

# MISP PROJECT UPDATE

THE PAST 6 MONTHS

CIRCL / TEAM MISP PROJECT



EUROCONTROL 2022



# THE AIM OF THIS PRESENTATION

- A small update on the state of MISP's ongoing development
- Some highlights of the changes that were introduced
- Upcoming changes
- Cerebrate update
- Workflows

# MISP'S EVOLUTION SINCE PAST 6 MONTHS

- 9 releases
- 1775 commits
- 74 contributors contributing to the core software and its components

- 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**

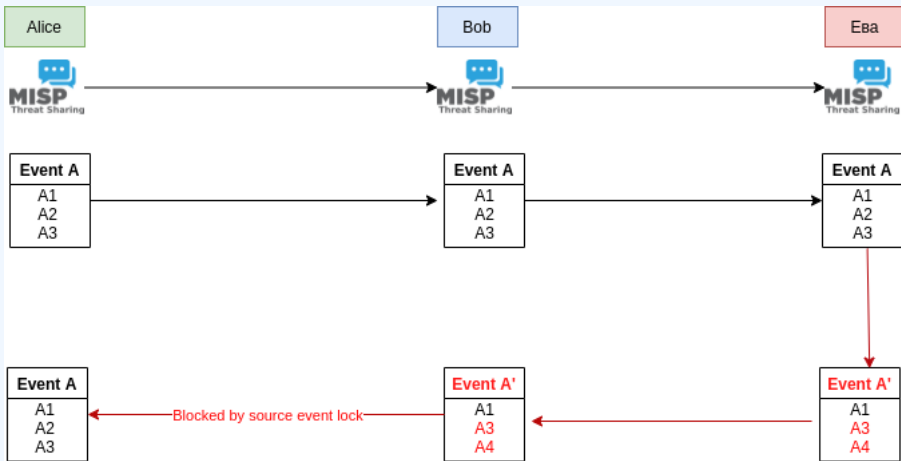
- Solving the issue of **sharing group lifecycle management**
- Build SG blueprints for reusable, maintainable sharing groups
- Abstract sharing groups, organisation metadata as building blocks
- Solve newly arising sharing challenges

# 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"  
      ]  
    }  
  }  
}
```

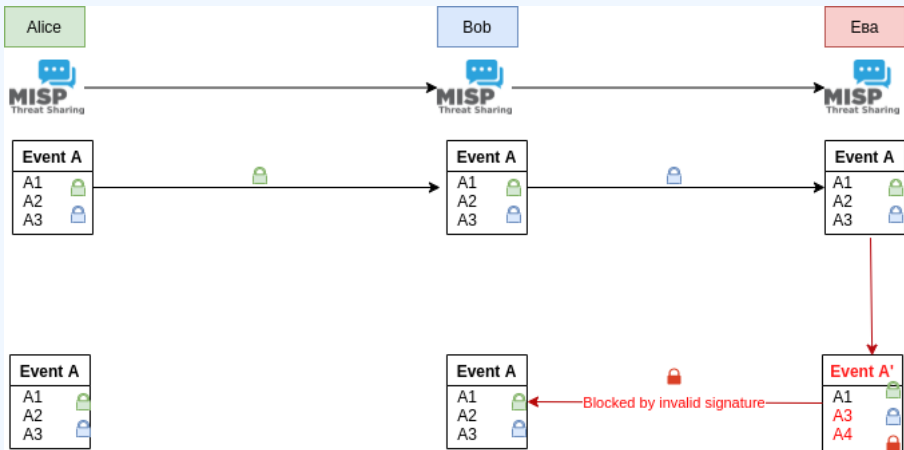
- Need to be able to share and ensure the **veracity of critical events**
- Tampering by **malicious intermediaries**, even in closed networks became a new fear
- We came up with a solution that allows us to **lock down critical events**
- Limits the distribution, but **increases the resilience** of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

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

- 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.

- 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

Warnings	<p><b>Content:</b> 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.</p> <p><b>Contextualisation:</b> 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.</p> <p><b>Recommended galaxy missing:</b> Whilst contextualisation in general can be done through many means, we recommend that the Mitre ATT&amp;CK Attack Patterns are used as a bare minimum.</p>
----------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

# MASSIVE REWORK OF THE STIX INTEGRATIONS

- Our resident STIX guru (Christian Studer) has become **co-chair of the STIX committee** 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**<sup>1</sup>
- Can be used a standalone to convert in both directions MISP standard format to all the STIX variantes

---

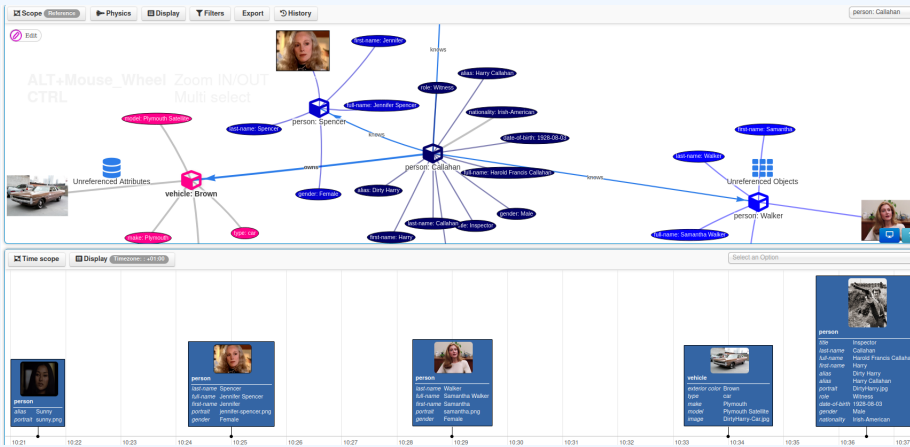
<sup>1</sup><https://github.com/MISP/misp-stix>



- 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**

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

# TIMELINING



- 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)
- Implementation by @righel (Luciano Righetti)

- 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**

- Outcome of our initial work from GeekWeek 7.5<sup>2</sup>
- 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**

---

<sup>2</sup>Workshop organized by the Canadian Cyber Center

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

# WORKFLOWS IN MISP

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API

Workflow index

## Workflows

Blocking test

+ New Save

[unsaved] Last saved change: a day ago

## Blocks

Email sent

Triggers Logic Actions

- Add tag**  
Lorem ipsum dolor, sit amet consectetur adipiscing elit.
- blockaction**  
This module is merely a test, always returning true. Triggers on event publishing.
- User-defined Module**  
Lorem ipsum dolor, sit amet consectetur adipiscing elit.
- Do Nothing**  
Essentially a Jdevnull
- Enrich Event**  
Enrich all Attributes contained in the Event with the provided module.
- MatterMost Message**  
Lorem ipsum dolor, sit amet consectetur

```
graph LR; A[Publish 1] --> B[Push to ZMQ];
```

**Publish 1**  
Lorem ipsum dolor, sit amet consectetur adipiscing elit.

**Push to ZMQ**  
Push to the ZMQ channel

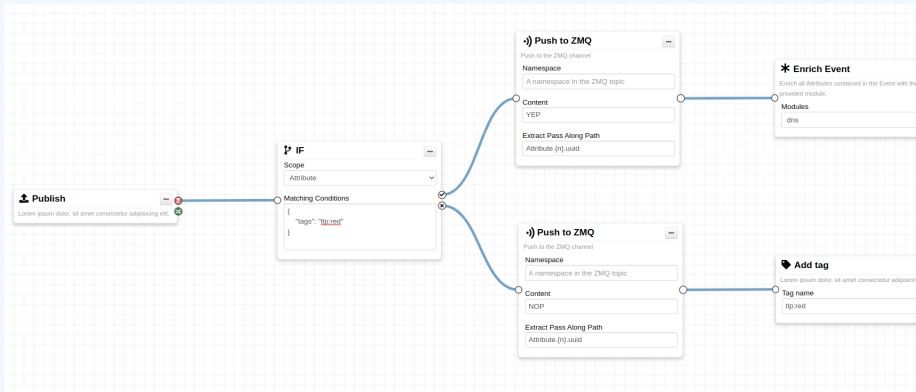
Namespace  
test

Content  
ALLOWED 1.0

Extract Pass Along Path  
Attribute.{n}.uuid



# WORKFLOWS IN MISP



- Work in **collaboration with BICES**
- Proxy server<sup>3</sup> that **inspects and blocks potential data leaks** during synchronisation
- Standalone
- Simplistic design and **easy to audit**
- Modular **rule based** system

---

<sup>3</sup><https://github.com/MISP/misp-guard>

- **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

The logo for the Cerebrate Project features the words "CEREBRATE" and "PROJECT" in white, uppercase, sans-serif font, stacked vertically. The text is centered on a dark purple, tilted rectangular background. This background is layered over a larger, lighter purple, tilted rectangular background. At the bottom of the composition, there is a faint, stylized graphic of a brain with several curved lines extending from it, suggesting neural activity or connectivity.

CEREBRATE  
PROJECT

- 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

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

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

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



- 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>

## ■ Contact CIRCL

- ▶ [info@circl.lu](mailto:info@circl.lu)
- ▶ [https://twitter.com/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>