

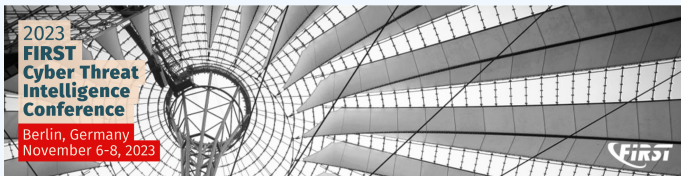
MISP 3 - Teaching an Old Dog New Tricks

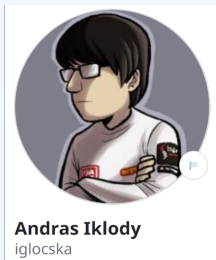
Paving the way forward

Andras Iklody & Sami Mokaddem

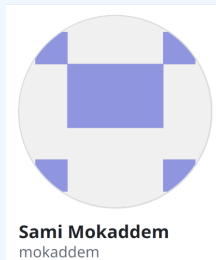
MISP Project

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





🐦 @iglocska



🐦 @mokaddem_sami





- Why MISP 3?
- The plan
- Considerations

WHY MISP 3?

> AN OUTDATED VERSION OF THE FRAMEWORK

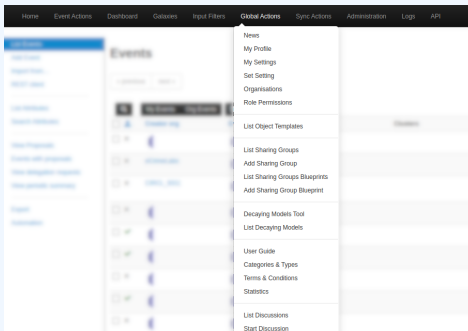


- MISP is based on CakePHP 2.x
 - ▶ End of Security Support in **June 2021**
 - ▶ Maintained fork github.com:MISP/cakephp.git
- CakePHP supports PHP version **<=7.4**
 - ▶ End of Security Support in **November 2022**



> 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



> 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



- 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

Refactoring the codebase for improved portability using factories

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

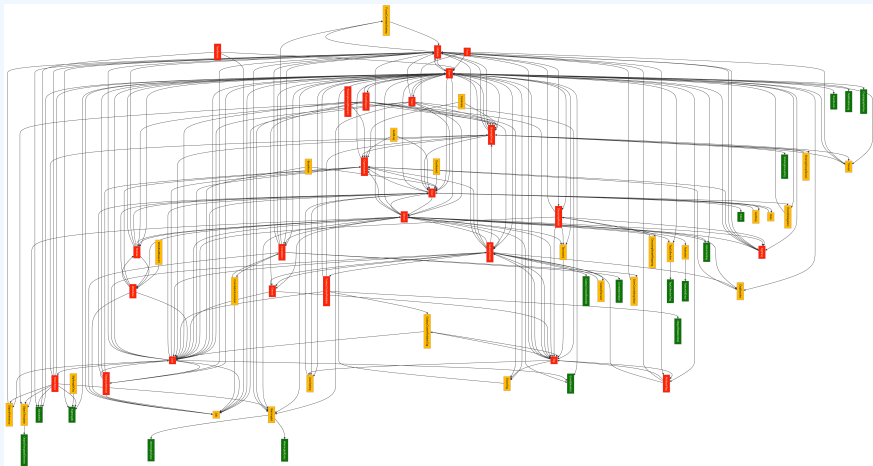


Setting the stage with Cerebrate

- 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

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

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

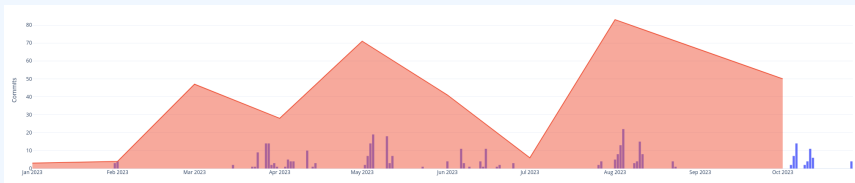
The WireMock server is started ....
port:                8080
enable-browser-proxying:  false
disable-banner:      true
no-request-journal:  false
verbose:             false

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 II



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

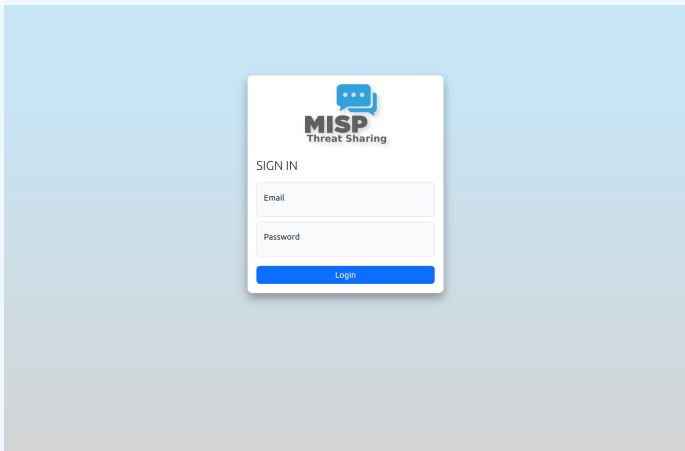
The screenshot shows a GitHub repository interface. At the top, there are navigation buttons: "Go to file", "Add file +", and "Code +". Below these, a status bar indicates "This branch is 333 commits ahead, 914 commits behind 2.4." and a "Contribute +" button.

- 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

Search MISP

Contact Organisation

Organisation Index ¹

Nationalities

Sectors

Previous Next

+ Add organisation All Local orgs External orgs Country: Luxembourg

Enter value to search Search

#	Name	UUID	Members	URL	Nationality	Sector	Type	Actions
1	ORGNOME	7e9251cb-3b15-417a-9e92-e508479c5b4d	2		Luxembourg		ADMIN	
2	CERT-FR_1510	56bd7779-46f9-4353-bd79-2bb95bce212	0		France			

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

Previous Next



CODEBASE MIGRATION: LOOK AND FEEL II

The screenshot displays the MISP (Metasploit Incident Response System) interface. At the top, the navigation bar shows 'Organisations Index > ORGNAME' and a search bar. The main content area is titled 'Organisation View' and contains a 'Details' tab. Below this, a metadata table lists the following information:

ID	1
Name	ORGNAME
UUID	7e9251cb-3b15-417a-9e92-4508479c5b4d
URL	
Nationality	Luxembourg
Sector	
Type	ADMIN
Contacts	

Below the metadata is a 'Users' section with a 'User index' table. The table has columns for ID, Org, Role, Email, and various status icons (active, disabled, etc.), along with SID, Last Login, and Created dates. The table contains two rows of user data:

ID	Org	Role	Email	Active	Disabled	Locked	SID	Last Login	Created	Actions	
1	ORGNAME	admin	admin@admin.test	X	X	X	4000000	X	2023-03-08 07:15:14	[Icons]	
2	ORGNAME	sync_user	sync@admin.test	X	X	X	3367861	✓	0	2022-03-17 10:19:40	[Icons]

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

CODEBASE MIGRATION: LOOK AND FEEL II

The screenshot displays the MISP user interface for the user `admin@admin.test`. The page features a dark header with the MISP logo, navigation links, and a search bar. A sidebar on the left contains various icons for navigation. The main content area shows the user's profile details, including ID, email, organization, role, and notification preferences. Below the profile details are sections for authentication keys and events.

Users Index > `admin@admin.test` Search MISP...

admin

User `admin@admin.test`

ID	1
Email	<code>admin@admin.test</code>
Organisation	ORGNAME
Role	<code>admin</code>
Email notifications	Event published notification No 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

[Authentication keys](#)

[Events](#)

CODEBASE MIGRATION: LOOK AND FEEL II

MISP SharingGroups index > Test edit SG Search MISP...

Create SharingGroups **Online** View Edit

New Sharing Group

General Organisations Instances Summary & Save

Local Organisations Select a local organisation

Remote Organisations Select a remote organisation

Type	Name
local	CERT-FR_1510

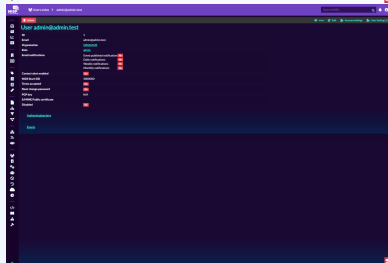
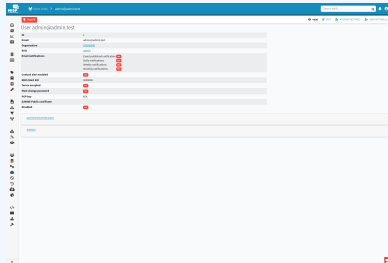
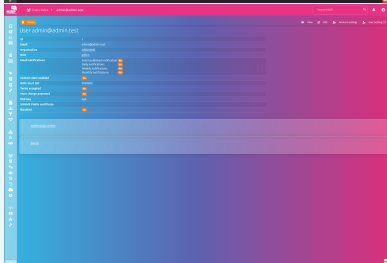
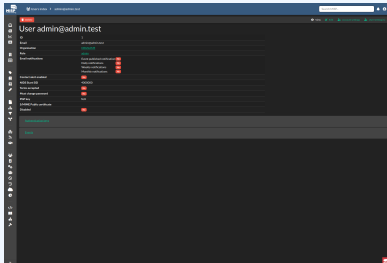
Next page

CODEBASE MIGRATION: LOOK AND FEEL II

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



CODEBASE MIGRATION: LOOK AND FEEL II

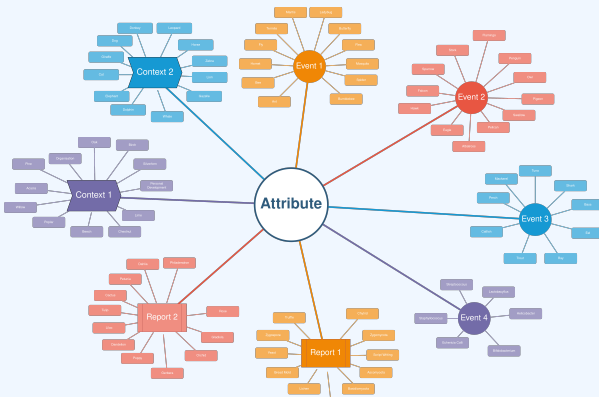


STEP III - THE TODOs

> 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

Export

Export functionality is designed to automatically generate signatures for various AWS services. To enable signature generation for a given attribute, sign the attribute (and be sure to use the same key) as all attribute types are applicable for signature generation, currently we only support X.509 signature generation for ID, domains, host names, user agents etc. and hash for generation for X.509(X.509) values of the attribute. Support for more attribute types is planned.

Simply click on any of the following buttons to download the appropriate data.

Type	Last Update	Description	Outbound	Inbound	Progress	Actions
ZONE	NA	Click this to download all events and attributes that you have access to in MSP-ZONE format. Attachments are enabled on this instance.	Yes	NA	NA	Download Cancel
API	NA	Click this to download all attributes that are indicators and that you have access to in MSP-API format. Attachments are enabled on this instance.	Yes	NA	NA	Download Cancel
CDN_IP	NA	Click this to download all attributes that you have access to in IP-CIDR format.	Yes	NA	NA	Download Cancel
CDN_IP	NA	Click this to download all attributes that you have access to in IP-CIDR format.	Yes	NA	NA	Download Cancel
Domains	NA	Click this to download all relevant content attributes that you have access to under the Domains role format. Only published events and attributes marked as OS Signatures are exported. Administration is able to maintain a whitelist containing host, domain name and IP numbers to exclude from the X.509 export.	Yes	NA	NA	Download Cancel
Host	NA	Click this to download all relevant content attributes that you have access to under the Host role format. Only published events and attributes marked as OS Signatures are exported. Administration is able to maintain a whitelist containing host, domain name and IP numbers to exclude from the X.509 export.	Yes	NA	NA	Download Cancel
IPs	NA	Click this to download all relevant content attributes that you have access to under the IP role format. Only published events and attributes marked as OS Signatures are exported. Administration is able to maintain a whitelist containing host, domain name and IP numbers to exclude from the X.509 export.	Yes	NA	NA	Download Cancel
IPV4	NA	Click this to download a IPv4 document containing the IPv4 version of all events and attributes that you have access to. Attachments are enabled on this instance.	Yes	NA	NA	Download Cancel
STAC	NA	Click this to download a STAC document containing the STAC version of all events and attributes that you have access to. Attachments are enabled on this instance.	Yes	NA	NA	Download Cancel
REC	NA	Click this to download an REC Zone file generated from all zone-wide, hostnames, domain attributes. This can be used for DNS look forwarding. Only published events and attributes marked as OS Signatures are exported.	Yes	NA	NA	Download Cancel
TEXT	NA	Click on any of the buttons below to download all of the attributes with the matching type. This list can be used to feed back into software when searching for suspicious files. Only published events and attributes marked as OS Signatures are exported. Attachments are enabled on this instance.	Yes	NA	NA	Download
File	NA	Click this to download file rules generated from all relevant attributes.	Yes	NA	NA	Download Cancel
Raw	NA	Click this to download raw data generated from all relevant attributes. Rules are returned in a JSON format with information about origin (generated or parsed) and validity.	Yes	NA	NA	Download Cancel

Download CSV (xlsx) file

Powered by AWS IAM, © 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon, the Amazon logo, AWS, the AWS logo, and the AWS text logo are either registered trademarks or trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries.

■ 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

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

[Add Object](#) [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	c5166000-7400-4e30-8085-2f4562b1167e	Analysis	1
Creator org	ORCNAME	Tags	operator top amber phishing/techspies/email-spearfing phishing/distribution/spear-phishing phishing/state/active phishing/psychological/acceptability/needed evictive-language/initial-probability/very-likely
Owner org	ORCNAME	Galaxies	misp-galaxy/target-information/lookup misp-galaxy/contri/lookup misp-galaxy/misp-attack-pattern/spear-phishing-messages-with-malicious-attachments-T1167 misp-galaxy/misp-attack-pattern/spearphishing-Attachment-T1136-001 misp-galaxy/misp-attack-pattern/Phishing-T1166
Contributors		Extends	
Creator user	admin@admin.test	Extended by	46
Protected Event		Related Events	6 related hits
Date	2023-02-07	Feed Hits	1 feed hits
Distribution	1	Server Hits	0 server hits
Published	No	Warninglist Hits	3 warninglist hits

Event activity

27 Oct	29 Oct	31 Oct	02 Nov
1	1	2	1

0 PROPOSALS	2 SIGHTINGS
0 EXTENSIONS	0 DELETED
1 FEED HITS	1 WARNINGLIST HITS
6 RELATIONSHIPS	17 IMA JOCS

Distribution

Objects 6

Attributes 31

Recent sightings

27 Oct	29 Oct	31 Oct
1	2	1

Relevant correlations go here

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

notice for empty event, ...

[Objects](#) [Attributes](#) [Reports](#) [Event Graph](#) [Event Timeline](#) [ATTACK](#) [Discussion](#)

objects

26

35

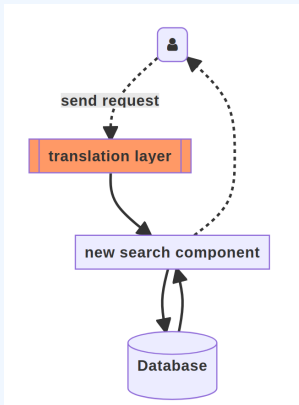
CONSIDERATIONS



- 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



- 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



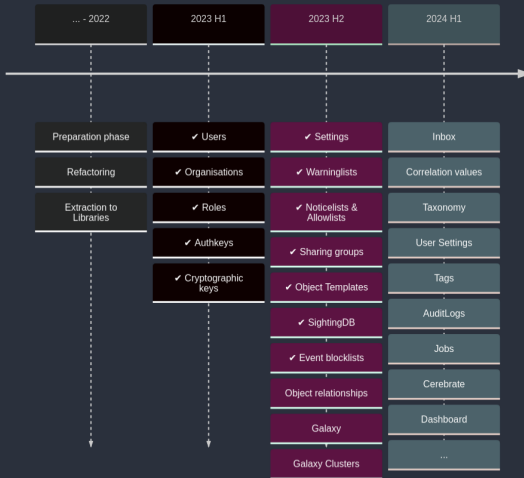
- No one-click update; manual script execution required
- Migration tools will be included in MISP 3 to help you
- This allows us to make underlying changes such as
 - ▶ Database changes
 - ▶ Libraries changes (e.g supervisor in favour of cake-rescue)

> 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 ▾ 3-x branch - [MISP/MISP/tree/3.x](https://github.com/MISP/MISP/tree/3.x)
 - ▶  Project for migration - github.com/orgs/MISP/projects/2