

# AN INTRODUCTION TO CYBERSECURITY INFORMATION SHARING

MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

MISP PROJECT

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

MISP PROJECT



2022-09-16

An Introduction to Cybersecurity Information Sharing

AN INTRODUCTION TO CYBERSECURITY INFORMATION SHARING

MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

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

MISP PROJECT



- Agenda and details available <https://hdoc.csirt-tooling.org/tq-qyvTQTLeZowy-OPXjiw?view>

- 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 Vandeplass (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.**

2022-09-16

## An Introduction to Cybersecurity Information Sharing

└ 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 Vandeplass (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](https://www.securitymadein.lu) g.i.e.

2022-09-16

## An Introduction to Cybersecurity Information 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](https://www.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

- 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

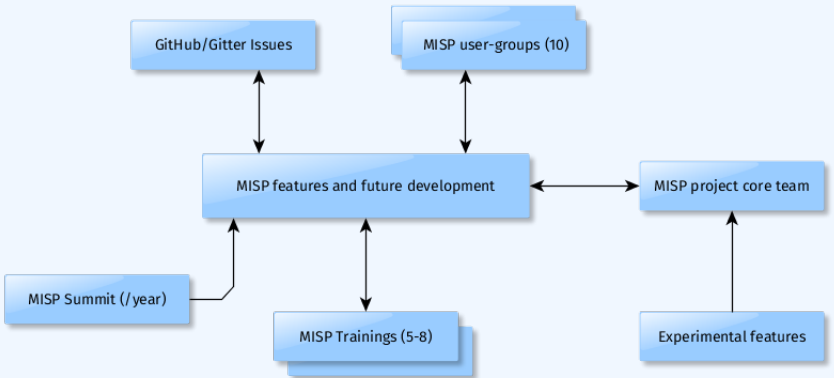
- There are many different types of users of an information sharing platform like MISP:
  - ▶ **Malware reversers** willing to share indicators of analysis with respective colleagues.
  - ▶ **Security analysts** searching, validating and using indicators in operational security.
  - ▶ **Intelligence 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.

└ 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, 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)

└ 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)

- 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)

### └ Communities using MISP

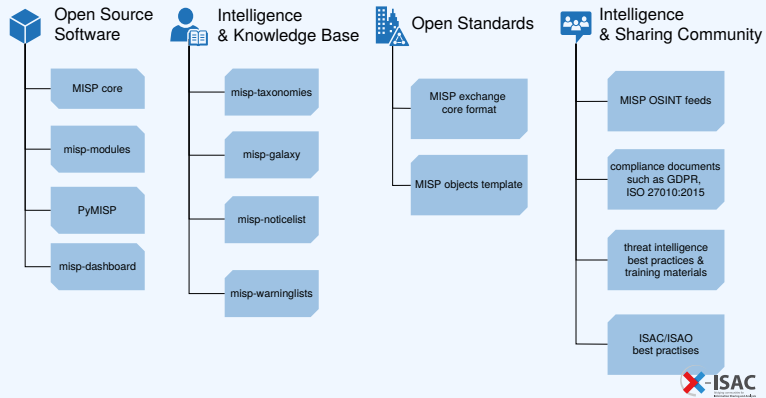
- Communities are groups of users sharing within a set of common objectives/values.
- CIRCL operates multiple MISP instances with a significant user base (more than 1200 organizations with more than 4000 users).
- **Trusted groups** running MISP communities in island mode (air gapped system) or partially 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 restriction<sup>1</sup>
  - ▶ "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."

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

### └ Sharing Difficulties

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



### MISP Project Overview



# 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
- ▶ **Sightings** are time-specific occurrences of a given data-point detected

## ■ Context layer

- ▶ **Tags** are labels attached to events/attributes and can come from **Taxonomies**
- ▶ **Galaxy-clusters** are knowledge base items used to label events/attributes and come from **Galaxies**
- ▶ **Cluster relationships** denote pre-defined relationships between clusters

2022-09-16

## An Introduction to Cybersecurity Information Sharing

└ Getting some naming conventions out of the way...

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
  - ▶ **Sightings** are time-specific occurrences of a given data-point detected
- Context layer
  - ▶ **Tags** are labels attached to events/attributes and can come from **Taxonomies**
  - ▶ **Galaxy-clusters** are knowledge base items used to label events/attributes and come from **Galaxies**
  - ▶ **Cluster relationships** denote pre-defined relationships between clusters

## ■ Indicators<sup>2</sup>

- ▶ Indicators contain a pattern that can be used to detect suspicious or malicious cyber activity.

## ■ Attributes in MISP can be network indicators (e.g. IP address), system indicators (e.g. a string in memory) or even bank account details.

- ▶ **A type (e.g. MD5, url) is how an attribute is described.**
- ▶ An attribute is always in a category (e.g. Payload delivery) which puts it in a context.
  - **A category is what describes** an attribute.
- ▶ An IDS flag on an attribute allows to determine if **an attribute can be automatically used for detection.**

<sup>2</sup>IoC (Indicator of Compromise) is a subset of indicators

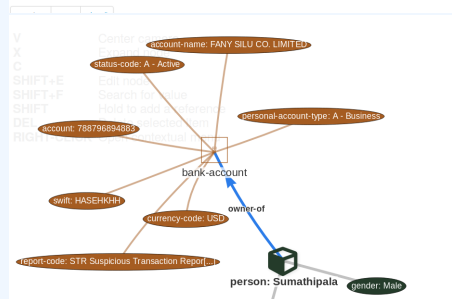
### └ Terminology about Indicators

- Indicators<sup>2</sup>
  - ▶ Indicators contain a pattern that can be used to detect suspicious or malicious cyber activity.
- Attributes in MISP can be network indicators (e.g. IP address), system indicators (e.g. a string in memory) or even bank account details.
  - ▶ **A type (e.g. MD5, url) is how an attribute is described.**
  - ▶ An attribute is always in a category (e.g. Payload delivery) which puts it in a context.
    - **A category is what describes** an attribute.
  - ▶ An IDS flag on an attribute allows to determine if **an attribute can be automatically used for detection.**

<sup>2</sup>IoC (Indicator of Compromise) is a subset of indicators

# A RICH DATA-MODEL: TELLING STORIES VIA RELATIONSHIPS

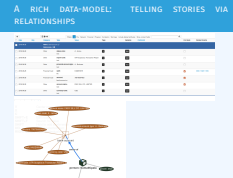
| Date       | Org | Category        | Type                   | Value                             | Tags | Galaxies | Comment | Correlate                           | Related Events   |
|------------|-----|-----------------|------------------------|-----------------------------------|------|----------|---------|-------------------------------------|------------------|
| 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:                 | HASEH00H                          |      | 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"/>            |                  |



2022-09-16

## An Introduction to Cybersecurity Information Sharing

└ A rich data-model: telling stories via relationships



- 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                    | Keychain                               | System Service Discovery               | Third-party Software               | Automated Collection               |   | Data Encoding                         |

2022-09-16

## An Introduction to Cybersecurity Information Sharing

Contextualisation and aggregation

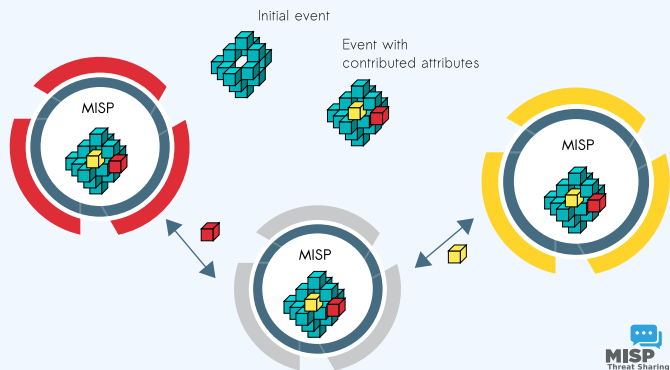
MISP integrates at the event and the attribute levels MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK).



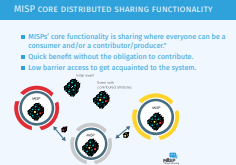
- Sharing via distribution lists - **Sharing groups**
- **Delegation** for pseudo-anonymised information sharing
- **Proposals** and **Extended events** for collaborated information sharing
- Synchronisation, Feed system, air-gapped sharing
- User defined **filtered sharing** for all the above mentioned methods
- Cross-instance information **caching** for quick lookups of large data-sets
- Support for multi-MISP internal enclaves

- 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

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



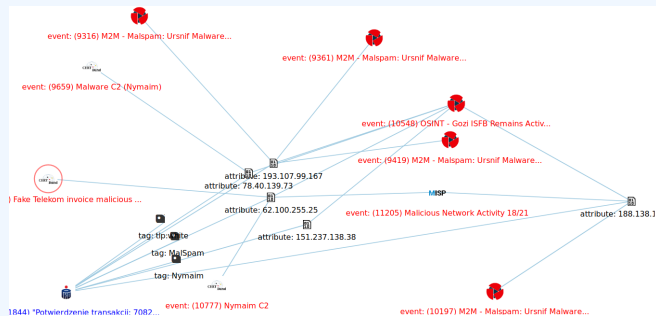
└ MISP core distributed sharing functionality



- 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**

### └ 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**



- 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.

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.

### Sightings support

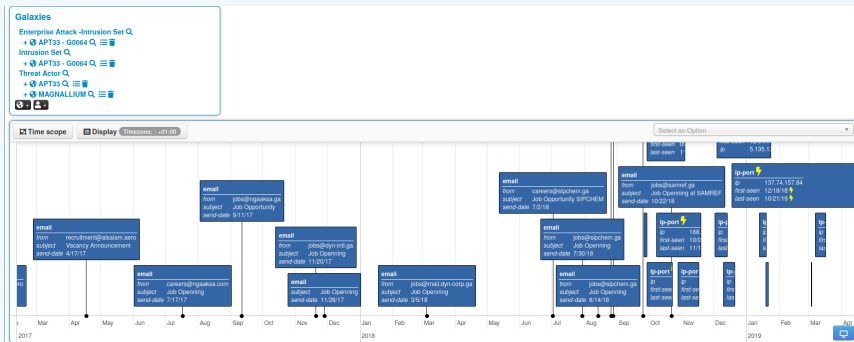
- Has a data-point been **sighted** by me or the community before?
- Additionally, the sighting system supports negative sightings (FP) and expiration sightings.
- Sightings can be performed via the API or the UI.
- Many use-cases for **scoring indicators** based on users sighting
- For large quantities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

The screenshot displays the Sighting system interface. At the top, there is a table of events with columns for 'Events', 'Sightings', and 'CIRCL: 2 (2017-03-19 16:17:59)'. Below the table, there are sections for 'Tags', 'Date', 'Threat Level', 'Analysis', and 'Distribution'. A 'Sighting Details' popup is visible, showing 'No' as the sighting status, 'MISP: 2' and 'CIRCL: 2' as indicators, and '4 (2) - restricted to own organisation only.' as a count. A 'Discussion' button is also present.

- 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



2022-09-16

## An Introduction to Cybersecurity Information Sharing

└ Timelines and giving information a temporal context

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 these is a "Decay" filter set to "45". A search box labeled "Galaxies" is present. 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 lists several indicators with their respective scores and associated models. A "Decay score toggle button" is visible in the top right of the table area.

| 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)     |          | NIDS Simple Decaying ... 65.26<br>Model 5 79.88 |         |
| 2019-08-13 |     | Network activity | ip-src | 8.8.8.8 | adm:admiralty-scale:source-reliability="A" x<br>retention:expired x  |          |         |           | 1 2 2 2<br>Show<br>S1.1<br>S1.2<br>11<br>more... |           | Inherit |              | (5/0)     |          | NIDS Simple Decaying ... 54.6<br>Model 5 52.69  |         |
| 2019-08-13 |     | Network activity | ip-src | 9.9.9.9 | adm:admiralty-scale:source-reliability="C" x<br>msp:confidence-level="completely-confident" x<br>ip:remember x |          |         |           | 1 3 19<br>Show<br>S1.1<br>28<br>more...          |           | Inherit |              | (4/1)     |          | NIDS Simple Decaying ... 37.43<br>Model 5 0     |         |
| 2019-08-13 |     | Network activity | ip-src | 7.7.7.7 | adm:admiralty-scale:information-credibility="4" x<br>retention:20 x  |          |         |           | 41   |           | Inherit |              | (3/0)     |          | NIDS Simple Decaying ... 37.41<br>Model 5 0     |         |
| 2019-07-18 |     | Network activity | ip-src | 6.6.6.6 |  |          |         |           | 41   |           | Inherit |              | (0/0)     |          | NIDS Simple Decaying ... 23.31<br>Model 5 0     |         |

- Decay score toggle button
  - ▶ Shows Score for each Models associated to the Attribute type

2022-09-16

## An Introduction to Cybersecurity Information Sharing

Life-cycle management via decaying of indicators

A small thumbnail version of the dashboard interface shown in the main screenshot, located in the top right corner of the slide.

# DECAYING OF INDICATORS: FINE TUNING TOOL

Home | Event Actions | Alerts | Host Filters | Global Actions | Sync Actions | Administration | Audit

Import Decaying Model  
Add Decaying Model  
Decaying Tool  
List Decaying Models

## Decaying Of Indicator Fine Tuning Tool

Show All Types | Show MISP Objects | Search Attribute Type

| Attribute Type      | Category         | Model ID |
|---------------------|------------------|----------|
| aba-rtn             | Financial fraud  |          |
| authen@hash         | Payload delivery |          |
| bank-account-iv     | Financial fraud  |          |
| bc                  | Financial fraud  |          |
| bn                  | Financial fraud  |          |
| bn                  | Network activity | 10 11    |
| bc                  | Financial fraud  | 11       |
| cc-number           | Financial fraud  |          |
| cdhash              | Payload delivery |          |
| community-id        | Network activity |          |
| domain              | Network activity |          |
| domain@p            | Network activity | 10 94    |
| email-attachment    | Payload delivery |          |
| email-otp           | Network activity | 11       |
| email-otp           | Payload delivery |          |
| headers             | Payload delivery |          |
| headers/authen@hash | Payload delivery |          |
| headers@p@fuzzy     | Payload delivery |          |
| headers@p@hash      | Payload delivery |          |
| headers@p@t5        | Payload delivery | 12       |
| headers@p@hash      | Payload delivery | 13       |
| headers@p@h1        | Payload delivery | 13       |

Polynomial

Adjust base score | Simulate this model

Phishing model | Simple model to rapidly decay | Edit

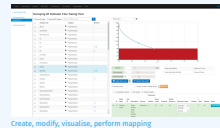
| Parameters |                |        |  |            |          |             |           |                   |                   |          |         |         |        |   |            |
|------------|----------------|--------|--|------------|----------|-------------|-----------|-------------------|-------------------|----------|---------|---------|--------|---|------------|
| Model ID   | 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 using phishing website | Polynomial | 3        | 2.3         | 30        | 80                | estimate-language | phishing | 0.5     | 0.5     | 3      | ✓ | Load model |

Create, modify, visualise, perform mapping

2022-09-16

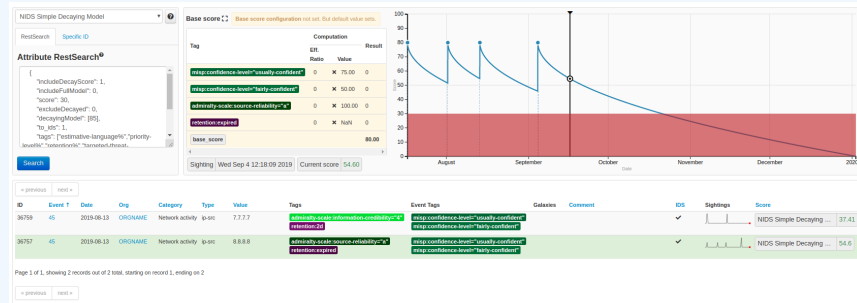
## An Introduction to Cybersecurity Information Sharing

Decaying of indicators: Fine tuning tool





# DECAYING OF INDICATORS: SIMULATION TOOL



Simulate Attributes with different Models

2022-09-16

## An Introduction to Cybersecurity Information Sharing

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 data<sup>3</sup>.

<sup>3</sup>A recurring challenge in information sharing

### └─ Bootstrapping your MISP with data

- 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 data<sup>3</sup>.

<sup>3</sup>A 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.

- 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.