

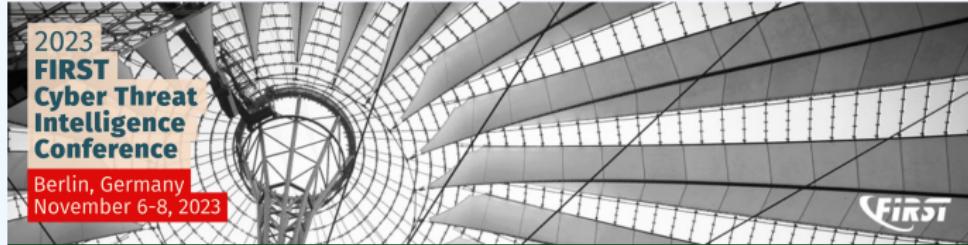
MISP 3 - Teaching an Old Dog New Tricks

Paving the way forward

Andras Iklody & Sami Mokaddem

MISP Project

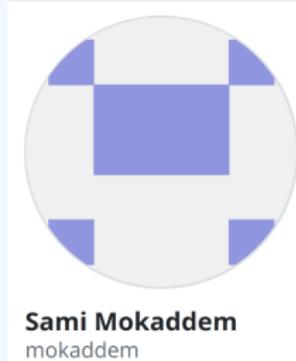
<https://www.misp-project.org/>





Andras Iklody
iglocska

 @iglocska



 @mokaddem_sami



AGENDA



- Why MISP 3?
- The plan
- Considerations

WHY MISP 3?

> AN OUTDATED VERSION OF THE FRAMEWORK



- MISP is based on CakePHP 2.x
 - ▶ End of Security Support in **June 2021**
 - ▶ Maintained fork [github.com:MISP/cakephp.git](https://github.com/MISP/cakephp.git)
- CakePHP supports PHP version **<=7.4**
 - ▶ End of Security Support in **November 2022**



> TACKED ON MECHANICS

- MISP supports a wide range of use cases...
- ... meaning loads of feature-clutter the interface
- All options visible regardless of the user profile
- Lack of coherent page navigation



The screenshot shows the MISP web application interface. At the top, there is a horizontal navigation bar with links: Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions (which is currently selected and highlighted in black), Sync Actions, Administration, Logs, and API. Below the navigation bar, on the left, is a sidebar containing a list of various system and event-related categories. The main content area displays a table titled "Events" with several rows of data. A vertical ellipsis icon is located at the bottom right of the table. On the far left, there is a vertical sidebar with additional navigation links.

> SHORTCOMINGS DUE TO INITIAL DESIGN CHOICES

To list a few..

- Sub-optimal database structure
- Start with something small, build it out has its disadvantages
 - ▶ Attribute type, value not a first-class citizen
 - ▶ Logs all in one place
 - ▶ Indexing rework (performance and moving validation to the DB)
- Confusing mess of multiple graphing interfaces
- Files - Especially tricky with dockerised and load balanced setups
- Tagging



> THE ONGOING PLAN FORWARD

- Port of the codebase to a new stack
 - ▶ CakePHP 2.x → CakePHP 5
- Rework of old baggage
 - ▶ Database updates
 - ▶ Front-end libraries (Bootstrap, Graphing, ...)
 - ▶ Background jobs & Scheduled tasks
 - ▶ Purging old libraries

> PRUNING UNUSED / DEAD END FUNCTIONALITIES

- Populate using the templating system
- Deprecated export functionalities
- Discussion / Posts
- ...



STEP I - PREPARING THE GROUNDS

STEP I - PREPARING THE GROUNDS

Refactoring the codebase for improved portability using factories

- Framework-agnostic
- Reusable code for front and back-end
- Extracting and encapsulating specialised functionalities into libraries

STEP I - PREPARING THE GROUNDS

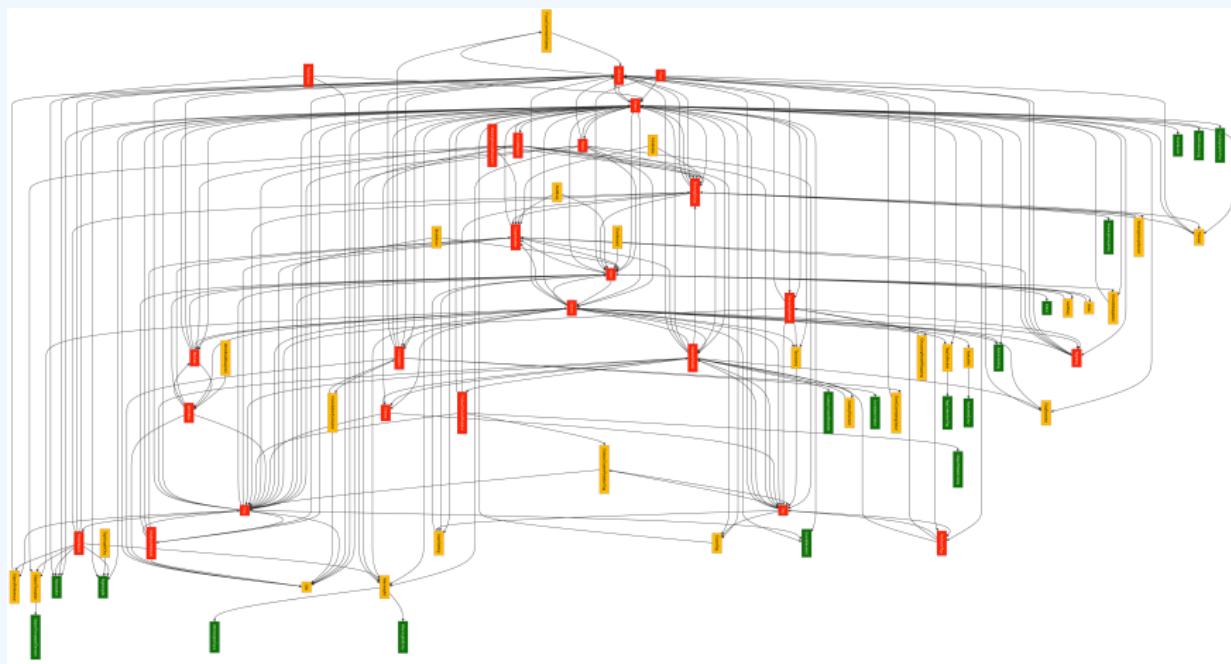


Setting the stage with Cerebrate

- Dev started in May 2020, built on MISP3's stack
- Application built on top of ported MISP libraries
- New UI laying the foundation for MISP 3
- Streamlined integration of new features into MISP3
 - ▶ Tagging, Inbox system, Settings, ...

STEP I - IDENTIFYING INTER-DEPENDENCIES

Migrate least connected part first



STEP II - PORTING THE CODEBASE

> STEP II - ROADMAP FOR A 3-WAVE PORTING

⌚ MISP 3.x

Task list Progress board Timeline + New View

Filter by keyword or by field

⌚ Todo 9
This item hasn't been started

- MISP #8881 TagCollectionTag
- MISP #8885 Inbox
- MISP #8886 ObjectRelationship
- MISP #8887 NotificationLog
- MISP #8890 GalaxyClusterBlocklist
- MISP #8891 EventLock
- MISP #8892 EventBlocklist

⌚ In Progress 1
This is actively being worked on

- MISP #8882 Sightingdb

⌚ Done 8
This has been completed

- MISP #8879 AdminSettings
- MISP #8880 WarninglistEntry
- MISP #8883 SharingGroups
- MISP #8884 ObjectTemplates
- MISP #8888 Noticelists
- MISP #8889 AllowedList
- MISP #8893 CryptographicKey
- MISP #9209 Authkeys

> STEP II - ROADMAP FOR A 3-WAVE PORTING

Wave 1 Least complex/inter-connected models

- ▶ E.g. Blocklist, Warninglist, Object-template, User

Wave 2 More glue relying on component already migrated

- ▶ E.g. Authkey, *-Tag, Taxonomy

Wave 3 The actual meat of the application

- ▶ E.g. Attribute, Event, Workflow

> STEP II - TEST DRIVEN DEVELOPMENT

```
$ composer test
> sh ./tests/Helper/wiremock/start.sh
WireMock 1 started on port 8080
> phpunit
[ * ] Running DB migrations, it may take some time ...

The WireMock server is started .....
port:                      8080
enable-browser-proxying:   false
disable-banner:            true
no-request-journal:       false
verbose:                  false

PHPUnit 8.5.22 by Sebastian Bergmann and contributors.
```



- Complementary to PyMISP test
- In-framework **Unit Tests** and **Endpoint Tests**
- Improved CI pipeline and enforced code standard

> CODEBASE MIGRATION: WHERE WE STAND I

Migration officially started in January 2023

The screenshot shows a GitHub commit history for a repository. At the top, there are summary statistics: 333 commits, 2,467 files changed, and 5 contributors. Below this, a specific commit is highlighted:

new: [3.x] initial skeleton added ...
iglokska committed on Jan 31

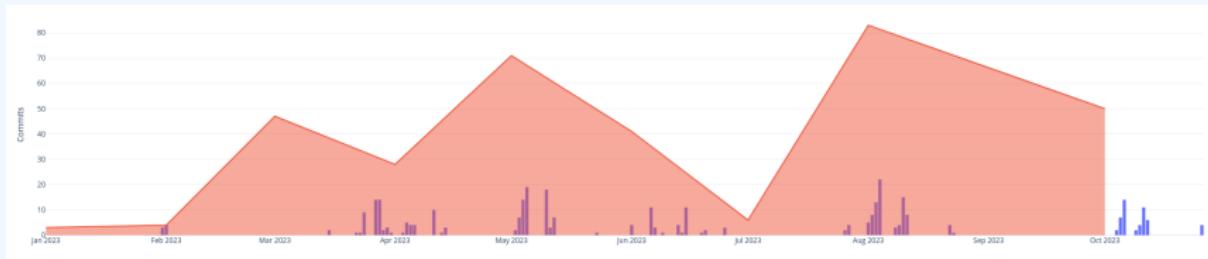
This commit is marked as **Verified**. To the right are buttons for copy, commit ID (35932db), and refresh. The commit message is "new: [3.x] initial skeleton added".

The main list of commits shows numerous entries, mostly from iglokska, all dated Jan 31, 2023. The commits are listed by file name, such as `AdminTable.php`, `CategoryTable.php`, etc., with brief descriptions like "new: [3.x] initial skeleton added" or "fix: parsing issue".

- Around **27 tables** have been moved
- Some partially, others completely

Name	Last commit message	Last commit date
<code>___.php</code>		7 months ago
<code>SettingModel.php</code>	fix: depreciation notices	7 months ago
<code>glossary</code>	new: [3.x] initial skeleton added	7 months ago
<code>AdministratorTable.php</code>	new: migration AdminTable to model instead	7 months ago
<code>AdministratorTable.php</code>	fix: rename table for consistency	6 months ago
<code>AppTable.php</code>	No merge conflicts	3 months ago
<code>AvatarLogTable.php</code>	new: [3.x] initial skeleton added	14 months ago
<code>AvatarTable.php</code>	add: app-end tests	4 months ago
<code>CryptographicKeyTable.php</code>	No use -remove(dlg)	3 months ago
<code>EventBuddyListTable.php</code>	No fix	3 months ago
<code>EventTable.php</code>	add basic crud app tests for sharing groups	5 months ago
<code>InteractionTable.php</code>	add basic user tests, remove contribute part, code from rec...	7 months ago
<code>JobTable.php</code>	drag: refrence to user migration	last month
<code>LogoTable.php</code>	add migrate command to test jobs	last month
<code>NewsletterTable.php</code>	add post notifications	3 months ago
<code>ModuleTable.php</code>	No fix	3 months ago
<code>ObjectTableAndSelectable.php</code>	No: properly handle requirements	3 months ago
<code>ObjectTemplateTableAndSelectable.php</code>	new: migrate object template	3 months ago
<code>ObjectTemplateTable.php</code>	fix: parsing poor values	3 months ago
<code>OrganizationTable.php</code>	add more tests, No bugs	5 months ago
<code>AvatarTable.php</code>	new: [3.x] initial skeleton added	14 months ago
<code>ServerTable.php</code>	drag: refrence to user migration	last month
<code>UserLogTable.php</code>	No merge conflicts	3 months ago
<code>UserLogTable.php</code>	No merge conflicts	3 months ago
<code>UserLogTable.php</code>	No merge conflicts	3 months ago
<code>SignatureTable.php</code>	No use -remove(dlg) instead of -constructor	8 months ago
<code>TagCollectionLogTable.php</code>	drag: parsecategory models added	8 months ago
<code>UserTable.php</code>	drag: parsecollection models added	8 months ago
<code>NewsEngagementTable.php</code>	add (empty) post of Sonnenfeld tool and related dataset adjustments	last month
<code>NewsEngagementTable.php</code>	new: [parseEngagement] migration - first revision, Fixes #1000	8 months ago

> CODEBASE MIGRATION: WHERE WE STAND II



- Migration speed ramping up. The more we port, the faster we go

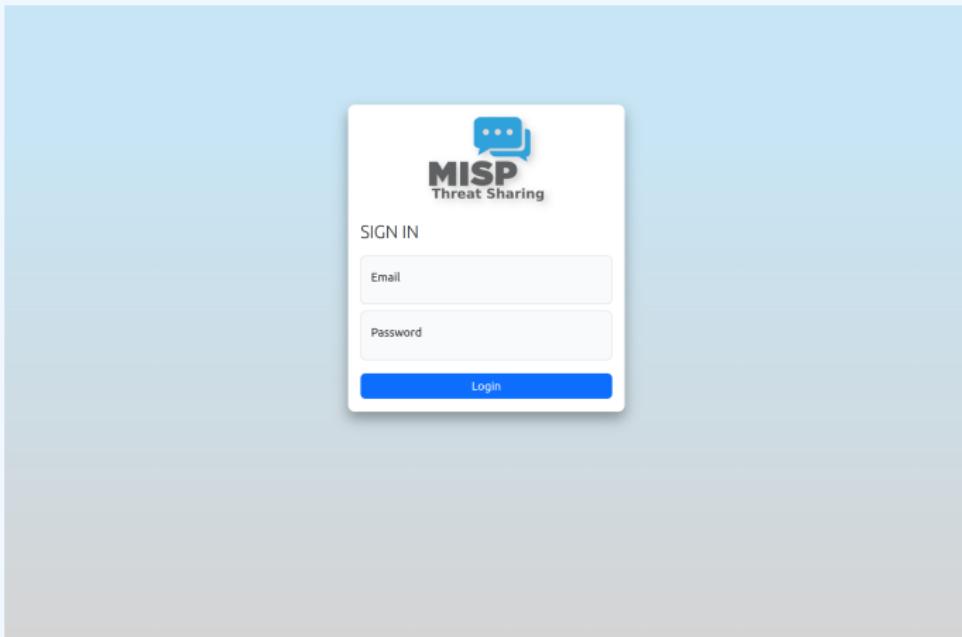
This branch is 333 commits ahead, 914 commits behind 2.4.

- Even while supporting and improving 2.4

LOOK AND FEEL

CODEBASE MIGRATION: LOOK AND FEEL I

- Most of the changes are **invisible**
- Some user interfaces can still be displayed



CODEBASE MIGRATION: LOOK AND FEEL II

MISP

Organisations index

Contact Organisation

Organisation Index¹

Nationalities:

Sectors: No data

Previous Next

+ Add organisation All Local orgs External orgs Country: Luxembourg

#	Name	UUID	Members	URL	Nationality	Sector	Type	Actions
1	ORGNAME	7e9251cb-3b15-417a-9e92-e508479c5b4d	2		Luxembourg		ADMIN	
2	CERT-FR_1510	56bdff779-46f9-4353-bd99-2bb95bce2212	0		France			

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

Previous Next

17

CODEBASE MIGRATION: LOOK AND FEEL II

CODEBASE MIGRATION: LOOK AND FEEL II

The screenshot shows the MISP user profile for the user 'admin@admin.test'. The page has a dark header with the MISP logo and navigation links for 'View', 'Edit', 'Account settings', and 'User Setting'. A search bar is also present. The main content area displays the user's details in a table format:

ID	1
Email	admin@admin.test
Organisation	GRCNAME
Role	admin
Email notifications	Event published notification: Yes Daily notifications: No Weekly notifications: No Monthly notifications: No
Contact alert enabled	No
NIDS Start SID	4000000
Terms accepted	No
Must change password	No
PGP key	N/A
S/MIME Public certificate	
Disabled	No

Below the table, there are two sections with blue hyperlinks: 'Authentication keys' and 'Events'.

CODEBASE MIGRATION: LOOK AND FEEL II

The screenshot shows the MISP Sharing Groups Index page. The top navigation bar includes the MISP logo, a search bar, and user icons for View and Edit. The main content area is titled "New Sharing Group". It features three tabs: General (selected), Organisations, and Instances. The General tab contains fields for Local Organisations (dropdown placeholder: "Select a local organisation") and Remote Organisations (dropdown placeholder: "Select a remote organisation"). Below these is a table listing organisations:

Type	Name	UUID	Extend	Actions
local	ORIONAME	7e9251c8-3b15-417a-9e92-a508479c5b4d	<input checked="" type="checkbox"/>	
remote	CERT-FR_1510	56bdff779-4ef8-4353-bdf9-2bb95bce2212	<input type="checkbox"/>	

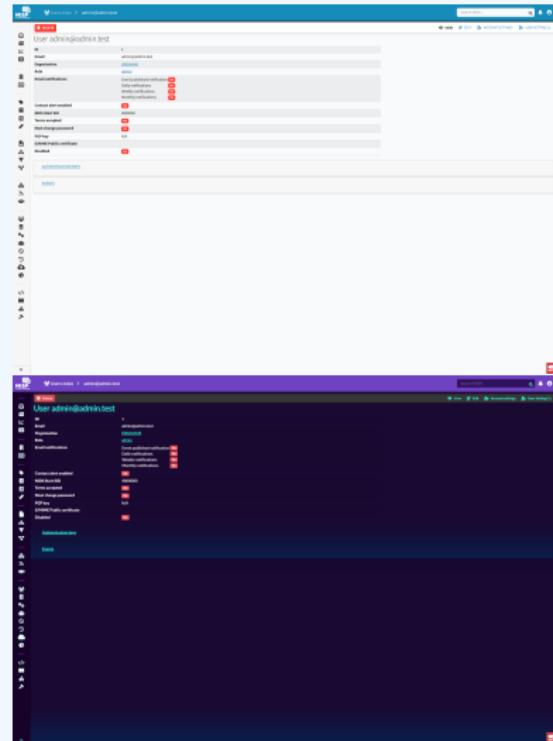
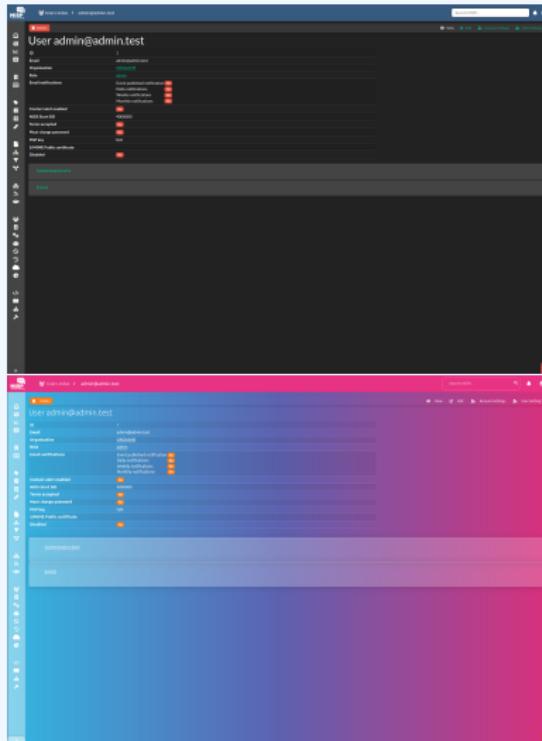
A "Next page" button is located at the bottom left of the table.

CODEBASE MIGRATION: LOOK AND FEEL II

- Updating Bootstrap greatly improves aesthetics
- And allow us to integrate themes seamlessly



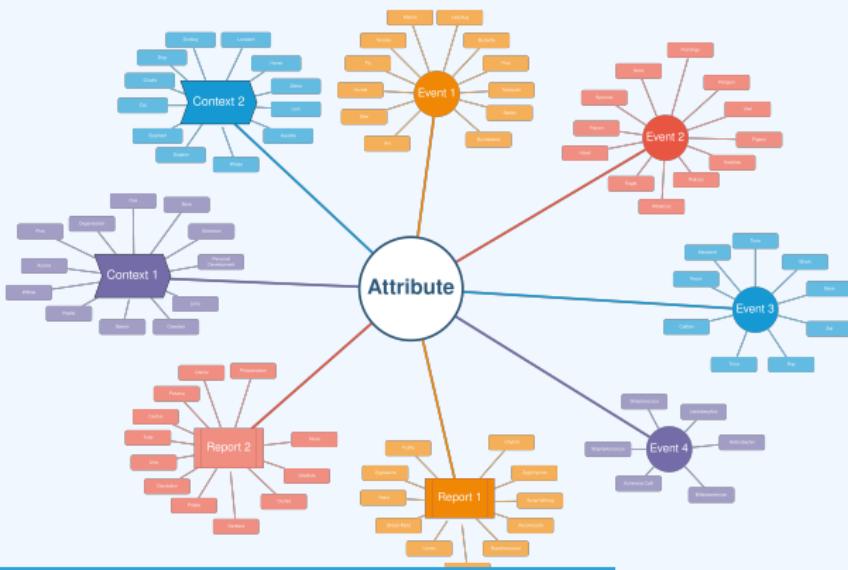
CODEBASE MIGRATION: LOOK AND FEEL II



STEP III - THE TODOS

> REDEFINE HOW WE INTERACT WITH DATA I

- Indicator centric perspective
 - ▶ Alternative to the Event centric view
 - ▶ Unified view of everything we know about a given Indicator
 - ▶ Allows us to take better decisions
 - ▶ Enable users to manage their IoC working set
 - ▶ Start an investigation more easily from a single indicator



> REDEFINE HOW WE INTERACT WITH DATA II

■ Unified search mechanics

- ▶ Code deduplication
 - ▶ Streamlined way to search for data
 - ▶ Opening up the full power of the API searches to UI users
 - ▶ Translation layer for the deprecated endpoints

REDEFINE HOW WE INTERACT WITH DATA III

- Refactor the Event view
 - ▶ Key Elements at first glance
 - ▶ Emphasis on the context (Insights, Taxonomies, Galaxies, Correlation, .)
 - ▶ Massive performance gains by moving to the composition of separate atomic endpoints
 - ▶ Unified graph interface
 - ▶ Sneak peak ? 😊

SNEAK PEAK OF THE NEW EVENT VIEW - WIP

Events index > [id] Search MISP... X

Add Objects + Publish + Event Actions + Import/Export + View Edit View History Explore

Spear-phishing attempt targeting telco sector

critical notice like delegation requests, tag conflicts, ...

Event ID	46	Threat Level	2
UUID	c5168000-740b-4e2b-8b85-2f4562b116fe	Analysis	1
Creator org	ORGNAME	Tags	spam phishing phishing techniques "email-spoofing" phishing distribution "spear-phishing" phishing state "active" phishing psychological acceptability "medium" exploit-language/that/lead/probability="very-likely"
Owner org	ORGNAME	Galaxies	misp-galaxy-target-information "Leverage" misp-galaxy-country "Leverage" misp-galaxy-mitre-attack-pattern "Spear-phishing messages with malicious attachments - T1337" misp-galaxy-mitre-attack-pattern "Spearphishing Attachment - T1386.001" misp-galaxy-mitre-attack-pattern "Phishing - T1360"
Contributors		Extends	
Creator user	admin@admin.test	Extended by	46
Protected Event		Related Events	5 related hits
Date	2023-02-07	Feed Hits	3 feed hits
Distribution	1	Server Hits	0 server hits
Published	No	Warninglist Hits	2 warninglist hits

Event activity

0 PROPOSALS 2 SIGHTINGS
0 EXTENSIONS 0 DELETED
1 FEED HITS 1 WARNINGLIST HITS
6 RELATIONSHIPS 17 5% IOCS

Distribution Objects Attributes

Recent sightings

Relevant correlations go here

- Events with some context overlap
- Events created by other orgs
- ...

notice for empty event... X

Objects 13 Attributes 13 Reports 1 Event Graph Event Timeline ATTACK® Discussion 1

objects

CONSIDERATIONS

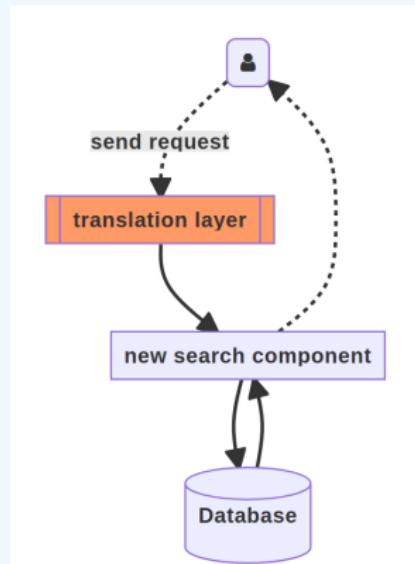
> MISP CORE FORMAT



- Created in **2012**, Officially became a standard in 2016
- **No breaking changes** since its birth, And we'll maintain this streak
- Format will keep evolving to support new functionalities

> API COMPATIBILITY

- The aim is to achieve a **near 100% compatibility** with the old API
- "Near" only due to the functionalities removed as a result of deprecation.
- Strategy: Mapping with a translation layer



> SYNCHRONISATION COMPATIBILITY

- API Compatibility means Synchronisation compatibility
- MISP 3 servers will be able to sync with MISP 2.4 and vice versa

BUT

- MISP **2.4 → 3**
 - ▶ Full support
- MISP **3 → 2.4**
 - ▶ Lossy when sharing new types of datapoints
 - ▶ E.g: Tags on Objects

> SUPPORT FOR MISP 2.4



- MISp 2.4 will be **supported for a limited time**
- **6 months** support post MISp 3 release
 - ▶ Potential changes/improvements on 2.4 to better support MISp 3 interactions

> MIGRATION SUPPORT FOR 2.4 → 3



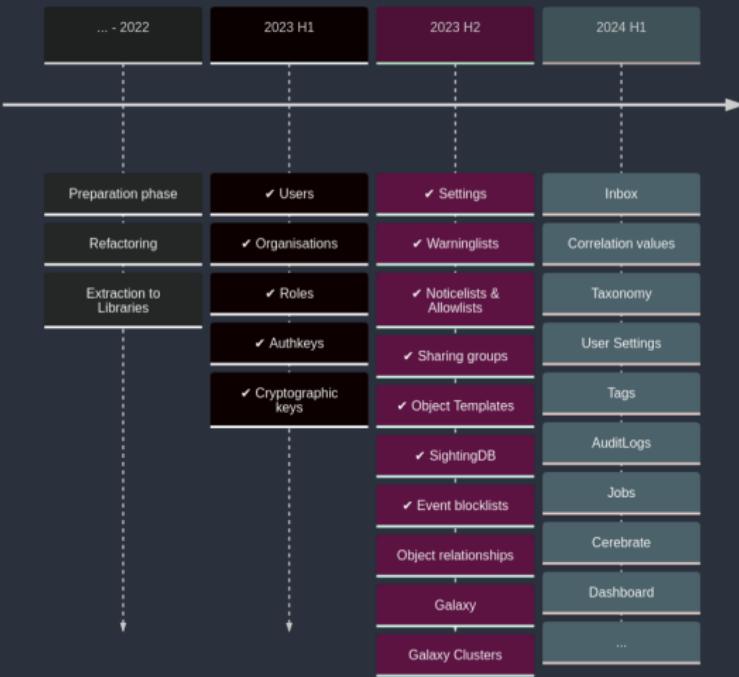
- No one-click update; manual script execution required
- Migration tools will be included in MISp 3 to help you
- This allows us to make underlying changes such as
 - ▶ Database changes
 - ▶ Libraries changes (e.g supervisor in favour of cake-resque)

> INSTALLATION FOR NEW INSTANCES

- Simplified installation based on package managers
- Upstream Docker installer
- OS targets: **Ubuntu** and **RHEL**



Model migration timeline



> KEY TAKE-AWAYS FROM THE UPCOMING VERSION

- Reworked UX
- Alternative, Analyst centric in addition to the data centric approach
- Improved search and trend monitoring tools
- Improved performance and resilience
- Want to get involved?
- Removal of the main painpoints of MISP 2.x's limitations across the board

> OUR HOPES AND EXPECTATIONS FOR THE FIRST COMMUNITY



- We will list features marked for culling
 - ▶ If you're using any of them, please let us know!
- We will be launching a beta phase in the future
 - ▶ Feedback & improvements are more than welcome!
- Want to get involved?
 - ▶ 3.x branch - MISP/MISP/tree/3.x
 - ▶ Project for migration - github.com/orgs/MISP/projects/2