

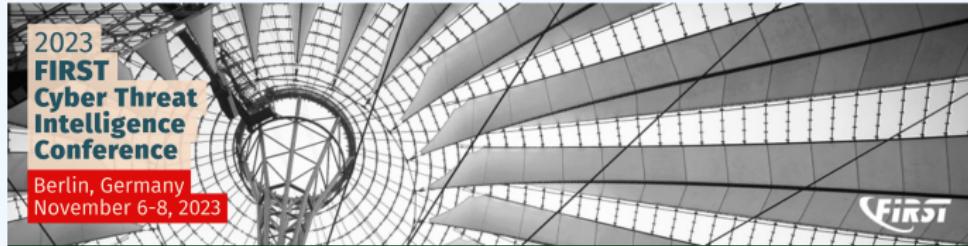
MISP 3 - Teaching an Old Dog New Tricks

Paving the way forward

Andras Iklody & Sami Mokaddem

MISP Project

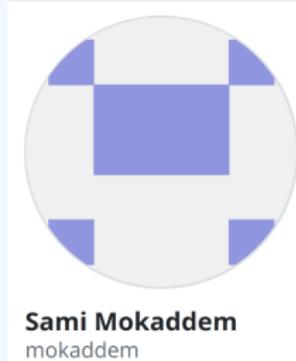
<https://www.misp-project.org/>





Andras Iklody
iglocska

 @iglocska



 @mokaddem_sami



AGENDA



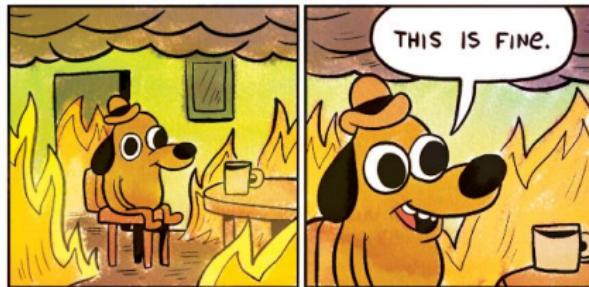
- Why MISP 3?
- The plan
- Considerations

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 AN OUTDATED VERSION OF THE FRAMEWORK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 modules and features. The main content area displays a table titled "Events" with several rows of event data. A vertical ellipsis icon is located at the bottom right of the table. On the far left, there is a vertical sidebar with more navigation options.

> 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

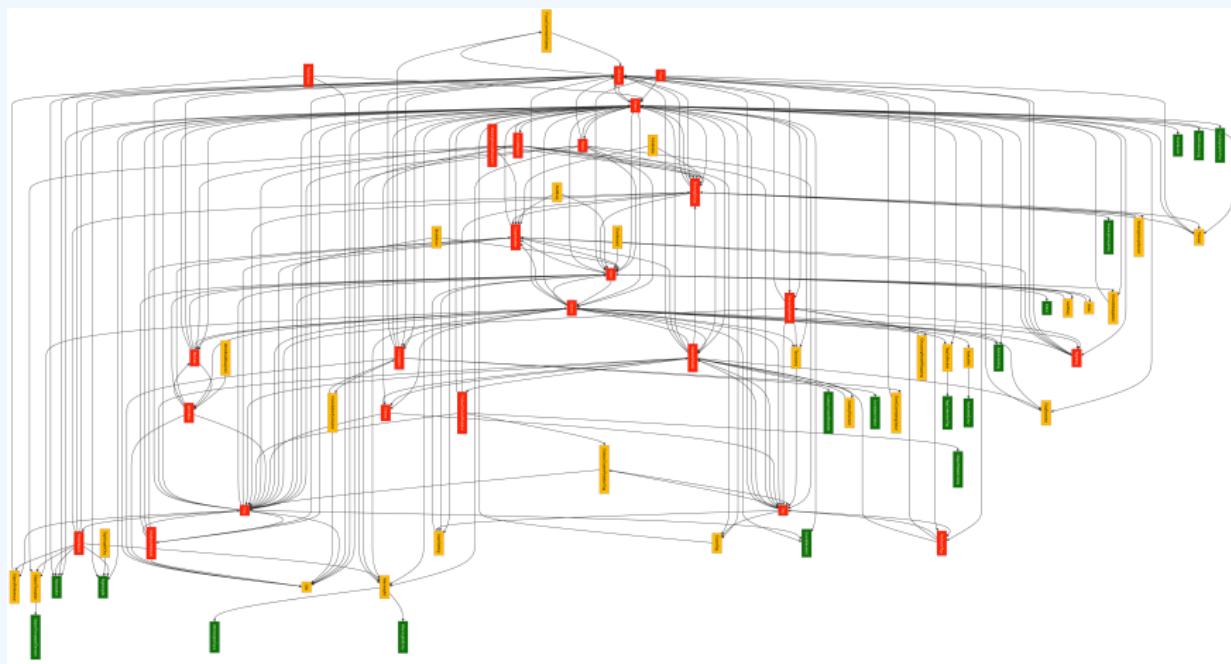


Setting the stage with Cerebrate

- 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

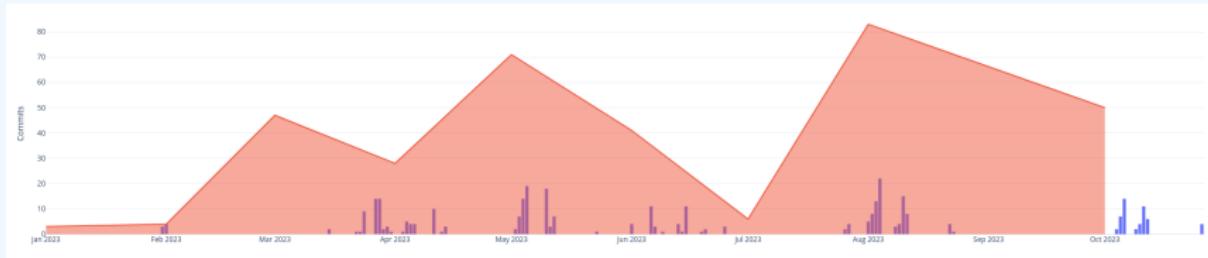
This commit is marked as **Verified**. To the right are buttons for copy, commit ID (35932db), and refresh. The commit message is "new: [3.x] initial skeleton added".

The main list of commits shows numerous entries, mostly from iglokska, dated from January 31 to February 1. The commits are mostly about moving tables and adding basic crud API tests. Some commits mention renaming tables or adding foreign key constraints.

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

Name	Last commit message	Last commit date
...		
billingHeaders	No depreciation notices	7 months ago
glueApp	new: [3.x] initial skeleton added	10 months ago
AdministratorTable.php	new: migration Administrator table created	10 months ago
AdministratorTable.php	(ch) rename table for consistency	8 months ago
AppTable.php	No merge conflicts	3 months ago
AvatarLogTable.php	new: [3.x] initial skeleton added	10 months ago
AvatarTable.php	add: app crud tests	4 months ago
CryptographicKeyTable.php	No use -remove(dlg)	5 months ago
EventBuddyListTable.php	No cs	3 months ago
EventTable.php	add basic crud API tests for sharing groups	5 months ago
EventTable.php	add add basic user tests, remove contribute part code from ...	7 months ago
JobTable.php	drop reference to user migration	last month
LogTable.php	add migrate command to test jobs	last month
InvestmentReviewTable.php	add post notifications	3 months ago
InvestTable.php	No cs	3 months ago
InvestTable.php	No properly validate requirements	3 months ago
ObjectTableAndScriptable.php	new: migrate object template	3 months ago
ObjectTableAndScriptable.php	No parsing poor values	3 months ago
OrganizationTable.php	add more tests, No bugs	5 months ago
AvatarTable.php	new: [3.x] initial skeleton added	10 months ago
ServerTable.php	drop reference to user migration	last month
UserLogTable.php	No merge conflicts	3 months ago
UserLogTable.php	No merge conflicts	3 months ago
UserLogTable.php	No use -remove(dlg) instead of -remove	3 weeks ago
SigninTable.php	drop: user migration models added	4 months ago
TagCollectorLogTable.php	drop: user migration models added	4 months ago
UserTable.php	add (empty) port of SonarCloud tool and related docker adjustments	last month
WarmingElementTable.php	new: [userlog entry] 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

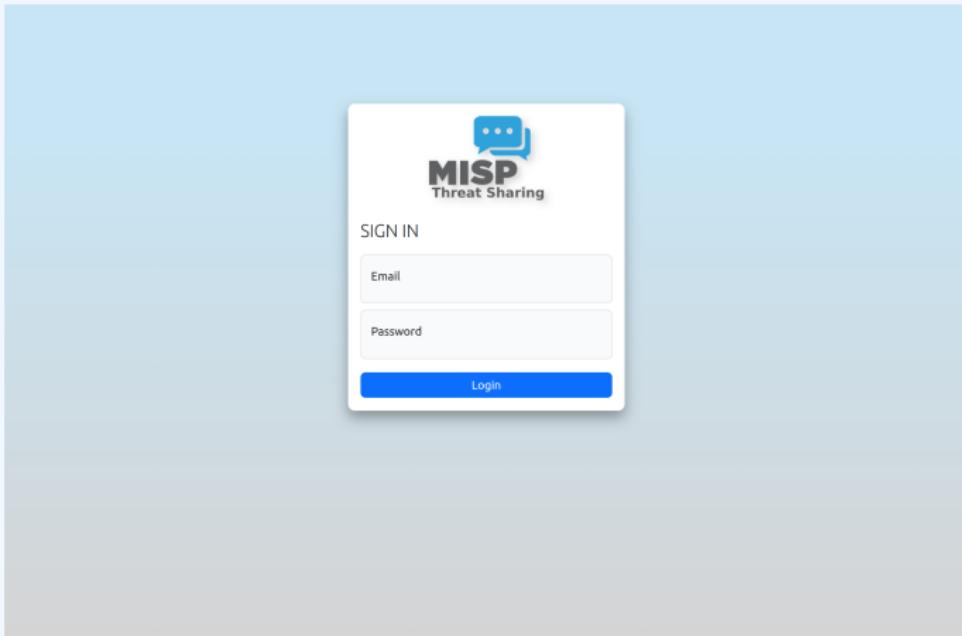
This branch is 333 commits ahead, 914 commits behind 2.4.

- 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

MISP

Organisations index > ORGNAME

Search MISP... View Edit

Delete

Organisation View

ID	1
Name	ORGNAME
UUID	7e9251cb-3b15-417a-9e92-a508479c5b4d
URL	
Nationality	Luxembourg
Sector	
Type	ADMIN
Contacts	

[Users](#)

User index ¹

Previous Next

<input type="button" value="+ add user"/>	All	Active	Disabled	<input type="button" value="Roles"/>	Enter value to search	Search	<input type="button" value="New"/>					
<input type="checkbox"/>	ID	Org	Role	Email					Last Login	Created	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> Actions	
<input type="checkbox"/>	1	ORGNAME	edMin	admin@admin.test					2023-03-08 07:15:14		<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	
<input type="checkbox"/>	2	ORGNAME	Sync user	sync@admin.test					3367851	0	2022-03-17 10:19:40	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>

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

Previous Next

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'. 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 SharingGroups index page. The URL is `SharingGroups index > Test edit SG`. The top navigation bar includes a search field "Search MISP..." and icons for View and Edit.

The main content area is titled "New Sharing Group". It has tabs: General (selected), Organisations, Instances, and Summary & Save.

Under "Local Organisations", there is a dropdown menu labeled "Select a local organisation".

Under "Remote Organisations", there is a dropdown menu labeled "Select a remote organisation".

A table lists organisations:

Type	Name
local	ORGNAME
	FR CERT-FR_IS10

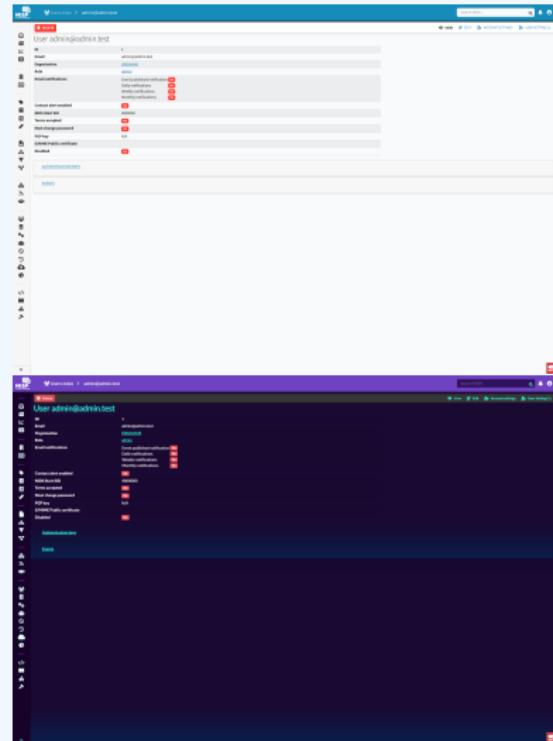
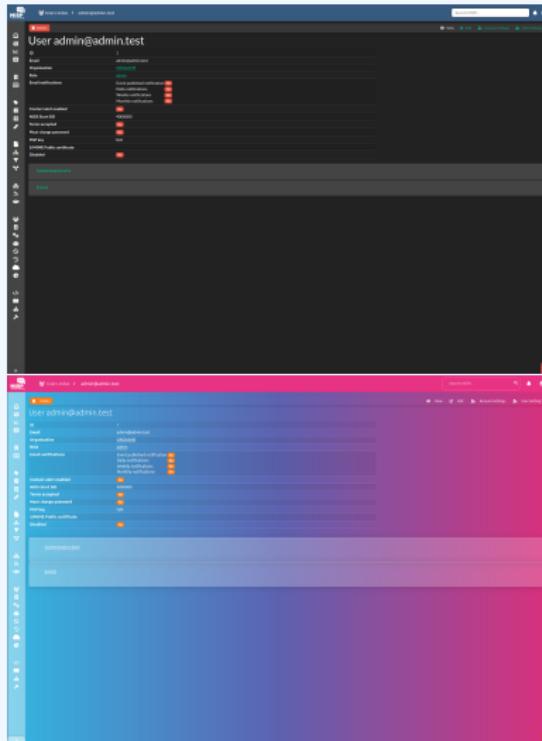
Below the table is a "Next page" button.

CODEBASE MIGRATION: LOOK AND FEEL II

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



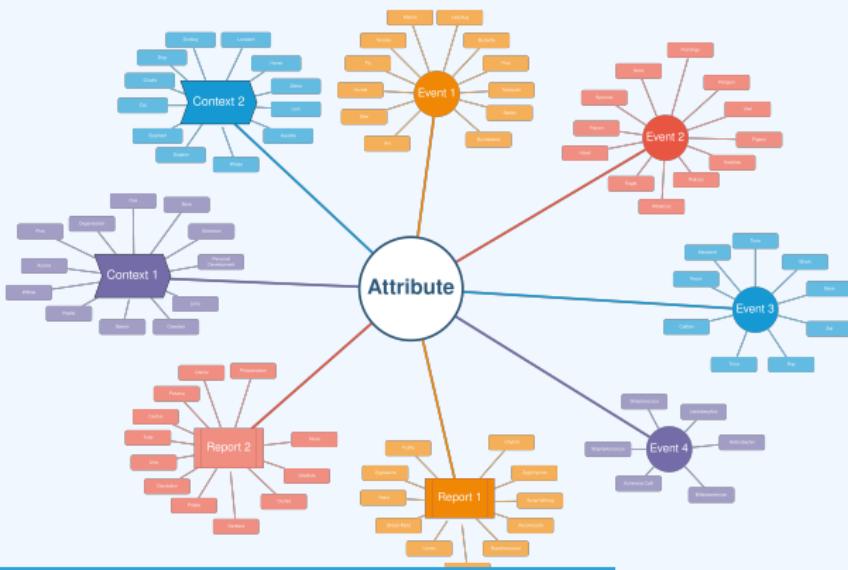
CODEBASE MIGRATION: LOOK AND FEEL II



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

The screenshot shows the Microsoft Defender XDR interface with the 'Export' tab selected. The page title is 'Export' and it includes a detailed description of what each export type does. Below this is a table with columns for Type, Description, Generated, Failed, Progress, and Actions.

Type	Description	Generated	Failed	Progress	Actions
JSON	Click this to download all events and attributes that you have access to in JSON (JSON format). Attachments are enabled on this instance.	Yes	No	N/A	Download Generate
XML	Click this to download all events and attributes that you have access to in XML (XML format). Attachments are enabled on this instance.	Yes	No	N/A	Download Generate
CSV_Img	Click this to download all attributes that are included and that you have access to (except for attachments) in CSV format.	Yes	No	N/A	Download Generate
CSV_Ad	Click this to download all attributes that are included and that you have access to (including attachments) in CSV format.	Yes	No	N/A	Download Generate
Sentra	Click this to download all attributes that you have access to (except for attachments) in SISG format. Only published events and attributes marked as SISG Signatures are exported. Administrations is used to determine which events and attributes are published.	Yes	No	N/A	Download Generate
Sent	Click this to download all network related attributes that you have access to under the Server role filter. Only published events and attributes marked as SISG Signatures are exported. Administrations is used to determine which events and attributes are published.	Yes	No	N/A	Download Generate
Src	Click this to download all network related attributes that you have access to under the Device role filter. Only published events and attributes marked as SISG Signatures are exported. Administrations is used to determine which events and attributes are published.	Yes	No	N/A	Download Generate
STIX	Click this to download a STIX document containing the STIX version of all events and attributes that you have access to. Attachments are enabled on this instance.	Yes	No	N/A	Download Generate
STIX2	Click this to download a STIX2 document containing the STIX version of all events and attributes that you have access to. Attachments are enabled on this instance.	Yes	No	N/A	Download Generate
NSF	Click this to download an NSF file generated from all of your logs. This can be used to feed forensic software when searching for suspicious files. Only published events and attributes marked as SISG Signatures are exported.	Yes	No	N/A	Download Generate
TEXT	Click one of the buttons below to download all the attributes with the matching type. This can be used to feed forensic software when searching for suspicious files. Only published events and attributes marked as SISG Signatures are exported. Attachments are enabled on this instance.	Yes	No	N/A	Generate
YAML	Click this to download Yaml files generated from all relevant attributes. Rules are returned in a JSON format with information about origin (generated or parsed) and validity.	Yes	No	N/A	Download Generate
XML	Click this to download XML files generated from all relevant attributes.	Yes	No	N/A	Download Generate

At the bottom of the page, there is a 'Download PDF guide' button and a footer note: 'Powered by Microsoft 365 E3 | 2023-01-03 13:05:14'.

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

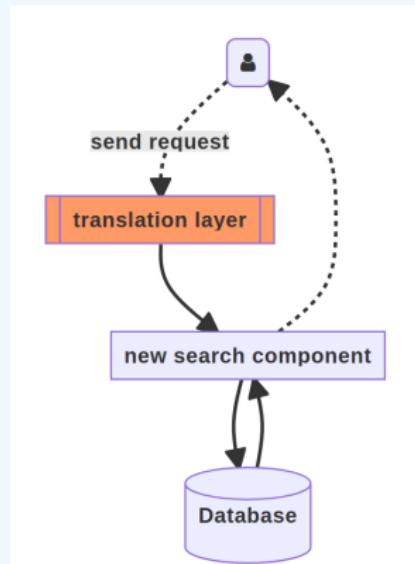
> MISP CORE FORMAT



- 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



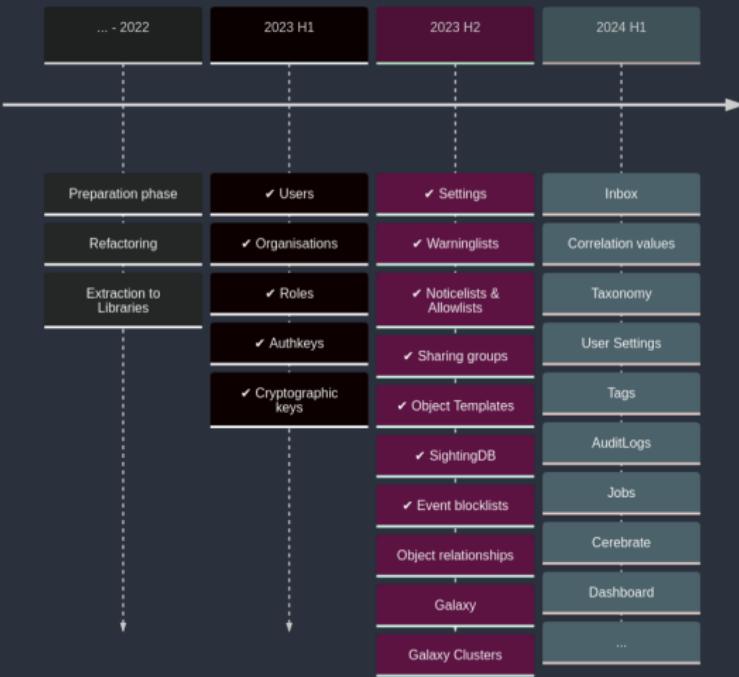
- No one-click update; manual script execution required
- Migration tools will be included in MISp 3 to help you
- This allows us to make underlying changes such as
 - ▶ Database changes
 - ▶ Libraries changes (e.g supervisor in favour of cake-resque)

> 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/UI
- 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