10 years of MISP

What’s next in threat intelligence information sharing?

CIRCL / Team MISP Project

ENISA CTI-EU

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** and **connects** the data
- Allows teams and communities to **collaborate** and **share**
- **Feeds** automated protective tools and analyst tools with the output
- MISP is a **complete threat intelligence platform** with strong sharing capabilities and extendability

Two years from now, threat intelligence will be easy.

Bill Gates if he did work in threat intelligence

The aim of this presentation

- Showing the **evolution of threat intelligence**[1] and
- **data-driven threat hunting** over the past years
- What can we expect in **the future**?

[1] based on our empirical view from users using/integrating MISP

From standalone indicator to advanced object data models

- In early 2010, MISP supported basic indicators sharing with a limited set of types
- In 2022, MISP integrates a dynamic object model with advanced custom relationships
- Why such evolution?
  - **Increase of intelligence usage in different sectors**. From threat-hunting[2] to risk assessment or strategic decisions
  - **Increased diversity among analysts**

[2] With different types of threat hunts including TTP-driven, intelligence-driven, asset-driven...

Multitude of intelligence models

- Chains, triangles, circles, diamonds, arrows, a mix or even a multi-layer matrix
- There is **no perfect intelligence models**
- Organisations invent their model, reuse existing ones or are even more creative
- Showing **how diverse**[3] **our societies are**

[3] Embrace the diversity of models, taxonomies

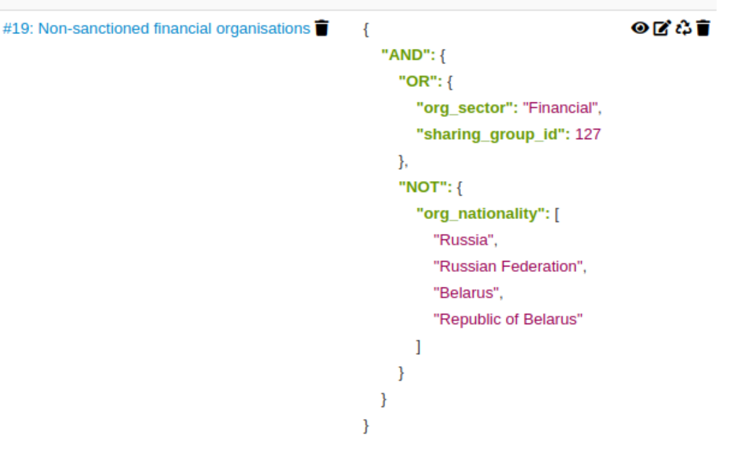
Main focus was securing our data and tooling

- Current **geo-political situation** lead to new challenges
- It has been an interesting time period with quite some activity
- Our goal was to **shore up the security** aspects of MISP and Cerebrate
- Build new functionalities and tools to allow users to **protect their data**

Sharing group blueprints

- Solving the issue of **sharing group lifecycle management**
- Build SG blueprints for reusable, maintainable sharing groups
- Abstract sharing groups, organisation metadata as building blocks
- Solve newly arising sharing challenges

Sharing group blueprints



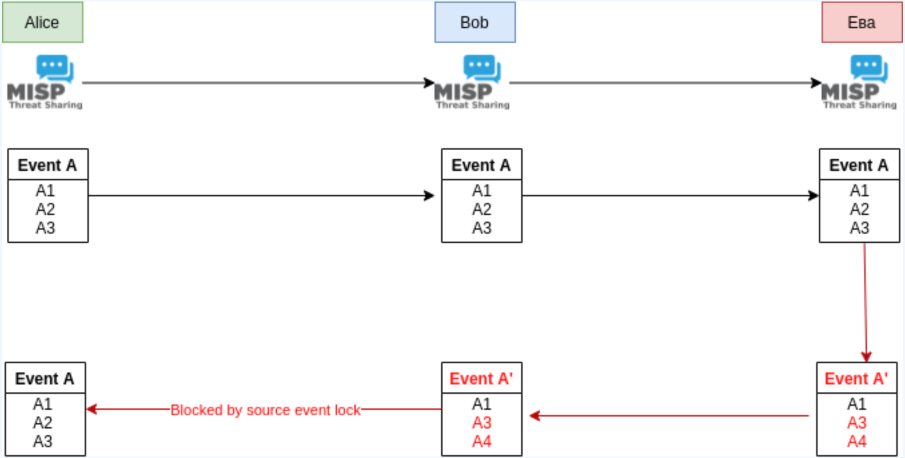
#19: Non-sanctioned financial organisations

```
{
    "AND": {
        "OR": {
            "org_sector": "Financial",
            "sharing_group_id": 127
        },
        "NOT": {
            "org_nationality": [
                "Russia",
                "Russian Federation",
                "Belarus",
                "Republic of Belarus"
            ]
        }
    }
}
```

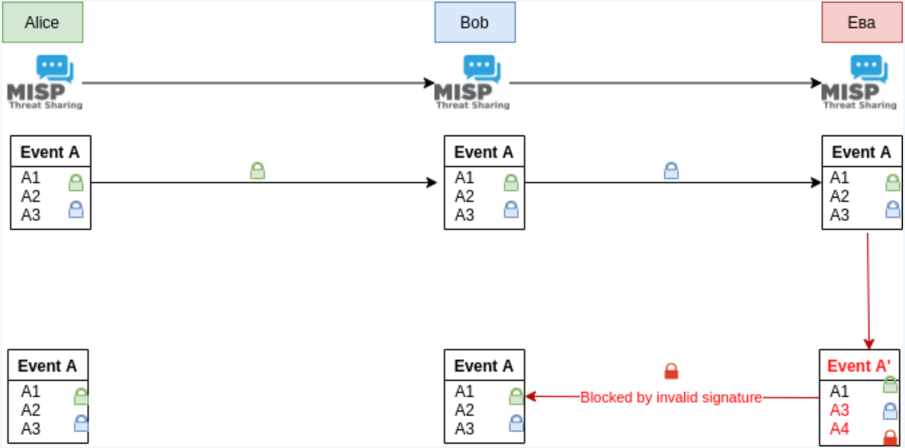
Cryptographic signing and tamper protection

- Need to be able to share and ensure the **veracity of critical events**
- Tampering by **malicious intermediaries**, even in closed networks became a new fear
- We came up with a solution that allows us to **lock down critical events**
- Limits the distribution, but **increases the resilience** of MISP immensely

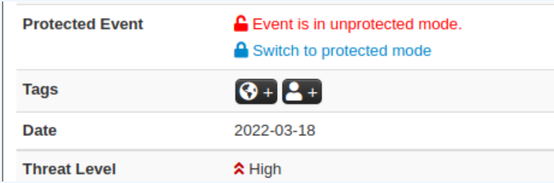
Cryptographic signing and tamper protection



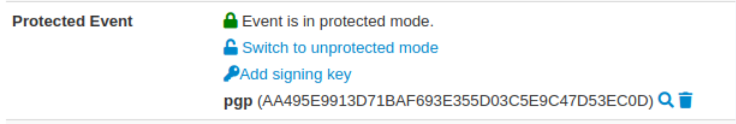
Cryptographic signing and tamper protection



Cryptographic signing and tamper protection



Protected Event	Event is in unprotected mode. Switch to protected mode
Tags	+ +
Date	2022-03-18
Threat Level	High



Protected Event	Event is in protected mode. Switch to unprotected mode Add signing key **pgp** (AA495E9913D71BAF693E355D03C5E9C47D53EC0D)

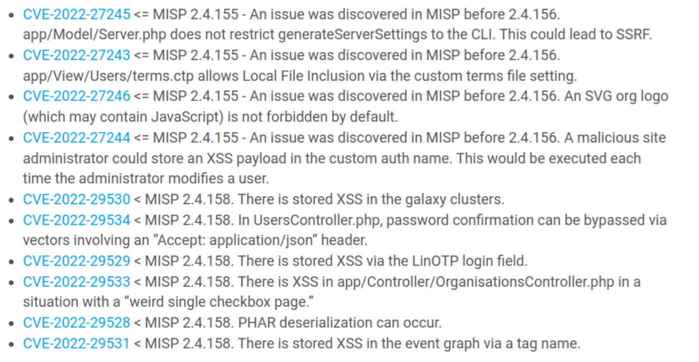
Other major improvements

- Various other new functionalities that improve our day to day use of the tool

Long list of security fixes

- Partially from user reports
- Partially by an exhaustive pentest series
- Massive thank you to **Zigrin Security** for conducting the tests...
- ...and to the **Luxembourgish Army** for financing it
- Multiple **CVEs** resolved, including a **critical one that required a silent release**
- Make sure you stay up to date!

Long list of security fixes

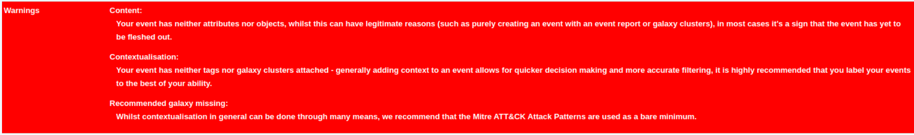


- CVE-2022-27245 <= MISP 2.4.155 - An issue was discovered in MISP before 2.4.156. app/Model/Server.php does not restrict generateServerSettings to the CLI. This could lead to SSRF.
- CVE-2022-27243 <= MISP 2.4.155 - An issue was discovered in MISP before 2.4.156. app/View/Users/terms.ctp allows Local File Inclusion via the custom terms file setting.
- CVE-2022-27246 <= MISP 2.4.155 - An issue was discovered in MISP before 2.4.156. An SVG org logo (which may contain JavaScript) is not forbidden by default.
- CVE-2022-27244 <= MISP 2.4.155 - An issue was discovered in MISP before 2.4.156. A malicious site administrator could store an XSS payload in the custom auth name. This would be executed each time the administrator modifies a user.
- CVE-2022-29530 < MISP 2.4.158. There is stored XSS in the galaxy clusters.
- CVE-2022-29534 < MISP 2.4.158. In UsersController.php, password confirmation can be bypassed via vectors involving an “Accept: application/json” header.
- CVE-2022-29529 < MISP 2.4.158. There is stored XSS via the LinOTP login field.
- CVE-2022-29533 < MISP 2.4.158. There is XSS in app/Controller/OrganisationsController.php in a situation with a “weird single checkbox page.”
- CVE-2022-29528 < MISP 2.4.158. PHAR deserialization can occur.
- CVE-2022-29531 < MISP 2.4.158. There is stored XSS in the event graph via a tag name.

Event warning system

- Build a rule based tool that analyses an event and **recommends improvements**
- Typical issues easily caught (missing TLP, lack of context, etc)
- Simple to extend, flexible

Event warning system



Warnings

Content:

Your event has neither attributes nor objects, whilst this can have legitimate reasons (such as purely creating an event with an event report or galaxy clusters), in most cases it's a sign that the event has yet to be fleshed out.

Contextualisation:

Your event has neither tags nor galaxy clusters attached - generally adding context to an event allows for quicker decision making and more accurate filtering, it is highly recommended that you label your events to the best of your ability.

Recommended galaxy missing:

Whilst contextualisation in general can be done through many means, we recommend that the Mitre ATT&CK Attack Patterns are used as a bare minimum.

Massive rework of the STIX integrations

- Our resident STIX guru (Christian Studer) has become **co-chair of the STIX commitee** at OASIS
- Massive rework of how we handle **STIX ingestion / generation**
- Continuous work with **MITRE/CISA** to improve the integration
- STIX subsystem spun off as a standalone system **misp-stix**[4]
- Can be used a standalone to convert in both directions MISP standard format to all the STIX variantes

[4] https://github.com/MISP/misp-stix

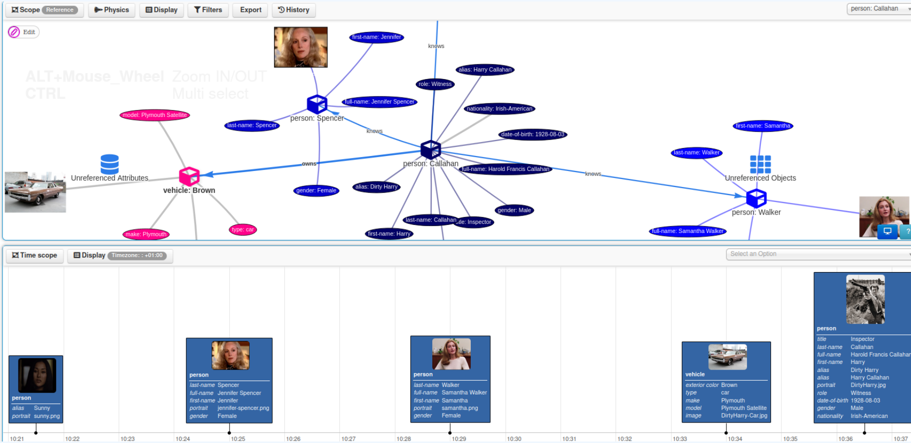
Further synchronisation filtering methods

- The ability to **exclude** certain attribute **types from the synchronisation**
- Comes with some risks, but solves some issues
- An example: **Exclusion of malware samples when sharing towards classified networks**

Advanced timelining

- Rework of the timelining in MISP
- Inclusion of images, sightings
- Various other improvements

TIMELINING



person

alias	Sunny
portrait	sunny.png

person

last-name	Spencer
full-name	Jennifer Spencer
first-name	Jennifer
portrait	jennifer-spencer.png
gender	Female

person

last-name	Walker
full-name	Samantha Walker
first-name	Samantha
portrait	samantha.png
gender	Female

vehicle

exterior color	Brown
type	car
make	Plymouth
model	Plymouth Satellite
image	DirtyHarry-Car.jpg

person

title	Inspector
last-name	Callahan
full-name	Harold Francis Callahar
first-name	Harry
alias	Dirty Harry
alias	Harry Callahan
portrait	DirtyHarry.jpg
role	Witness
date-of-birth	1928-08-03
gender	Male
nationality	Irish-American

New background processor

- Since late November last year we have had a **new background processing engine**
- Fully optional for now
- Lean, closer to an OS native implementation via **Supervisor**
- Gets rid of a lot of the baggage of our previous system (scheduling)
- Implemetation by @righel (Luciano Righetti)

Long list of other fixes

- Usability fixes
- Performance improvements
- Bug fixes
- Too many improvements to the galaxies, taxonomies, object templates to list!
- Huge thank you to **Jakub Onderka** for the **constant stream of improvements**

Workflows in MISP

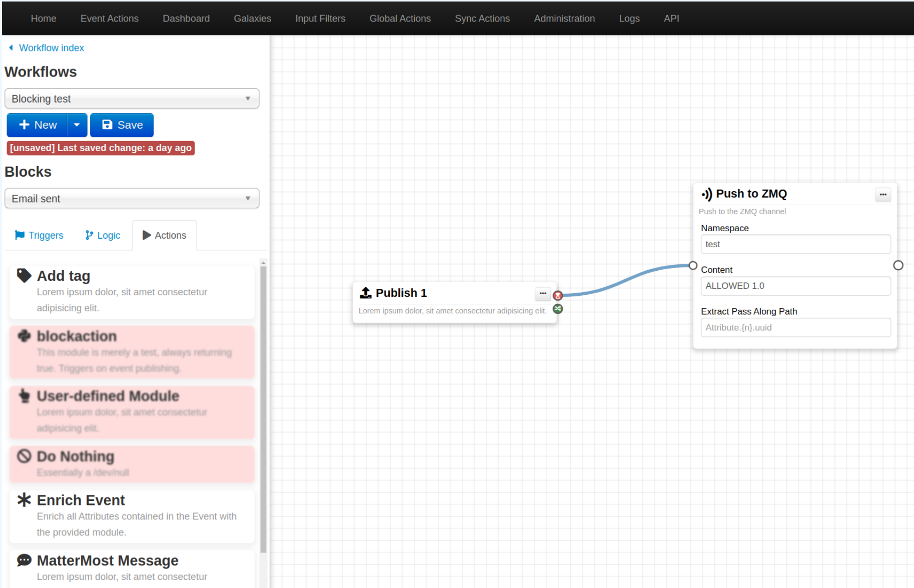
- Outcome of our initial work from GeekWeek 7.5[5]
- Goal: Modifying the execution of certain **core functionalities**
- Basically a **hooking mechanism**
- Modular approach using **MISP-modules** or **PHP modules**
- Build and execute admin defined tasks on various actions
- Modify data in place, block, fire-and-forget
- All exposed via a **completely new GUI**

[5] Workshop organized by the Canadian Cyber Center

Workflows in MISP

- **Branching** codebase
- Context sensitive, per-module filters
- Implemented by our UI expert Sami "GraphMan" Mokaddem

Workflows in MISP



Workflows

Blocking test

[unsaved] Last saved change: a day ago

Blocks

Email sent

Add tag
Lorem ipsum dolor, sit amet consectetur adipisicing elit.

blockaction
This module is merely a test, always returning true. Triggers on event publishing.

User-defined Module
Lorem ipsum dolor, sit amet consectetur adipisicing elit.

Do Nothing
Essentially a /dev/null

Enrich Event
Enrich all Attributes contained in the Event with the provided module.

MatterMost Message
Lorem ipsum dolor, sit amet consectetur

Publish 1
Lorem ipsum dolor, sit amet consectetur adipisicing elit.

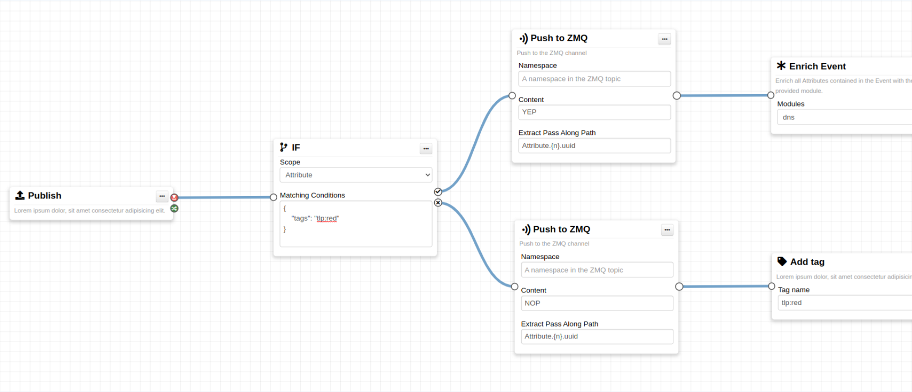
Push to ZMQ
Push to the ZMQ channel

Namespace: test

Content: ALLOWED 1.0

Extract Pass Along Path: Attribute.{n}.uuid

Workflows in MISP



Publish

Lorem ipsum dolor, sit amet consectetur adipisicing elit.

IF

Scope

Attribute

Matching Conditions

```
{
    "tags": "tlp:red"
}
```

Push to ZMQ

Push to the ZMQ channel

Namespace

A namespace in the ZMQ topic

Content

YEP

Extract Pass Along Path

Attribute.{n}.uuid

Enrich Event

Enrich all Attributes contained in the Event with the provided module.

Modules

dns

Push to ZMQ

Push to the ZMQ channel

Namespace

A namespace in the ZMQ topic

Content

NOP

Extract Pass Along Path

Attribute.{n}.uuid

Add tag

Lorem ipsum dolor, sit amet consectetur adipisicin

Tag name

tlp:red

External data guard

- Work in **collaboration with BICES**
- Proxy server[6] that **inspects and blocks potential data leaks** during synchronisation
- Standalone
- Simplistic design and **easy to audit**
- Modular **rule based** system

[6] https://github.com/MISP/misp-guard

Various reworks to support STIX mappings

- **Relationships for tags/galaxies**
- **Templating** for galaxy cluster creation
- Dot notation **deep cluster elements**
- Built in **TAXII 2.1 export support** with the help of MITRE/CISA

Quick Cerebrate update

Quick Cerebrate update

- 5 new releases
- Deployment for the **CSIRT network** ongoing
- A host of new functionalities to solve day to day issues we have in the CSIRT community

User management

- Reworked completely
- Tight integration with **KeyCloak**
- Full user provisioning / maintaining via Cerebrate

Reworked meta information system

- Introduction of **context specific custom fields**
- Custom **search algorithms** (for example CIDR block lookups for constituency information)
- Customisable and **blueprint-able data model**

API along with its documentation fleshed out

- **OpenAPI integration** similarly to MISP
- Integration tests and introduction of a **CI pipeline**
- Documentation and API examples available in Cerebrate directly

Security fixes

- Cerebrate, similarly to MISP received an in-depth pentest by **Zigrin Security**
- Likewise funded by the **Luxembourgish Army**
- Besides fixes to vulnerabilities, a host of usability findings and fixes
- **5 CVEs** published
- `https://www.cerebrate-project.org/security.html`

Get in touch if you have any questions

- Contact CIRCL
  - info@circl.lu
  - `https://twitter.com/circl_lu`
  - `https://www.circl.lu/`
- Contact MISPProject
  - `https://github.com/MISP`
  - `https://gitter.im/MISP/MISP`
  - `https://twitter.com/MISPProject`
- Cerebrate project
  - `https://github.com/cerebrate-project`
  - `https://github.com/cerebrate-project/cerebrate`