MISP - Open Source Threat Intelligence Sharing Platform

Supporting Law Enforcement Investigations

CIRCL / Team MISP Project

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

Interpol

MISP: Started 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**.

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

Many objectives from different user-groups

- Sharing indicators 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?*

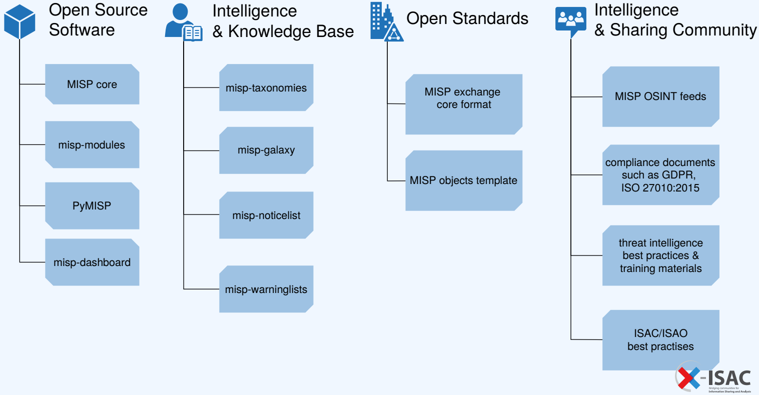
→ These objectives can be **conflicting**
(e.g. False-positives have different impacts)

Sharing Difficulties

- Sharing difficulties are not really technical issues but often it's a matter of **social interactions** (e.g. **trust**).
- Legal restriction[1]
  - *Our legal framework doesn't allow us to share information*
  - *Risk of information-leak is too high and it's too risky for our organization or partners.*
- Practical restriction
  - *We don't have information to share.*
  - *We don't have time to process or contribute indicators.*
  - *Our model of classification doesn't fit your model.*
  - *Tools for sharing information are tied to a specific format, we use a different one.*

[1] https://www.misp-project.org/compliance/

MISP Project Overview



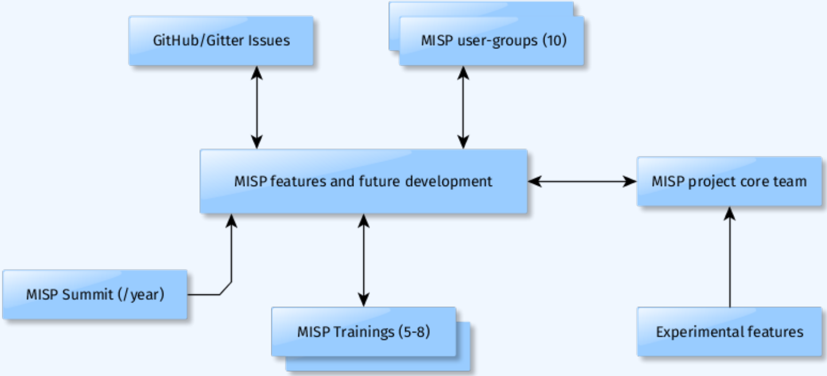
Open Source Software
- MISP core
- misp-modules
- PyMISP
- misp-dashboard

Intelligence & Knowledge Base
- misp-taxonomies
- misp-galaxy
- misp-noticelist
- misp-warninglists

Open Standards
- MISP exchange core format
- MISP objects template

Intelligence & Sharing Community
- MISP OSINT feeds
- compliance documents such as GDPR, ISO 27010:2015
- threat intelligence best practices & training materials
- ISAC/ISAO best practises

MISP MODEL OF GOVERNANCE



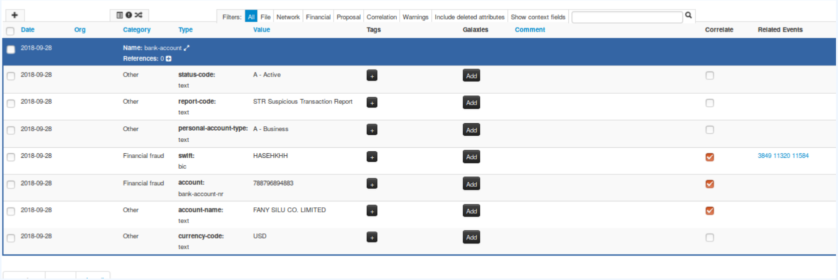
GETTING SOME NAMING CONVENTIONS OUT OF THE WAY...

- Data layer
  - **Events** are encapsulations for contextually linked information
  - **Attributes** are individual data points, which can be indicators or supporting data.
  - **Objects** are custom templated Attribute compositions
  - **Object references** are the relationships between other building blocks

Getting some naming conventions out of the way...

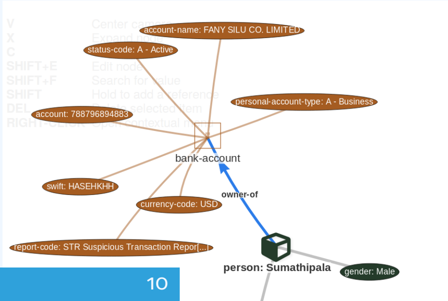
- Context layer
  - **Tags** are labels attached to events/attributes and can come from **Taxonomies**
    - `Android Malware`, C2, ...
  - **Taxonomies** are a set of common classification allowing to express the same vocabulary among a distributed set of users and organisations
    - `tlp:green`, `false-positive:risk="high"`, `gsma-fraud:technical="sim-card-cloning"`, `gsma-attack-category:spoofing`
  - **Galaxy-clusters** are knowledge base items used to label events/attributes and come from **Galaxies**. Basically a taxonomy with additional meta-information.
    - Typical **Galaxy-clusters**: **threat actors**, **preventive measures**, ...
    - `misp-galaxy:bhadra-framework="Billing frauds"`, `misp-galaxy:bhadra-framework="DNS-based attacks"`, `misp-galaxy:threat-actor="APT 29"`

A RICH DATA-MODEL: TELLING STORIES VIA RELATIONSHIPS

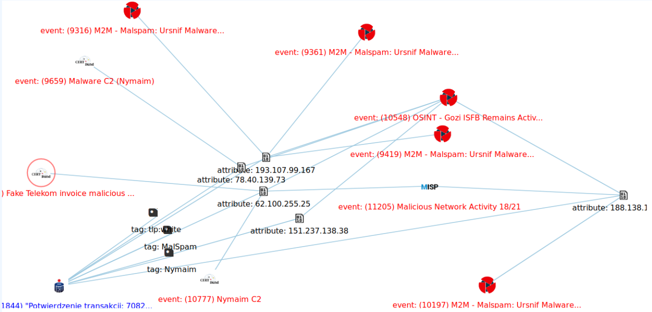


+
Filters: All File Network Financial Proposal Correlation Warnings Include deleted attributes Show context fields

☐	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		☐	



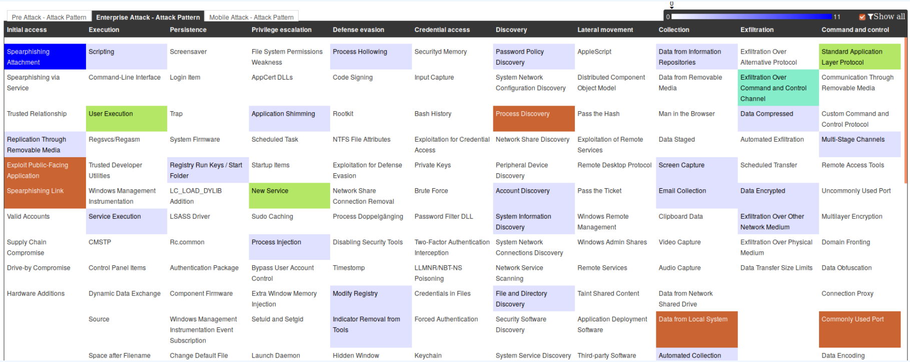
Correlation features: a tool for analysts


event: (9316) M2M - Malspam: Ursnif Malware...
event: (9361) M2M - Malspam: Ursnif Malware...
CERT Bund
event: (9659) Malware C2 (Nymaim)
event: (10548) OSINT - Gozi ISFB Remains Activ...
event: (9419) M2M - Malspam: Ursnif Malware...
attribute: 193.107.99.167
attribute: 78.40.139.73
CERT Bund
) Fake Telekom invoice malicious ...
attribute: 62.100.255.25
MISP
event: (11205) Malicious Network Activity 18/21
attribute: 188.138.1
attribute: 151.237.138.38
tag: tlp:white
tag: MalSpam
tag: Nymaim
CERT Bund
event: (10777) Nymaim C2
1844) "Potwierdzenie transakcji: 7082...
event: (10197) M2M - Malspam: Ursnif Malware...

- 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**.

Contextualisation and aggregation

- MISP integrates MITRE’s Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) and similar **Galaxy Matrix**



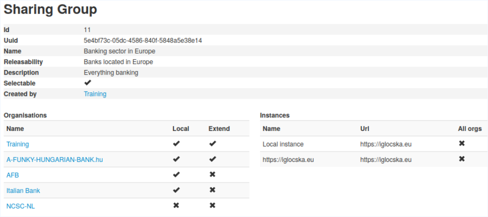
Pre Attack - Attack Pattern | Enterprise Attack - Attack Pattern | Mobile Attack - Attack Pattern

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

Sharing in MISP: Distribution

MISP offers granulars distribution settings:

- Organisation only
- This community
- Connected communities
- All communities
- Distribution lists - aka **Sharing groups**



Sharing Group

Id	11
Uuid	5e4bf73c-05dc-4586-840f-5848a5e38e14
Name	Banking sector in Europe
Releasability	Banks located in Europe
Description	Everything banking
Selectable	✔
Created by	Training

Organisations

Name	Local	Extend
Training	✔	✔
A-FUNKY-HUNGARIAN-BANK.hu	✔	✔
AFB	✔	✖
Italian Bank	✔	✖
NCSC-NL	✖	✖

Instances

Name	Url	All orgs
Local instance	https://iglocska.eu	✖
https://iglocska.eu	https://iglocska.eu	✖

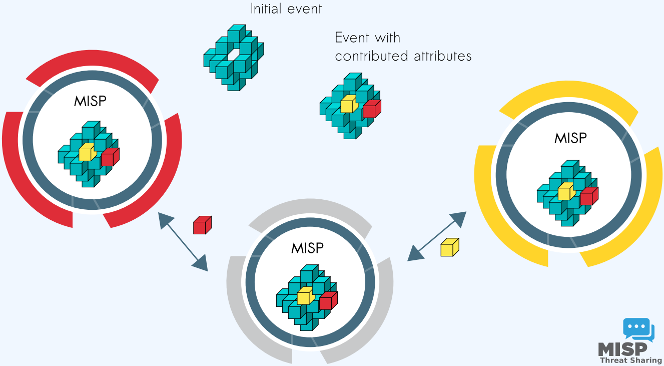
At multiple levels: Events, Attributes and Objects (and their Attributes)

Sharing in MISP: Advanced usage

- **Delegation** for pseudo-anonymised information sharing
- **Proposals** and **Extended events** for collaborated information sharing
- 2-way 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

MISP core distributed sharing functionality

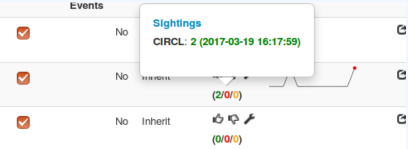
- MISP's core functionality is sharing where everyone can be a consumer and/or a contributor/producer.
- Quick benefit without the obligation to contribute.
- Low barrier access to get acquainted to the system.



Information quality management

- Correlating data
- Feedback loop from detections via **Sightings**
- **False positive management** via the warninglist system
- **Enrichment system** via MISP-modules
- **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**

Sightings support

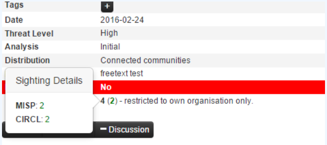


Events

☑	No		
☑	No	Inherit	(2/0/0)
☑	No	Inherit	(0/0/0)

Sightings

CIRCL: 2 (2017-03-19 16:17:59)



Tags	+
Date	2016-02-24
Threat Level	High
Analysis	Initial
Distribution	Connected communities
	freetext test
	No
	4 (2) - restricted to own organisation only.

Sighting Details

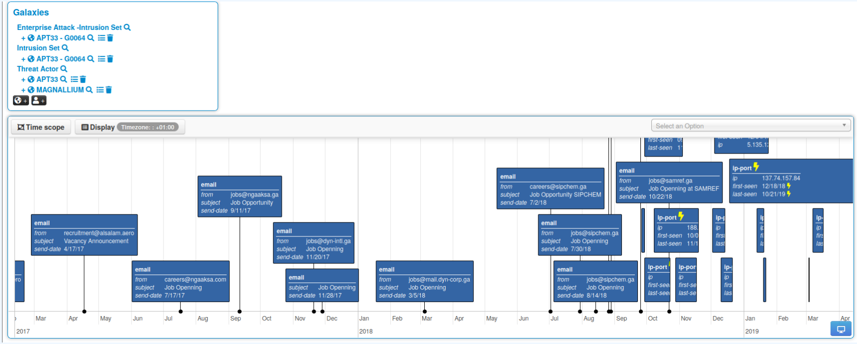
MISP: 2

CIRCL: 2

- *Has a data-point been* ***sighted*** *by me or the community before?*
- Additionally, the sighting system supports negative sigthings (FP) and expiration sightings.
- Sightings can be performed via the API or the UI.
- Many use-cases for **scoring indicators** based on users sighting.
- For large quantities of data, **SightingDB** by Devo

Timelines and giving information a temporal context

- Recently introduced **first_seen** and **last_seen** data points
- All data-points can be placed in time
- Enables the **visualisation** and **adjustment** of indicators timeframes



Galaxies

Enterprise Attack -Intrusion Set
+ APT33 - G0064
Intrusion Set
+ APT33 - G0064
Threat Actor
+ APT33
+ MAGNALLIUM

email
from recruitment@alsalam.aero
subject Vacancy Announcement
send-date 4/17/17

email
from careers@ngaaksa.com
subject Job Openning
send-date 7/17/17

email
from jobs@ngaaksa.ga
subject Job Opportunity
send-date 9/11/17

email
from jobs@dyn-intl.ga
subject Job Openning
send-date 11/20/17

email
subject Job Openning
send-date 11/28/17

email
from jobs@mail.dyn-corp.ga
subject Job Openning
send-date 3/5/18

email
from careers@sipchem.ga
subject Job Opportunity SIPCHEM
send-date 7/2/18

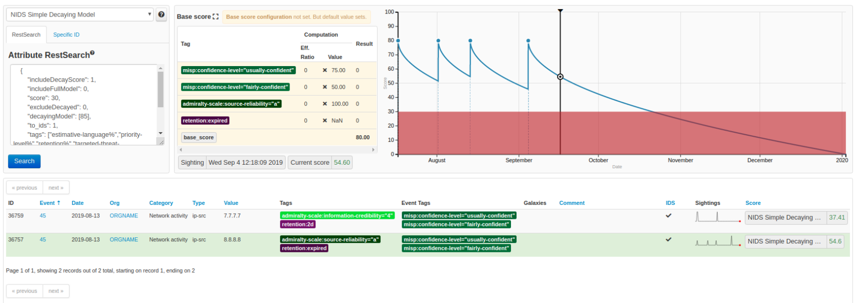
email
from jobs@sipchem.ga
subject Job Openning
send-date 7/30/18

email
from jobs@sipchem.ga
subject Job Openning
send-date 8/14/18

email
from jobs@samref.ga
subject Job Openning at SAMREF
send-date 10/22/18

ip-port
ip 137.74.157.84
first-seen 12/18/18
last-seen 10/21/19

Life-cycle management via decaying of indicators



NIDS Simple Decaying Model

RestSearch | Specific ID

Attribute RestSearch

```
{
    "includeDecayScore": 1,
    "includeFullModel": 0,
    "score": 30,
    "excludeDecayed": 0,
    "decayingModel": [85],
    "to_ids": 1,
    "tags": ["estimative-language%","priority-
level%","retention%","targeted-threat-
```

Search

Base score — **Base score configuration** not set. But default value sets.

Tag	Computation		Result
	Eff. Ratio	Value	
misp:confidence-level="usually-confident"	0	× 75.00	0
misp:confidence-level="fairly-confident"	0	× 50.00	0
admiralty-scale:source-reliability="a"	0	× 100.00	0
retention:expired	0	× NaN	0
base_score			80.00

Sighting: Wed Sep 4 12:18:09 2019 | Current score: 54.60

« previous | next »

ID	Event ↑	Date	Org	Category	Type	Value	Tags	Event Tags	Galaxies	Comment	IDS	Sightings	Score
36759	45	2019-08-13	ORGNAME	Network activity	ip-src	7.7.7.7	admiralty-scale:information-credibility="4" retention:2d	misp:confidence-level="usually-confident" misp:confidence-level="fairly-confident"			✓		NIDS Simple Decaying ... 37.41
36757	45	2019-08-13	ORGNAME	Network activity	ip-src	8.8.8.8	admiralty-scale:source-reliability="a" retention:expired	misp:confidence-level="usually-confident" misp:confidence-level="fairly-confident"			✓		NIDS Simple Decaying ... 54.6

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

« previous | next »

Expiration based on user-defined *Models*

DFIR and MISP digital evidences

- **Share analysis and report** of digital forensic evidences.
- **Propose changes** to existing analysis or report.
- Extending existing event with additional evidences for local or limited use (sharing can be defined at event level or attribute level).
- **Evaluate correlations**[2] of evidences against external or existing attributes.
- **Report sighting** such as false-positive or true-positive (e.g. a partner/analyst has seen a similar indicator).

[2] MISP has a flexible correlation engine which can correlate on 1-to-1 value but also fuzzy hashing (e.g. ssdeep) or CIDR block matching.

Benefits of using MISP

- LE can leverage the long-standing experience in information sharing and **bridge their use-cases** with MISP's information sharing mechanisms.
- **Accessing existing MISP information sharing communities** by getting actionable information from CSIRTs/CERTs networks or security researchers.
- **Bridging LE communities with other communities**. Sharing groups can be created (and managed) between cross-sectors to support specific use-cases.
- **MISP standard format** is a flexible format which can be extended by the users who use the MISP platform. A MISP object template can be created in 30 minutes and directly share information with your model towards existing communities.

Future of Information Sharing

- MISP is a long-term project (started in 2012) and since **information sharing is becoming more essential** than ever to thwart threats, we have long-term plans for the project as the project is used in various critical information exchange communities
- We hope to have the means to be the enablers and the interface for real cross-sectorial sharing and support the organisations facing hybrid threats
- Tools, open standards and interoperable software (e.g. DFIR tools) are driving forces behind resilient information exchange communities
- Getting ideas and practical **use-cases from LE community** is vital, don't hesitate to contact us