

AN INTRODUCTION TO CYBERSECURITY INFORMATION SHARING

MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

MISP PROJECT

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

CIISI-IE



MISP
Threat Sharing

- Agenda and details available
<https://tinyurl.com/CIISI-IE-MISP>

- 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.**

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.

- 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

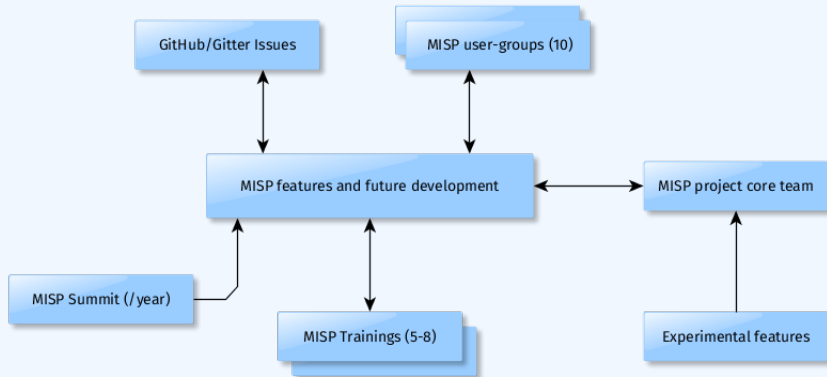
Connecting Europe Facility

WHAT IS MISP?

- 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

- 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.

MISP MODEL OF GOVERNANCE



- 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)

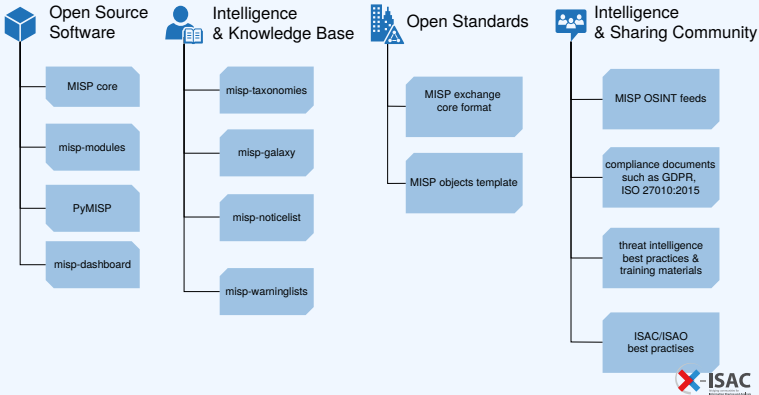
COMMUNITIES USING MISP

- 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)

- Sharing difficulties are not really technical issues but often it's a matter of **social interactions** (e.g. **trust**).
- Legal restriction¹
 - ▶ "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."

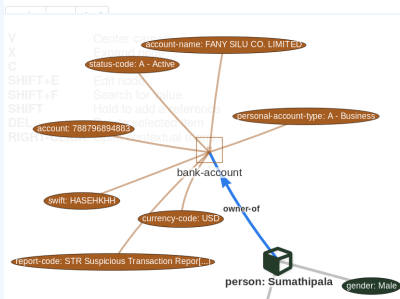
¹<https://www.misp-project.org/compliance/>

MISP PROJECT OVERVIEW



A RICH DATA-MODEL: TELLING STORIES VIA RELATIONSHIPS

| Date | Org | Category | Type | Value | Tags | Galaxies | Comment | Correlate | Related Events |
|------------|-----|-----------------|------------------------|-----------------------------------|------|----------|---------|-------------------------------------|------------------|
| 2018-09-28 | | Other | status-code: | A - Active | | Add | | <input type="checkbox"/> | |
| 2018-09-28 | | Other | report-code: | STR Suspicious Transaction Report | | Add | | <input type="checkbox"/> | |
| 2018-09-28 | | Other | personal-account-type: | A - Business | | Add | | <input type="checkbox"/> | |
| 2018-09-28 | | Financial fraud | swift: | HASEH09H | | Add | | <input checked="" type="checkbox"/> | 3849 11320 11584 |
| 2018-09-28 | | Financial fraud | account: | 788796894883 | | Add | | <input checked="" type="checkbox"/> | |
| 2018-09-28 | | Other | account-name: | FANY SILU CO. LIMITED | | Add | | <input checked="" type="checkbox"/> | |
| 2018-09-28 | | Other | currency-code: | USD | | Add | | <input type="checkbox"/> | |



CONTEXTUALISATION AND AGGREGATION

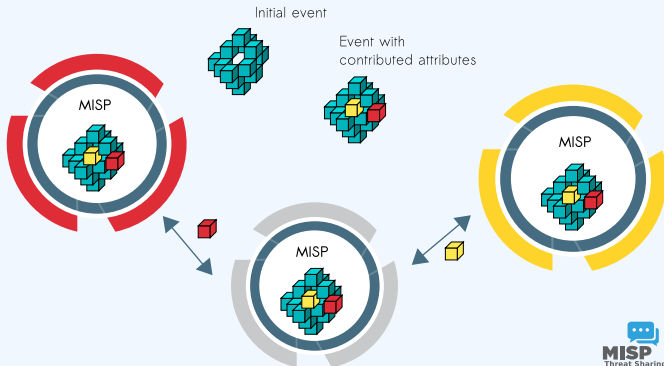
- MISP integrates at the event and the attribute levels MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK).

| 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 | Security 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 | Rookit | 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 Doppelgänger | Password Filter DLL | System Information Discovery | Windows Remote Management | Clipboard Data | Exfiltration Over Other Network Medium | Multi-layer 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 | Timestamp | 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 | Tairt 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 | Keypchain | System Service Discovery | Third-party Software | Automated Collection | | Data Encoding |

- 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

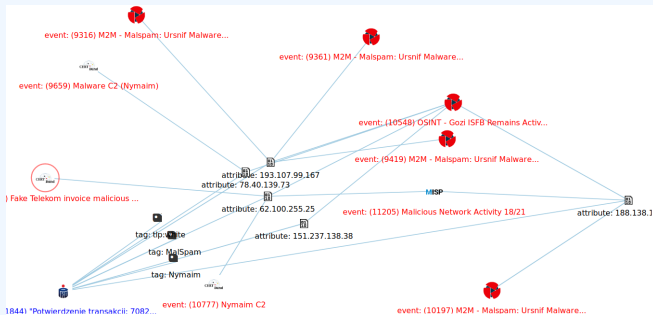
MISP CORE DISTRIBUTED SHARING FUNCTIONALITY

- 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.



- 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**

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.**

The screenshot displays the SightingDB interface. At the top, there is a table of events with columns for status, sighting status, and inheritance. A tooltip for a sighting shows the following details:

- Sightings**
- CIRCL: 2 (2017-03-19 16:17:59)**
- Score: (2/0/0)
- Score: (0/0/0)

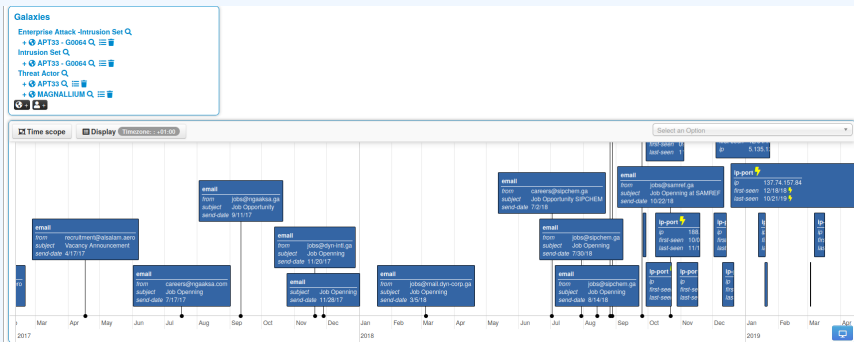
Below the table, there is a section for tags and a detailed view of a sighting:

- Tags**: +
- Date**: 2016-02-24
- Threat Level**: High
- Analysis**: Initial
- Distribution**: Connected communities
- Sighting Details**: No
- MISP: 2**: 4 (2) - restricted to own organisation only.
- CIRCL: 2**
- Discussion**

- Has a data-point been **sighted** by me or the community before?
- Additionally, the sighting system supports negative sightings (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



LIFE-CYCLE MANAGEMENT VIA DECAYING OF INDICATORS

The screenshot displays a web interface for managing indicators. At the top, there are navigation tabs: "Photos", "Galaxy", "Event graph", "Correlation graph", "ATTACK matrix", "Attributes", and "Discussion". Below this, a search bar contains the text "45: Decay...". A "Galaxies" section is visible with a search icon and a plus sign. Below that, there are navigation buttons: "previous", "next >", and "view all".

The main content area features a table with columns: "Date", "Org", "Category", "Type", "Value", "Tags", "Galaxies", "Comment", "Correlate", "Related Events", "Feed hits", "IDS", "Distribution", "Sightings", "Activity", "Score", and "Actions". The table is filtered by "Decay score" and "Context".

The table contains five rows of data. Each row has a "Decay score" column with a toggle button (a circle with a plus sign) and a "Score" column with a numerical value. The "Decay score" column also shows a "NIDS Simple Decaying ..." label and a "Model 5" label. The "Score" column shows a numerical value and a "Model 5" label.

| Date | Org | Category | Type | Value | Tags | Galaxies | Comment | Correlate | Related Events | Feed hits | IDS | Distribution | Sightings | Activity | Score | Actions |
|------------|-----|------------------|--------|---------|--|----------|---------|-----------|--|-----------|-----|--------------|-----------|----------|-------|---------|
| 2019-09-12 | | Network activity | ip-src | 5.5.5.5 | | | | | | | | Inherit | (0/0) | | 65.26 | |
| 2019-08-13 | | Network activity | ip-src | 8.8.8.8 | adm_rality_scale:source-reliability="A" x retention:expired x | | | | 1 2 2 2 Show S1.1 S1.2 11 more... | | | Inherit | (5/0) | | 54.6 | |
| 2019-08-13 | | Network activity | ip-src | 9.9.9.9 | adm_rality_scale:source-reliability="C" x msp:confidence-level="completely-confident" x Ipnumber | | | | 1 3 1 9 Show S1.1 28 more... | | | Inherit | (4/1) | | 37.43 | |
| 2019-08-13 | | Network activity | ip-src | 7.7.7.7 | adm_rality_scale:information-credibility="4" x retention:20 x | | | | 41 | | | Inherit | (3/0) | | 37.41 | |
| 2019-07-18 | | Network activity | ip-src | 6.6.6.6 | | | | | 41 | | | Inherit | (0/0) | | 23.31 | |

■ Decay score toggle button

- ▶ Shows Score for each Models associated to the Attribute type

DECAYING OF INDICATORS: FINE TUNING TOOL

Decaying Of Indicator Fine Tuning Tool

Attribute Type | Category | Model ID

| Attribute Type | Category | Model ID |
|---------------------|------------------|----------|
| aba_rtn | Financial fraud | |
| authen@hash | Payload delivery | |
| bank-account-ir | Financial fraud | |
| bc | Financial fraud | |
| bin | Financial fraud | |
| bro | Network activity | 10 11 |
| bc | Financial fraud | 11 |
| cc-number | Financial fraud | |
| cd@hash | Payload delivery | |
| community-id | Network activity | |
| domain | Network activity | |
| domain@ip | Network activity | 10 94 |
| email-attachment | Payload delivery | |
| email-@ip | Network activity | 11 |
| email-@ic | Payload delivery | |
| headers | Payload delivery | |
| headers@authen@hash | Payload delivery | |
| headers@ip@fuzzy | Payload delivery | |
| headers@ip@hash | Payload delivery | |
| headers@ip@rds | Payload delivery | 12 |
| headers@ip@hash | Payload delivery | 13 |
| headers@ip@h1 | Payload delivery | 13 |

Polynomial

Score

Days

Lifetime: 3 days

Decay speed: 2.3

Cutoff threshold: 30

Expire after (lifetime): 1 days and 7 hours

Score halved after (Half-life): 0 day and 6 hours

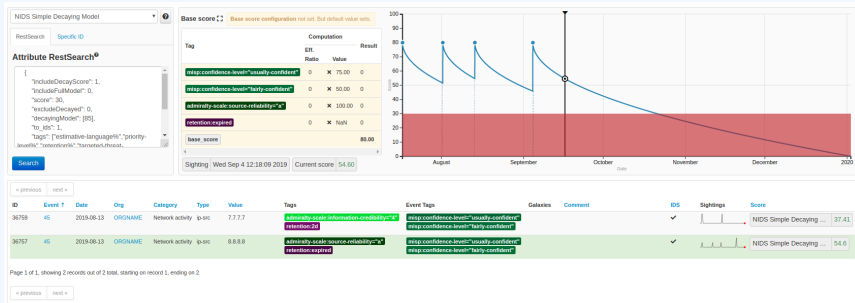
Adjust base score | Simulate this model

Phishing model | Simple model to rapidly decay | Edit

| Parameters | | | | | | | | | | | | | |
|------------|----------------|--------|---|------------|----------|-------------|-----------|-------------------|----------------------------|----------|---------|---------|------------|
| ID | Model Name | Org ID | Description | Formula | Lifetime | Decay speed | Threshold | Default basescore | Basescore config | Settings | # Types | Enabled | Action |
| 29 | Phishing model | 1 | Simple model to rapidly decay phishing website. | Polynomial | 3 | 2.3 | 30 | 80 | estimate-language phishing | 0.5 | 0.5 | ✓ | Edit model |

Create, modify, visualise, perform mapping

DECAYING OF INDICATORS: SIMULATION TOOL



Simulate *Attributes* with different Models

- We maintain the default CIRCL OSINT feeds (TLP:WHITE selected from our communities) in MISP to allow users to ease their bootstrapping.
- The format of the OSINT feed is based on standard MISP JSON output pulled from a remote TLS/HTTP server.
- Additional content providers can provide their own MISP feeds. (<https://botvrij.eu/>)
- Allows users to **test their MISP installations and synchronisation with a real dataset.**
- Opening contribution to other threat intel feeds but also allowing the analysis of overlapping data².

²A recurring challenge in information sharing

- **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.