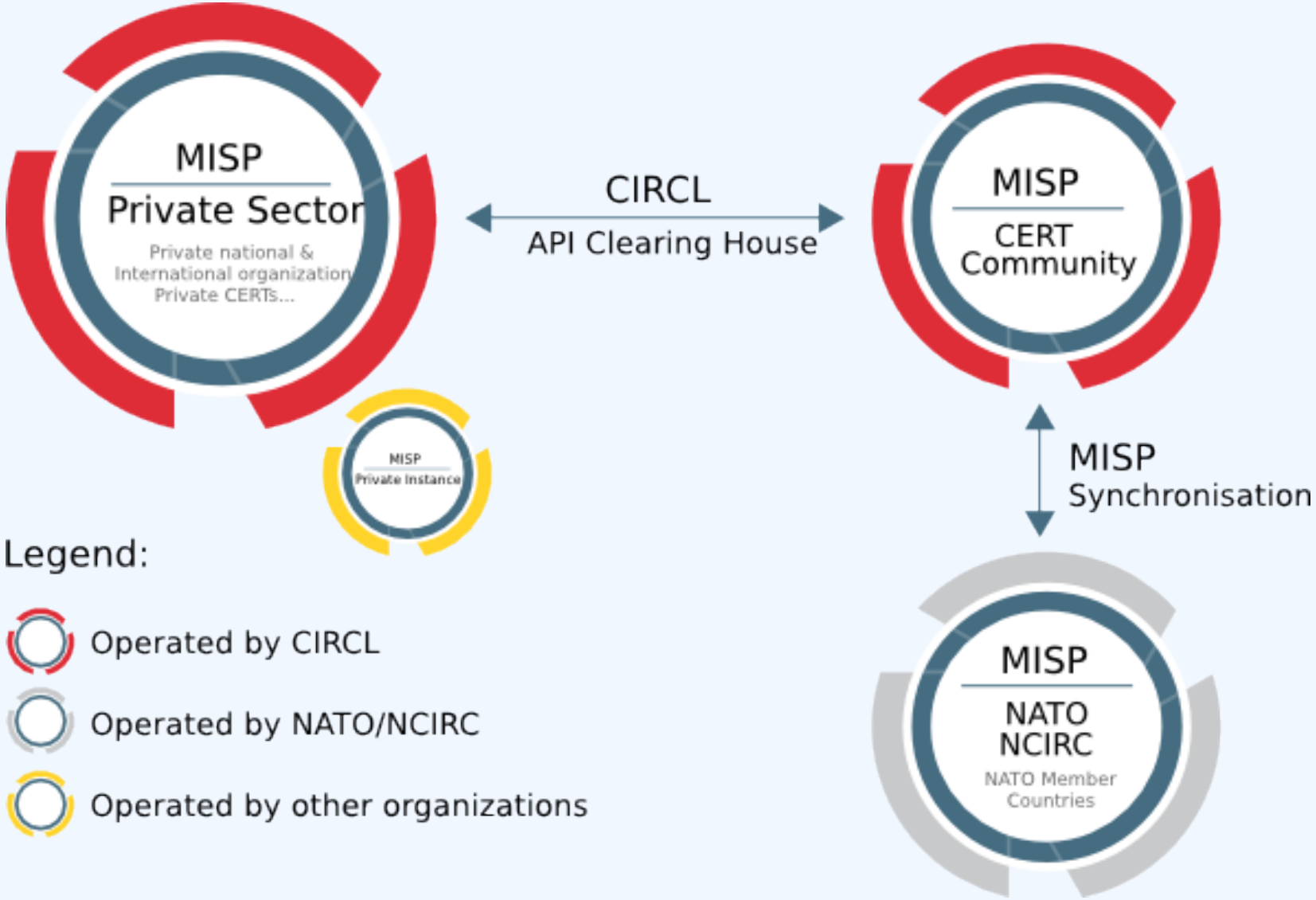
Many objectives from different user-groups

- 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?'
- $\rightarrow$ 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



Evolving Military Use Cases with MISP

- MISP's versatile standard[2] 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.

[2] https://www.misp-standard.org/

SIGINT - MISP Integration with SigMF

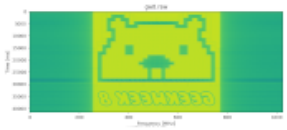
- MISP has added support for the Signal Metadata Format Specification (SigMF)[3], used widely in **software-defined radio and signal processing**.
- New SigMF-related object templates introduced:
  - SigMF Recording
  - SigMF Archive
  - SigMF Expanded Recording
- Enrichment features in MISP allow expansion 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.

[3] 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

		text	
2023-07-12	Other	**datatype:** text	cf32_le
2023-07-12	Other	**license:** text	https://creativecommons.org/licenses/by/4.0/
2023-07-12	Other	**recorder:** text	GNU Radio 3.8.2
2023-07-12	Other	**sample_rate:** float	480000
2023-07-12	Other	**sha512:** text	bb2f1f9222b172373e81d333a11a866d56611308fd481c7f9c2462e50fec62da1bddd93a94cd9b3e00dcaa6ba4ffe4546022aa50385bc582fc8dd7426740b564
2023-07-12	Other	**version:** text	0.0.2
2023-07-12	External analysis	**waterfall-plot:** attachment	

2023-07-12 **Object name:** sigmf-recording
References: 0
Referenced by: 1

2023-07-12	External analysis	**SigMF-data:** attachment	gw8.sigmf-data
2023-07-12	External analysis	**SigMF-meta:** attachment	gw8.sigmf-meta

HUMINT - MISP VERSATIBLE OBJECTS

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

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

Information quality management

- 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**

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.