Threat Intelligence and Information Sharing with MISP

Supporting and Expanding ISACs/CSIRTs Capabilities

CIRCL
Computer Incident
Response Center
Luxembourg

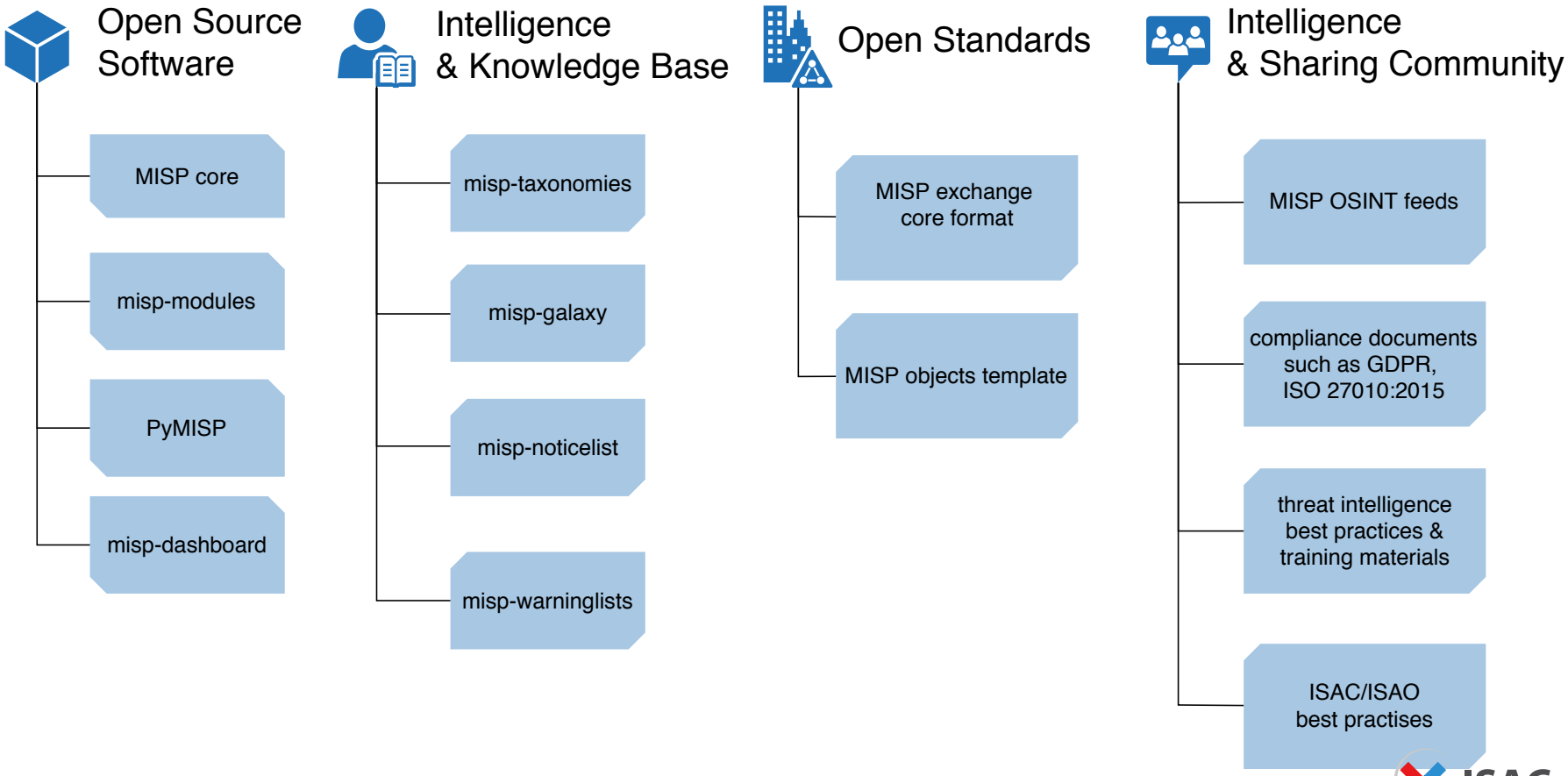
Team CIRCL

https://www.misp-project.org/
Twitter: *@MISPProject*

TheHive-MISP workshop -
TLP:WHITE

MISP Project is a **completely open collaborative effort** to support analysts and organisations in all efforts related to **information sharing and threat intelligence**.
The project includes a range of open source software, composed of a **threat intelligence platform** with sharing capabilities, expansion modules, advanced API capabilities and situational awareness tools.
It also includes a comprehensive intelligence library and knowledge base acting as reference material for common taxonomies and classifications, threat-actors, complex intelligence models and common false-positive warning libraries.
Furthermore, the project encompasses a set of **open standards**, of which the reference implementation is MISP itself, designed to be freely reused by communities developing their own software and tools.
In addition, the MISP project releases a set of best practises that can be used as guidelines meant **to support closed, semi-open and open sharing communities**.

MISP Threat Sharing



about CIRCL

The Computer Incident Response Center Luxembourg (CIRCL) 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 securitymadein.lu g.i.e.

MISP and CIRCL

- CIRCL is mandated by the Ministry of Economy and acting as the Luxembourg National CERT for private sector.
- 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

MISP information sharing communities

The largest community, operated by CIRCL, includes more than 950 organisations:

- National/Governmental/Military CSIRTs
- NATO (NCIRC and NICP)
- ISACs/ISAOs (Information Sharing and Analysis Center)
- along with many large private organisations
- security researchers and SMEs in the ICT field
- security vendors

On average 2500 indicators with threat-actor context are being shared each week within some MISP communities, which is used by National CERTs and other organisations worldwide to coordinate collaborative analysis of high level threats, including EU institutions and member states.

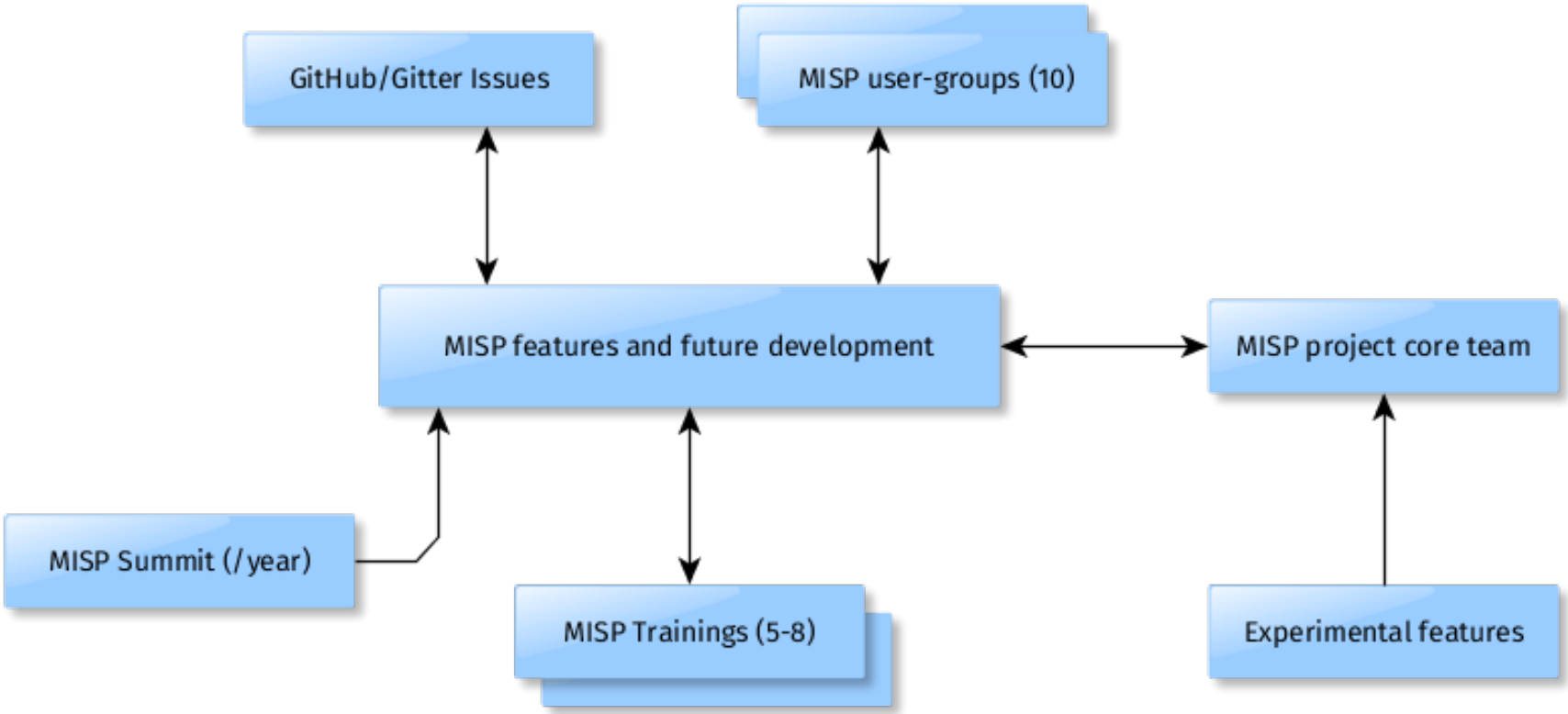
MISP and starting from a practical use-case

- During a malware analysis workgroup in 2012, we discovered that we worked on the analysis of the same malware.
- We wanted to share information in an easy and automated way **to avoid duplication of work**.
- Christophe Vandeplas (then working at the CERT for the Belgian MoD) showed us his work on a platform that later became MISP.
- A first version of the MISP Platform was used by the MALWG and **the increasing feedback of users** helped us to build an improved platform.
- MISP is now **a community-driven development** lead by CIRCL.

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.

MISP model of governance



MISP features

- MISP[1] is a free & open source threat information sharing software.
- MISP has **a host of functionalities** that assist users in creating, collaborating & sharing threat information - e.g. flexible sharing groups, **automatic correlation**, free-text import helper, event distribution & proposals.
- Many export formats which support IDSes / IPSes (e.g. Suricata, Bro, Snort), SIEMs (eg CEF), Host scanners (e.g. OpenIOC, STIX, CSV, yara), analysis tools (e.g. Maltego), DNS policies (e.g. RPZ) or financial AML format (e.g. goAML).

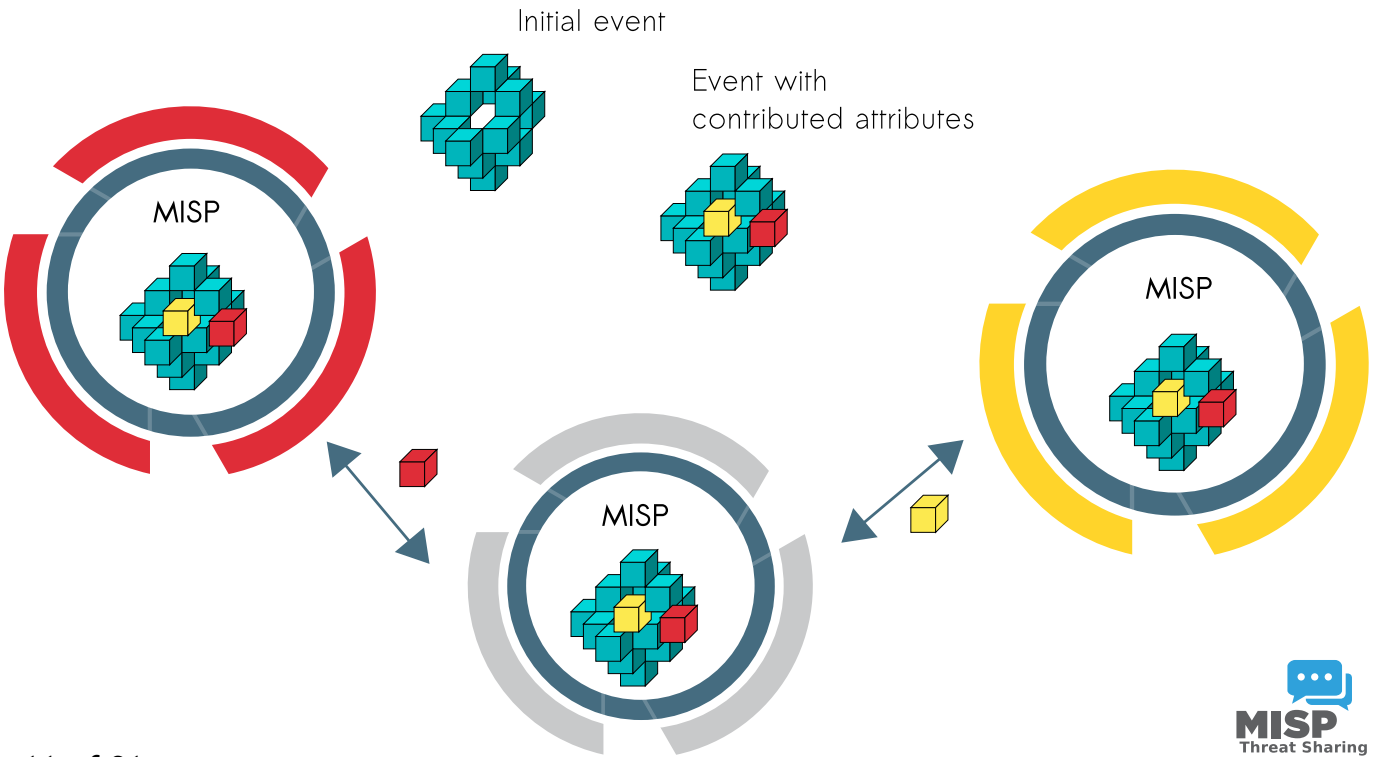
[1] `https://github.com/MISP/MISP`

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 950 organizations with more than 1900 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).

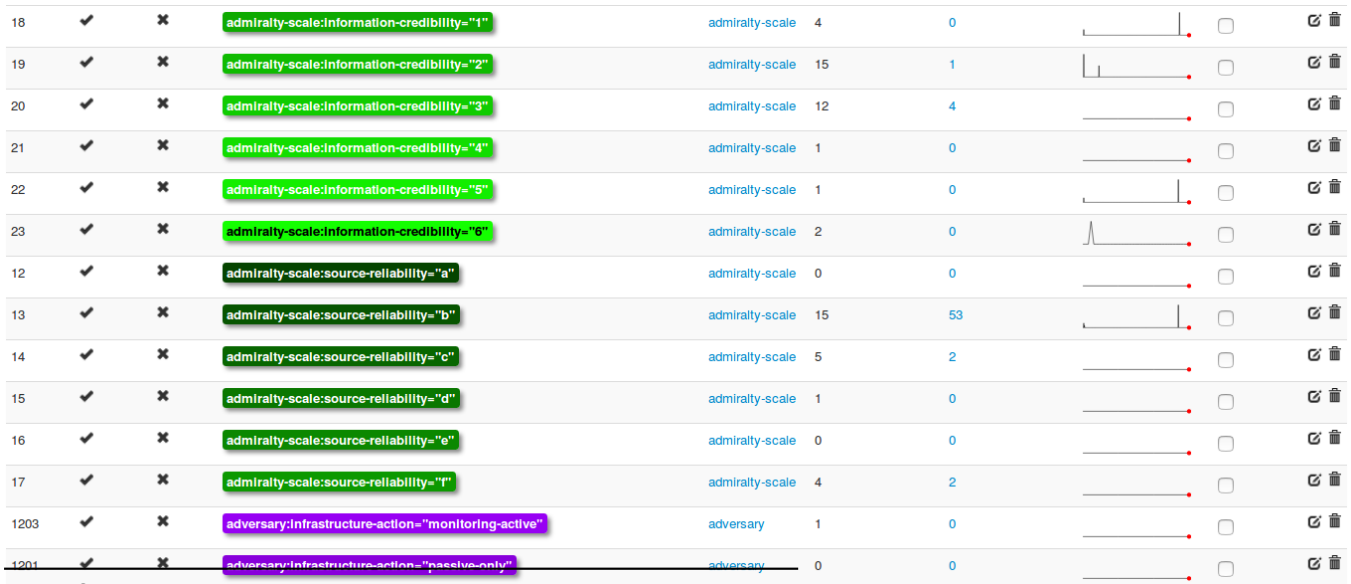
MISP core distributed sharing functionality

- MISPs core functionality is sharing, where everyone can be a consumer and/or a contributor/producer.
- Quick benefit without the obligation to contribute.
- Low barrier access to get acquainted to the system.



Supporting classification

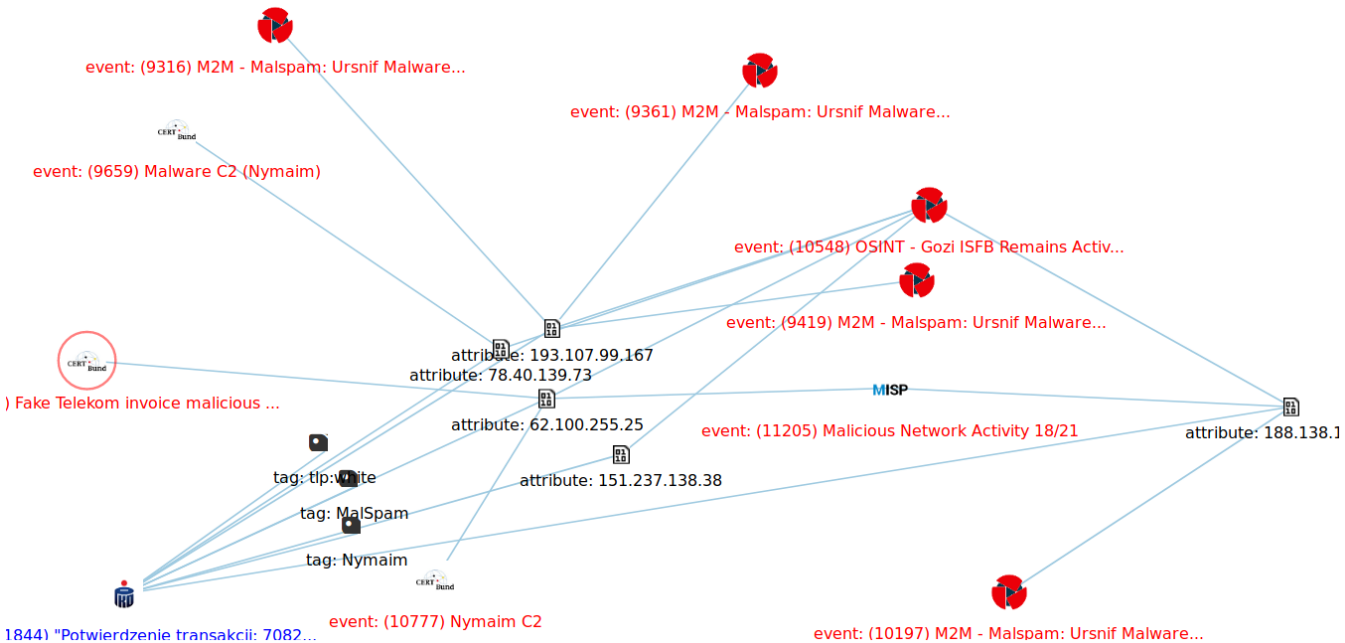
- Tagging is a simple way to attach a classification to an event or an attribute.
- **Classification must be globally used to be efficient**.
- MISP includes a flexible tagging scheme where users can select from more than 72 existing taxonomies[2] or create their own taxonomy.



18	✔	✖	admiralty-scale:information-credibility="1"	admiralty-scale	4	0			
19	✔	✖	admiralty-scale:information-credibility="2"	admiralty-scale	15	1			
20	✔	✖	admiralty-scale:information-credibility="3"	admiralty-scale	12	4			
21	✔	✖	admiralty-scale:information-credibility="4"	admiralty-scale	1	0			
22	✔	✖	admiralty-scale:information-credibility="5"	admiralty-scale	1	0			
23	✔	✖	admiralty-scale:information-credibility="6"	admiralty-scale	2	0			
12	✔	✖	admiralty-scale:source-reliability="a"	admiralty-scale	0	0			
13	✔	✖	admiralty-scale:source-reliability="b"	admiralty-scale	15	53			
14	✔	✖	admiralty-scale:source-reliability="c"	admiralty-scale	5	2			
15	✔	✖	admiralty-scale:source-reliability="d"	admiralty-scale	1	0			
16	✔	✖	admiralty-scale:source-reliability="e"	admiralty-scale	0	0			
17	✔	✖	admiralty-scale:source-reliability="f"	admiralty-scale	4	2			
1203	✔	✖	adversary:infrastructure-action="monitoring-active"	adversary	1	0			
1201	✔	✖	adversary:infrastructure-action="passive-only"	adversary	0	0			

[2] https://www.misp-project.org/taxonomies.html

Correlation features: a tool for analysts

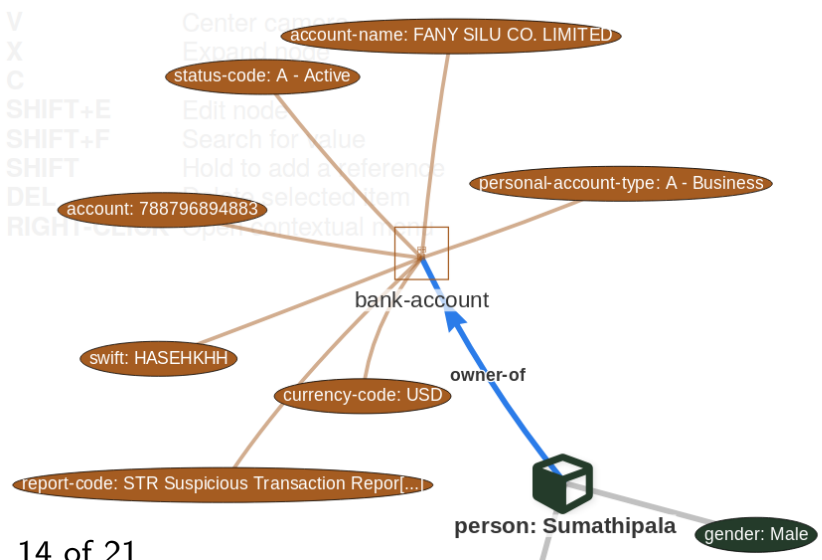


- To **corroborate a finding** (e.g. is this the same campaign?), **reinforce an analysis** (e.g. do other analysts have the same hypothesis?), **confirm a specific aspect** (e.g. are the sinkhole IP addresses used for one campaign?) or just find if this **threat is new or unknown in your community**.

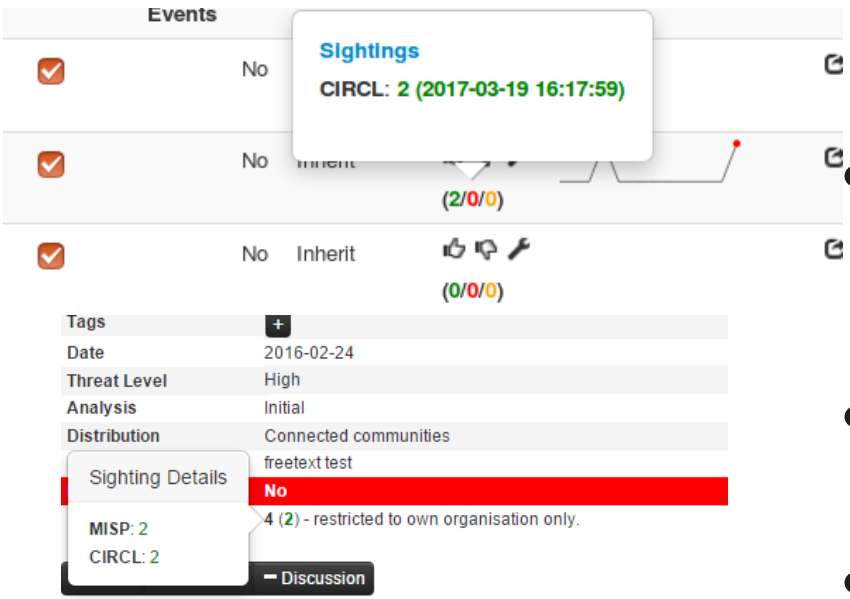
Supporting specific datamodel

Filters: All | File | Network | Financial | Proposal | Correlation | Warnings | Include deleted attributes | Show context fields

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
2018-09-28		Name: bank-account References: 0							
2018-09-28		Other	status-code: text	A - Active	+	Add		☐	
2018-09-28		Other	report-code: text	STR Suspicious Transaction Report	+	Add		☐	
2018-09-28		Other	personal-account-type: text	A - Business	+	Add		☐	
2018-09-28		Financial fraud	swift: bic	HASEHKHH	+	Add		☑	3849 11320 11584
2018-09-28		Financial fraud	account: bank-account-nr	788796894883	+	Add		☑	
2018-09-28		Other	account-name: text	FANY SILU CO. LIMITED	+	Add		☑	
2018-09-28		Other	currency-code: text	USD	+	Add		☐	



Sightings support



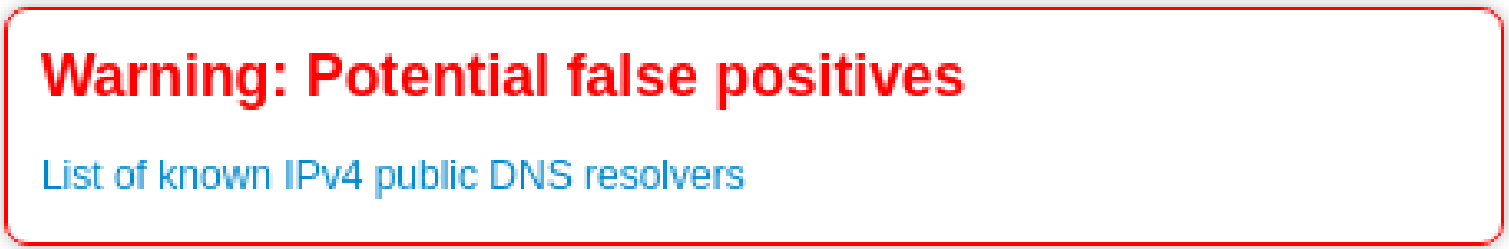
- Sightings allow users to notify the community about the activities related to an indicator.
- In recent MISP versions, the sighting system supports negative sigthings (FP) and expiration sightings.
- Sightings can be performed via the API, and the UI.
- Many use-cases for scoring indicators based on users sighting.

False-positive handling

- You might often fall into the trap of discarding seemingly "junk" data
- Besides volume limitations (which are absolutely valid, fear of false-positives is the most common reason why people discard data) - Our recommendation:
  - Be lenient when considering what to keep
  - Be strict when you are feeding tools
- **MISP allows you to filter out the relevant data** on demand when feeding protective tools
- What may seem like junk to you may be absolutely critical to other users

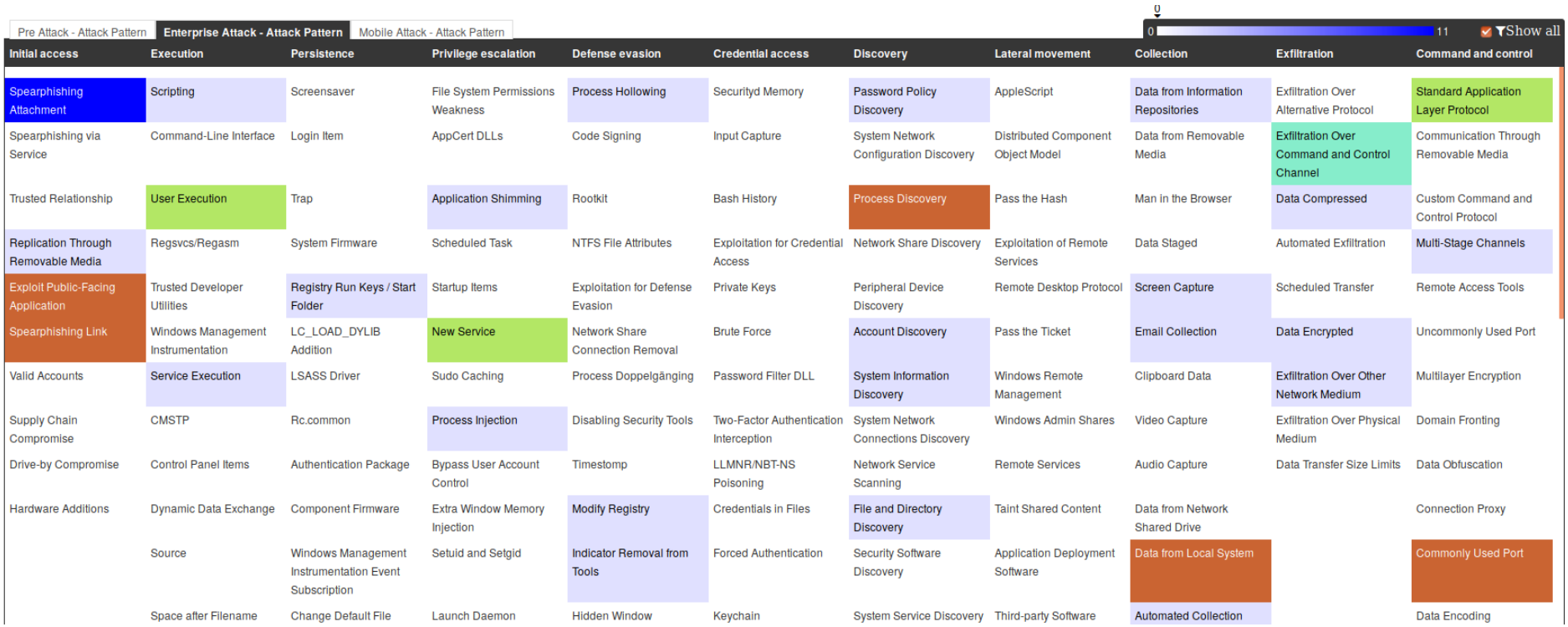
False-positive handling

- Analysts will often be interested in the **modus operandi of threat actors** over long periods of time
- Even cleaned up infected hosts might become interesting again (embedded in code, recurring reuse)
- Use the MISP warning-list feature to eliminate obvious false positives instead and limit your data-set to the most relevant sets



Sharing Attackers Techniques

- MISP integrates at event or attribute level MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK).



Pre Attack - Attack Pattern | **Enterprise Attack - Attack Pattern** | Mobile Attack - Attack Pattern

0 — 11 — Show all

Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Exfiltration	Command and control
Spearphishing Attachment	Scripting	Screensaver	File System Permissions Weakness	Process Hollowing	Securityd Memory	Password Policy Discovery	AppleScript	Data from Information Repositories	Exfiltration Over Alternative Protocol	Standard Application Layer Protocol
Spearphishing via Service	Command-Line Interface	Login Item	AppCert DLLs	Code Signing	Input Capture	System Network Configuration Discovery	Distributed Component Object Model	Data from Removable Media	Exfiltration Over Command and Control Channel	Communication Through Removable Media
Trusted Relationship	User Execution	Trap	Application Shimming	Rootkit	Bash History	Process Discovery	Pass the Hash	Man in the Browser	Data Compressed	Custom Command and Control Protocol
Replication Through Removable Media	Regsvcs/Regasm	System Firmware	Scheduled Task	NTFS File Attributes	Exploitation for Credential Access	Network Share Discovery	Exploitation of Remote Services	Data Staged	Automated Exfiltration	Multi-Stage Channels
Exploit Public-Facing Application	Trusted Developer Utilities	Registry Run Keys / Start Folder	Startup Items	Exploitation for Defense Evasion	Private Keys	Peripheral Device Discovery	Remote Desktop Protocol	Screen Capture	Scheduled Transfer	Remote Access Tools
Spearphishing Link	Windows Management Instrumentation	LC_LOAD_DYLIB Addition	New Service	Network Share Connection Removal	Brute Force	Account Discovery	Pass the Ticket	Email Collection	Data Encrypted	Uncommonly Used Port
Valid Accounts	Service Execution	LSASS Driver	Sudo Caching	Process Doppelgänging	Password Filter DLL	System Information Discovery	Windows Remote Management	Clipboard Data	Exfiltration Over Other Network Medium	Multilayer Encryption
Supply Chain Compromise	CMSTP	Rc.common	Process Injection	Disabling Security Tools	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Admin Shares	Video Capture	Exfiltration Over Physical Medium	Domain Fronting
Drive-by Compromise	Control Panel Items	Authentication Package	Bypass User Account Control	Timestomp	LLMNR/NBT-NS Poisoning	Network Service Scanning	Remote Services	Audio Capture	Data Transfer Size Limits	Data Obfuscation
Hardware Additions	Dynamic Data Exchange	Component Firmware	Extra Window Memory Injection	Modify Registry	Credentials in Files	File and Directory Discovery	Taint Shared Content	Data from Network Shared Drive		Connection Proxy
	Source	Windows Management Instrumentation Event Subscription	Setuid and Setgid	Indicator Removal from Tools	Forced Authentication	Security Software Discovery	Application Deployment Software	Data from Local System		Commonly Used Port
	Space after Filename	Change Default File	Launch Daemon	Hidden Window	Keychain	System Service Discovery	Third-party Software	Automated Collection		Data Encoding

Conclusion

- **Information sharing practices come from usage** and by example (e.g. learning by imitation from the shared information).
- Enabling users and organisations to customize MISP to meet their community's use-cases.
- CIRCL welcomes partnerships to improve MISP and build **new information sharing communities**.

Contact

- Getting started with building a new community can be daunting or want to provide feedback about MISP, don't hesitate to contact us:
- Contact: info@circl.lu
- `https://www.circl.lu/`
- `https://github.com/MISP` - `https://twitter.com/MISPProject`
- `https://github.com/CIRCL`