

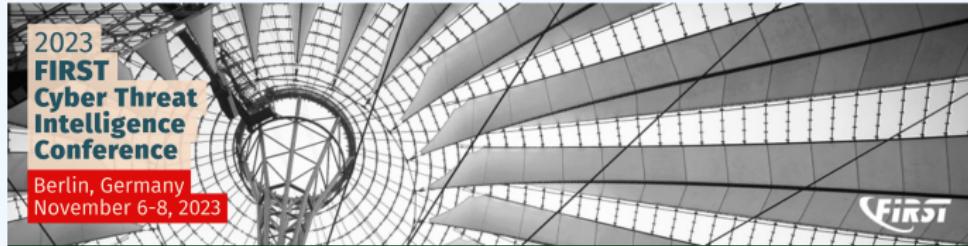
MISP 3 - Teaching an Old Dog New Tricks

Paving the way forward

Andras Iklody & Sami Mokaddem

MISP Project

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

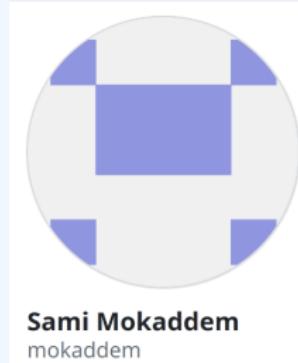


\$ whoarewe



Andras Iklody
iglocska

 @iglocska



 @mokaddem_sami



AGENDA



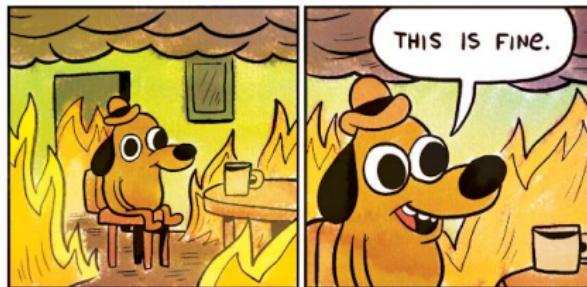
- Why MISP 3?
- The plan
- Considerations

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AN OUTDATED VERSION OF THE FRAMEWORK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 caters to a wide range of use cases
- Lots of features clutter the interface
- All options visible regardless of the user profile
- Lack of coherent page navigation



A screenshot of the MISP web interface. The top navigation bar includes links for Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, and API. A dropdown menu for 'Global Actions' is open, listing various administrative functions such as News, My Profile, My Settings, Set Setting, Organisations, Role Permissions, List Object Templates, List Sharing Groups, Add Sharing Group, List Sharing Groups Blueprints, Add Sharing Group Blueprint, Decaying Models Tool, List Decaying Models, User Guide, Categories & Types, Terms & Conditions, Statistics, List Discussions, and Start Discussion. The main content area shows a grid of event cards, each with a title, date, and other details.

SHORTCOMINGS DUE TO INITIAL DESIGN CHOICES

To list a few..

- Bad database structure
 - ▶ Attribute type, value not a first-class citizen
 - ▶ Logs all in one place
 - ▶ Indexing??
- Files
- 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

PRUNING UNUSED / DEAD END FUNCTIONALITIES

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



STEP I - PREPARING THE GROUND

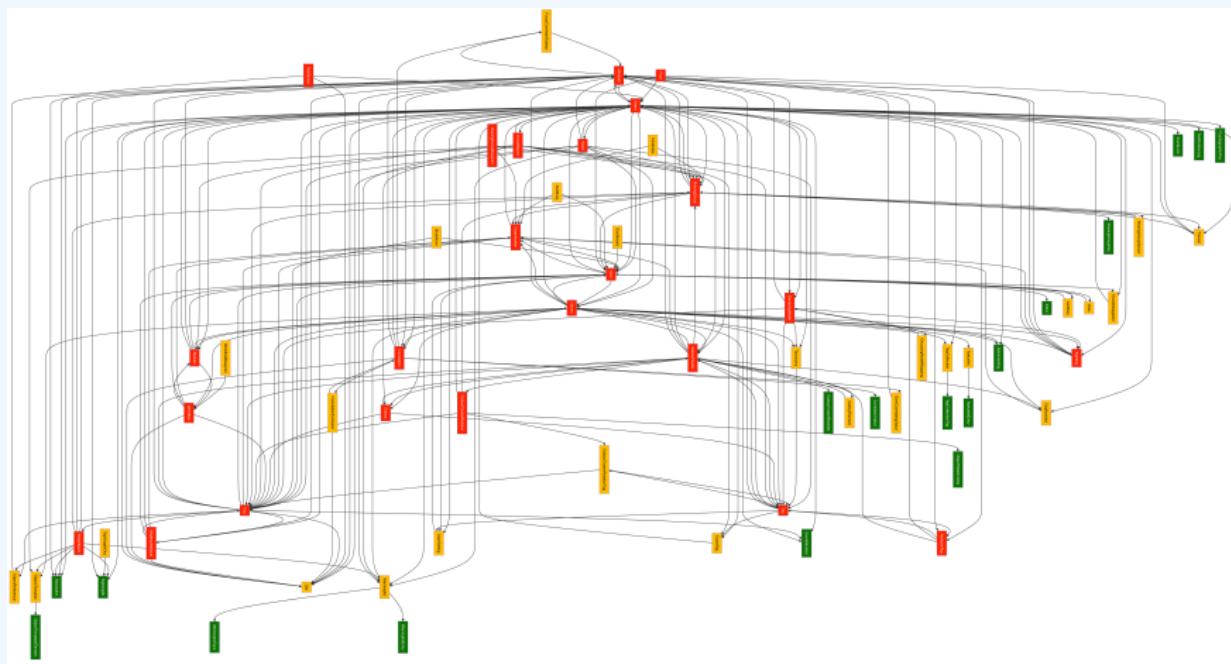
STEP I - PREPARING THE GROUND

- Refactoring the codebase for improved portability using factories
 - ▶ Framework-agnostic
 - ▶ Reusable code for front and back-end
- Setting the stage with Cerebrate
 - ▶ Development started in May 2020
 - ▶ Application built on top of MISP ported 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)	In Progress (1)	Done (8)
This item hasn't been started	This is actively being worked on	This has been completed
MISP #8881 TagCollectionTag	MISP #8882 Sightingdb	MISP #8879 AdminSettings
MISP #8885 Inbox		MISP #8880 WarninglistEntry
MISP #8886 ObjectRelationship		MISP #8883 SharingGroups
MISP #8887 NotificationLog		MISP #8884 ObjectTemplates
MISP #8890 GalaxyClusterBlocklist		MISP #8888 Noticelists
MISP #8891 EventLock		MISP #8889 AllowedList
MISP #8892 EventBlocklist		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:

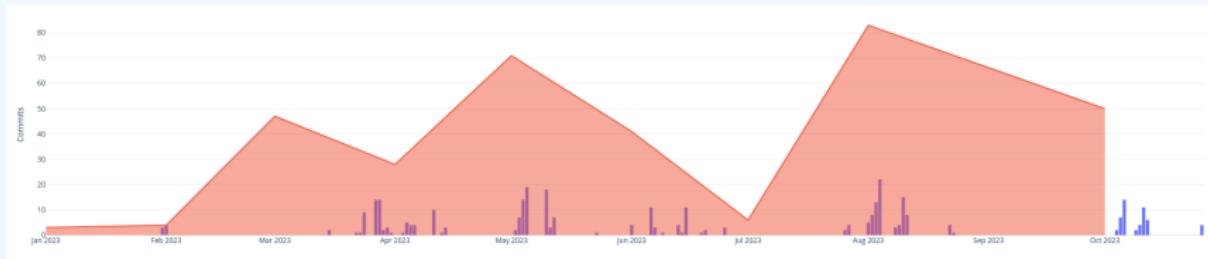
new: [3.x] initial skeleton added ...
iglokska committed on Jan 31

This commit is marked as **Verified**. To the right are buttons for copy, commit ID (35932db), and refresh. The main list of commits shows numerous entries starting with "new: [3.x] initial skeleton added" followed by various file names, indicating the migration of code from version 2.x to 3.x.

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

Name	Last commit message	Last commit date
...		
billingHeaders	fix depreciation notices	7 months ago
glossary	new [3.x] initial skeleton added	10 months ago
addressDesignation.php	new: migration AddressDesignation model moved	10 months ago
addressPlaceholder.php	fix rename table for consistency	8 months ago
Applicable.php	No merge conflicts	3 months ago
AvataregTable.php	new [3.x] initial skeleton added	10 months ago
AuditoryTable.php	add app-test tests	4 months ago
CryptographicKeyTable.php	No use -remove(dlg)	5 months ago
EventBibliotekTable.php	No fix	3 months ago
InventoryTable.php	add basic crud app tests for sharing groups	5 months ago
IntranetTable.php	add add basic user tests, remove contribute part code from ...	7 months ago
JobsTable.php	drag refrence to use migration	last month
LogsTable.php	add migrate command to test jobs	last month
InvestmentAreaTable.php	add post notifications	3 months ago
IndividualTable.php	No fix	3 months ago
ObjectTableAndScriptable.php	No properly validate requirements	3 months ago
ObjectTemplateTableAndScriptable.php	new: migrate object template	3 months ago
ObjectTemplateTable.php	fix parsing poor values	3 months ago
OrganizationsTable.php	add more tests, fix bugs	5 months ago
AreaTable.php	new [3.x] initial skeleton added	10 months ago
ServerTable.php	drag refrence to use migration	last month
SignatureTable.php	No merge conflicts	3 months ago
SignatureTemplateTable.php	No merge conflicts	3 months ago
SignatureTemplateTable.php	No merge conflicts	3 months ago
SignatureTable.php	No use -remove(dlg) instead of -constructor	3 months ago
SignatureTable.php	drag: parseSignature models added	4 months ago
TagCollectorLogTable.php	drag: parseCollector models added	8 months ago
UserTable.php	add (empty) port of SonoffCloud tool and related device adjustments	last month
WarmingElementTable.php	new [parseSigle entry] migration - first revision, Fixes #1000	8 months ago

CODEBASE MIGRATION: WHERE WE STAND II



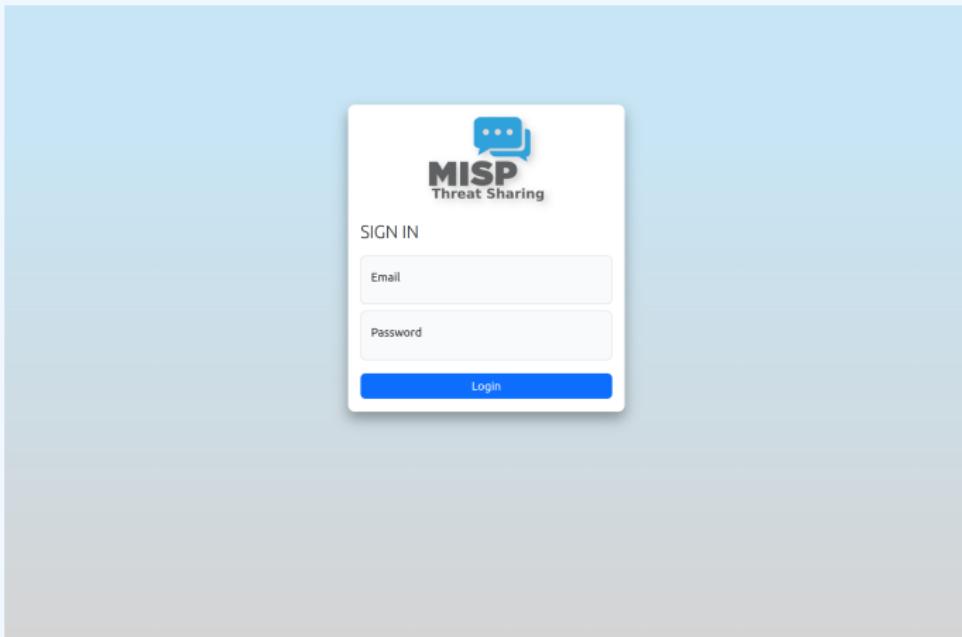
- Migration speed ramping up. The more we port, the faster we go

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

- Even while catering and improving 2.4

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

A vertical sidebar on the left contains numerous small, light-gray icons representing various system functions.

16

CODEBASE MIGRATION: LOOK AND FEEL II

MISP

Organisations index > ORGNAME

Search MISP...

Organisation View

ID	1
Name	ORGNAME
UUID	7e0251cb-3b15-417a-9e92-a508479c5b4d
URL	
Nationality	Luxembourg
Sector	
Type	ADMIN
Contacts	

[Users](#)

User index¹

Previous Next

<input type="checkbox"/> ID	Org	Role	Email						Last Login	Created					Actions	
<input type="checkbox"/>	1	ORGNAME	admin	admin@admin.test				4000000		2023-03-08 07:15:14						
<input type="checkbox"/>	2	ORGNAME	Syncuser	sync@admin.test				3367861		0	2022-03-17 10:19:40					

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 'User index' page of the MISP system. The interface includes a sidebar with various icons, a top navigation bar with 'Users index', a search bar, and user settings links. The main content area displays a table of users with columns: ID, Org, Role, Email, and several status and action icons. The table shows two entries:

ID	Org	Role	Email					SID	Last Login	Created				Actions
1	ORGNAME	admin	admin@admin.test	X	X	X	X	4000000	2023-03-08 07:15:14	2022-03-17 10:19:40	X	X	X	<input type="checkbox"/>
2	ORGNAME	Sync user	sync@admin.test	X	X	X	X	3367861	✓	0	✓	✓	✓	<input checked="" type="checkbox"/>

Below the table, a message indicates 'Page 1 of 1, showing 2 users out of 2 total, starting on record 1, ending on 2'. Navigation buttons for 'Previous' and 'Next' are also present.

CODEBASE MIGRATION: LOOK AND FEEL II

The screenshot shows the MISP user profile for the user 'admin@admin.test'. The top navigation bar includes links for 'Users Index' and 'admin@admin.test', along with search and account management options. The main content area displays the user's details, including their ID (1), email (admin@admin.test), organization (GRCNAME), and role (admin). Under 'Email notifications', there are four checkboxes: 'Event published notification' (checked), 'Daily notifications' (unchecked), 'Weekly notifications' (unchecked), and 'Monthly notifications' (unchecked). Other settings shown include 'Contact alert enabled' (unchecked), 'NIDS Start SID' (4000000), 'Terms accepted' (unchecked), 'Must change password' (unchecked), 'PGP key' (N/A), and 'S/MIME Public certificate' (disabled). Below these settings are two sections: 'Authentication keys' and 'Events', each containing a single link.

ID	1
Email	admin@admin.test
Organisation	GRCNAME
Role	admin
Email notifications	<input checked="" type="checkbox"/> Event published notification <input type="checkbox"/> Daily notifications <input type="checkbox"/> Weekly notifications <input type="checkbox"/> Monthly notifications
Contact alert enabled	<input type="checkbox"/>
NIDS Start SID	4000000
Terms accepted	<input type="checkbox"/>
Must change password	<input type="checkbox"/>
PGP key	N/A
S/MIME Public certificate	
Disabled	<input checked="" type="checkbox"/>

[Authentication keys](#)

[Events](#)

CODEBASE MIGRATION: LOOK AND FEEL II

SharingGroups index

Search MISP...

List Sharing Group Blueprints

Sharing Groups

Activity Past 7 days: + 0

Actives Roerings

Previous Next

+ Add sharing All Active Sharing Groups Passive Sharing Groups

<input type="checkbox"/>	ID	UUID	Name	Creator	Description	Org count	Releasable to	Roering	Active	Actions
<input type="checkbox"/>	3	05e79887-a8c2-413c-8c4f-b41ffcdce679	Financial group	ORIGINAME	No desc	2	Financial sector			
<input type="checkbox"/>	4	81ba3260-23c3-4309-b84a-cab27272993b	Banking group	ORIGINAME		2	Banking community			
<input type="checkbox"/>	15	13cd9717-195b-4d27-ab61-47f34c374146	Test edit SG	ORIGINAME		1	Not defined			

Page 1 of 1, showing 3 sharing groups out of 3 total, starting on record 1, ending on 3

Previous Next

CODEBASE MIGRATION: LOOK AND FEEL II

The screenshot shows the MISP SharingGroups Index page with the URL [SharingGroups Index > Financial group](#). The page title is "New Sharing Group". On the left is a vertical toolbar with various icons. The main area has tabs: General (selected), Organisations, Instances, and Summary & Save. Under "General", there are two dropdowns: "Local Organisations" (Select a local organisation) and "Remote Organisations" (Select a remote organisation). Below these is a table:

Type	Name	UUID	Extend	Actions
local	ORIONAME	7e9251c8-3b15-417a-9e92-a508479c5b4d	<input checked="" type="checkbox"/>	
remote	CERT-FR_1510	56bdf779-4ef8-4353-bd79-2bb95bce2212	<input type="checkbox"/>	

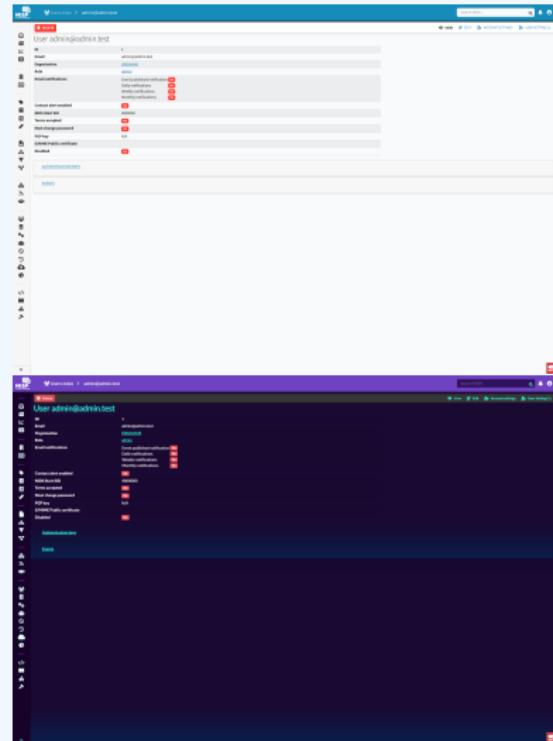
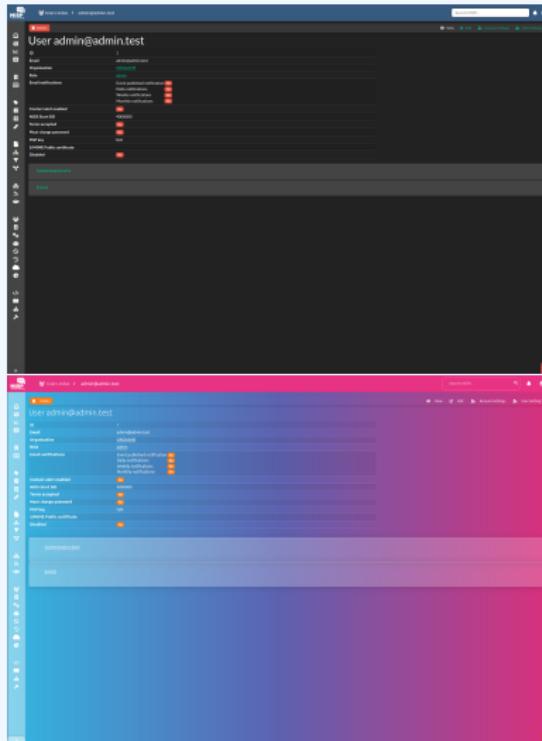
At the bottom left is a "Next page" button.

CODEBASE MIGRATION: LOOK AND FEEL II

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



CODEBASE MIGRATION: LOOK AND FEEL II

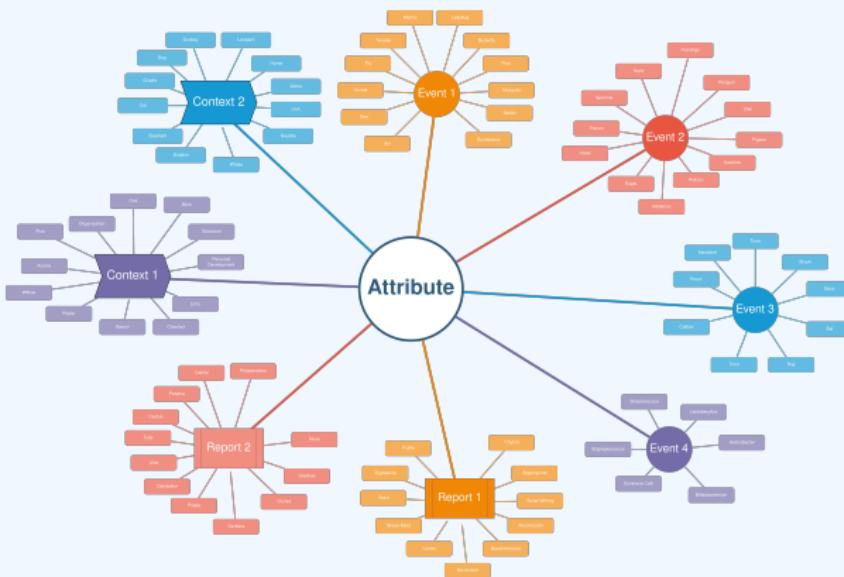


STEP III - THE TODOS

REDEFINE HOW WE INTERACT WITH DATA I

■ Indicator centric perspective

- ▶ Unified view of everything we know about the Indicator
- ▶ Allows to take better decisions
- ▶ Enable users to manage their IoC working set



REDEFINE HOW WE INTERACT WITH DATA II

■ Unified search mechanics

- ▶ Code deduplication
- ▶ Streamlined way to search for data
- ▶ Translation layer to known format

The Export feature is designed to automatically generate signatures for detection systems. To enable signature generation for a given attribute, the signature field of this attribute must be set to Yes. Note that not all attribute types are applicable for signature generation; currently we only support X509 signature generation for IP address, host names, user agents etc., and hash generation for MD5/HMAC values of the artifacts. Support for more attribute types is planned.

Simple click on any of the following buttons to download the appropriate files.

Type	Last Update	Description	Downloaded	Filesize	Progress	Actions
JSON	N/A	Click this to download all events and attributes that you have access to in X509 JSON format. All signatures are enabled on this instance.	Yes	N/A	N/A	Download Cancel
XML	N/A	Click this to download all events and attributes that you have access to in X509 XML format. All signatures are enabled on this instance.	Yes	N/A	N/A	Download Cancel
CSV_Req	N/A	Click this to download all attributes that are indicated and that you have access to (except for the attachment) in CSV format.	Yes	N/A	N/A	Download Cancel
CSV_Alt	N/A	Click this to download all events that are indicated and that you have access to in CSV format. Only published events and attributes marked as X509 Signatures are exported. Administration is able to filter by domain name or a subdomain containing host, domain name and IP numbers to exclude from the X509 export.	Yes	N/A	N/A	Download Cancel
Sumatra	N/A	Click this to download all events and attributes that you have access to in Sumatra XML format. Only published events and attributes marked as X509 Signatures are exported. Administration is able to filter by domain name or a subdomain containing host, domain name and IP numbers to exclude from the X509 export.	Yes	N/A	N/A	Download Cancel
Smart	N/A	Click this to download all relevant attributes that you have access to under the Smart file format. Only published events and attributes marked as X509 Signatures are exported. Administration is able to filter by domain name or a subdomain containing host, domain name and IP numbers to exclude from the X509 export.	Yes	N/A	N/A	Download Cancel
One	N/A	Click this to download all relevant attributes that you have access to under the One file format. Only published events and attributes marked as X509 Signatures are exported. Administration is able to filter by domain name or a subdomain containing host, domain name and IP numbers to exclude from the X509 export.	Yes	N/A	N/A	Download Cancel
STIX	N/A	Click this to download a STIX document containing the X509 version of all events and artifacts that you have access to. All signatures are enabled on this instance.	Yes	N/A	N/A	Download Cancel
STIX2	N/A	Click this to download a STIX2 document containing the X509 version of all events and artifacts that you have access to. All signatures are enabled on this instance.	Yes	N/A	N/A	Download Cancel
X509	N/A	Click this to download an X509 Zone file generated from a list of IP-only, hostname, domain attributes. This can be used for DNS level monitoring. Only published events and attributes marked as X509 Signatures are exported.	Yes	N/A	N/A	Download Cancel
TEXT	N/A	Click on 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 X509 Signatures are exported. Administrators are enabled on this instance.	Yes	N/A	N/A	Download
Yara	N/A	Click this to download Yara rules generated from all relevant artifacts. Rules are returned in a JSON format with information about origin (generated or parsed) and validity.	Yes	N/A	N/A	Download Cancel
Raw	N/A	Click this to download raw files generated from all relevant artifacts.	Yes	N/A	N/A	Download Cancel

Powered by [MISP 2.6.11](#) - 2020-01-02 11:30:54

REDEFINE HOW WE INTERACT WITH DATA III

- Refactor the Event view
 - ▶ Key Elements at first glance
 - ▶ Emphasis on the context (Taxonomies, Galaxies, Correlation, ·)
 - ▶ Sneak peak ? 😊

SNEAK PEAK OF THE NEW EVENT VIEW - WIP

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

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	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 , executive language , bad mood probability , very likely , misp-galaxy-target-information , Luxembourg , misp-galaxy-country , Luxembourg , 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
Owner org	ORGNAME	Galaxies	
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

0 PROPOSALS 2 SIGHTINGS

0 EXTENSIONS 0 DELETED

1 FEED HITS 1 WARNINGLIST HITS

6 RELATIONSHIPS 17 5% IOCS

Distribution

Objects 6

Attributes 31

Recent sightings

27 Oct 29 Oct 31 Oct 02 Nov

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 ATT&CK® Discussion 1

objects

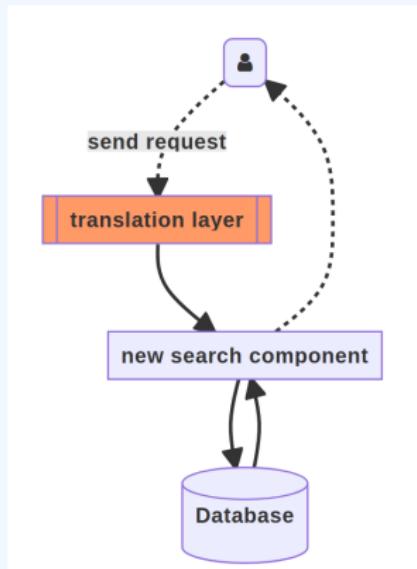
CONSIDERATIONS



- 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% match** with the old API
- Partially due to 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 datapoint
 - ▶ 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



- MISP 2.4 will be **supported for a limited time**
- **6 months** support post MISP 3 release
 - ▶ No one-click update; manual script execution required
 - ▶ Migration tools will be included in MISP 3 to help you
 - ▶ Allow us to make underlying changes such as
 - Database changes
 - Libraries changes (e.g supervisor in favor of cake-resque)

INSTALLATION FOR NEW INSTANCES

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



OUR EXPECTATIONS FROM 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