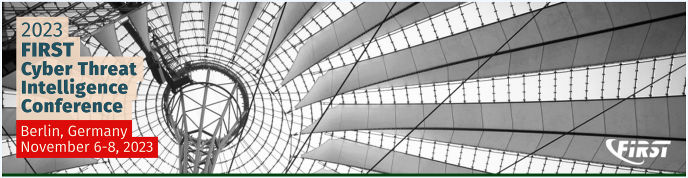
MISP 3 - Teaching an Old Dog New Tricks

Paving the way forward

Andras Iklody & Sami Mokaddem

MISP Project
https://www.misp-project.org/

MISP
Threat Sharing



$ whoarewe

Andras Iklody
iglocska

@iglocska

Sami Mokaddem
mokaddem

@mokaddem_sami

Agenda

- Why MISP 3?
- The plan
- Considerations

Why MISP 3?

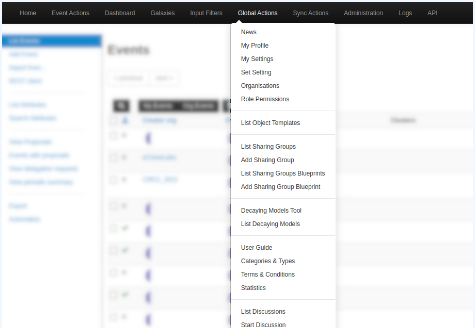
> An outdated version of the framework

CakePHP
Build fast, grow solid.

- 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

> 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

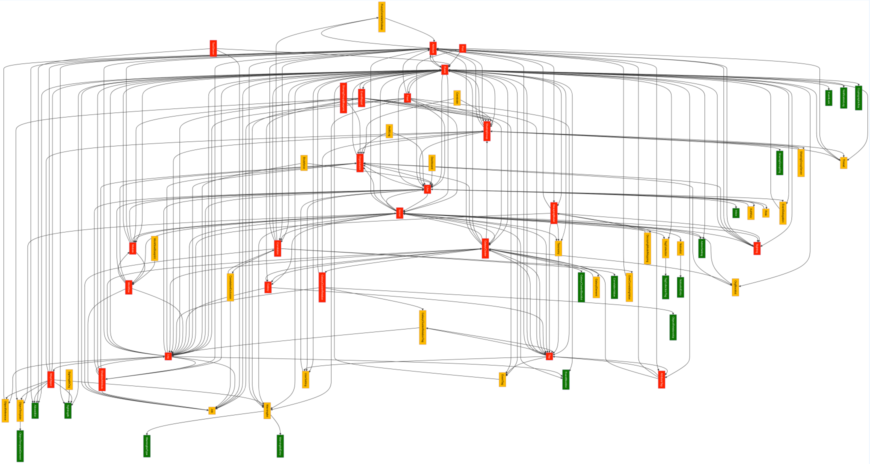
CEREBRATE
Project

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, ···

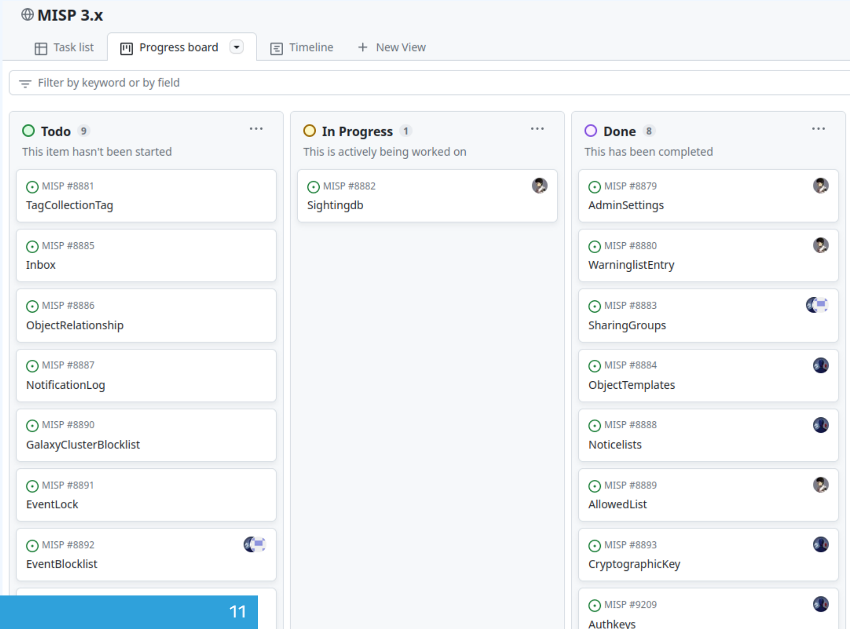
Step I - Identifying inter-dependencies

Migrate least connected part first



Step II - Porting the codebase

> Step II - Roadmap for a 3-wave porting



MISP 3.x

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

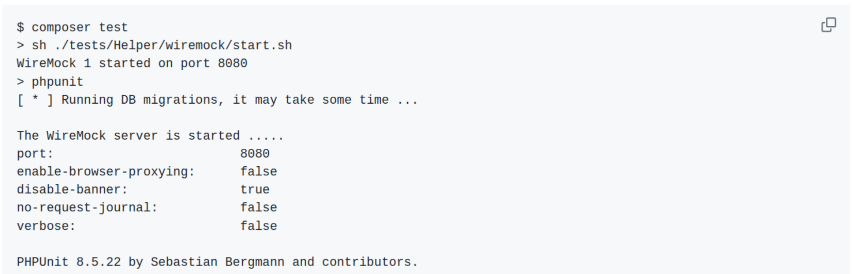
Wave 2 More glue relying on component already migrated

- E.g. Authkey, *-Tag, Taxonomy

Wave 3 The actual meat of the application

- E.g. Attribute, Event, Workflow

> Step II - Test driven development

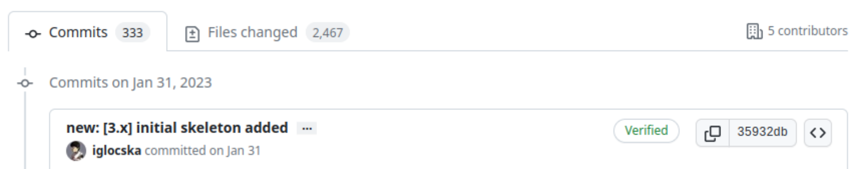


```
$ composer test
> sh ./tests/Helper/wiremock/start.sh
WireMock 1 started on port 8080
> phpunit
[ * ] Running DB migrations, it may take some time ...

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



Commits 333

Files changed 2,467

5 contributors

Commits on Jan 31, 2023

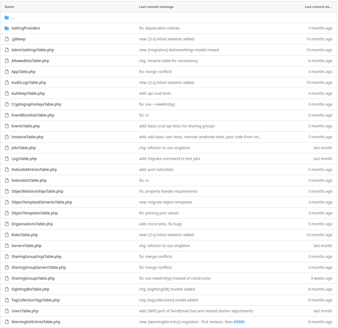
new: [3.x] initial skeleton added ···

iglocska committed on Jan 31

Verified

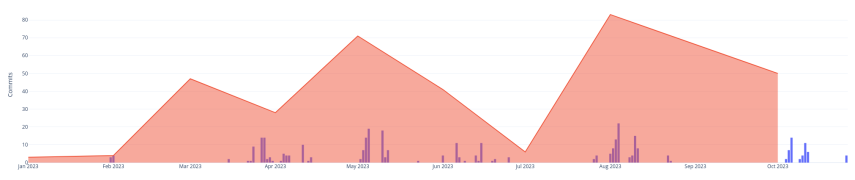
35932db

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

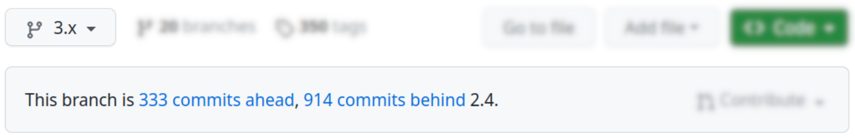


Name	Last commit message	Last commit da...
..		
SettingProviders	fix: deprecation notices	7 months ago
.gitkeep	new: [3.x] initial skeleton added	10 months ago
AdminSettingsTable.php	new: [migration] Adminsettings model moved	10 months ago
AllowedlistsTable.php	chg: rename table for consistency	6 months ago
AppTable.php	fix: merge conflicts	3 months ago
AuditLogsTable.php	new: [3.x] initial skeleton added	10 months ago
AuthKeysTable.php	add: api crud tests	4 months ago
CryptographicKeysTable.php	fix: use ->newEntity()	3 months ago
EventBlocklistsTable.php	fix: cs	5 months ago
EventsTable.php	add: basic crud api tests for sharing groups	5 months ago
InstanceTable.php	add: add basic user tests, remove cerebrate tests, port code from cer...	7 months ago
JobsTable.php	chg: refactor to use singleton	last month
LogsTable.php	add: migrate command to test jobs	last month
NoticelistEntriesTable.php	add: port noticelists	5 months ago
NoticelistsTable.php	fix: cs	3 months ago
ObjectRelationshipsTable.php	fix: properly handle requirements	3 months ago
ObjectTemplateElementsTable.php	new: migrate object templates	3 months ago
ObjectTemplatesTable.php	fix: parsing json values	3 months ago
OrganisationsTable.php	add: more tests, fix bugs	5 months ago
RolesTable.php	new: [3.x] initial skeleton added	10 months ago
ServersTable.php	chg: refactor to use singleton	last month
SharingGroupOrgsTable.php	fix: merge conflicts	3 months ago
SharingGroupServersTable.php	fix: merge conflicts	3 months ago
SharingGroupsTable.php	fix: use newEntity() instead of constructor	3 weeks ago
SightingdbsTable.php	chg: [sightingDB] models added	8 months ago
TagCollectionTagsTable.php	chg: [tagcollections] model added	8 months ago
UsersTable.php	add: [WiP] port of SendEmail tool and related docker adjustments	last month
WarninglistEntriesTable.php	new: [warninglist entry] migration - first revision, fixes #8880	8 months ago

> Codebase Migration: Where We Stand II



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



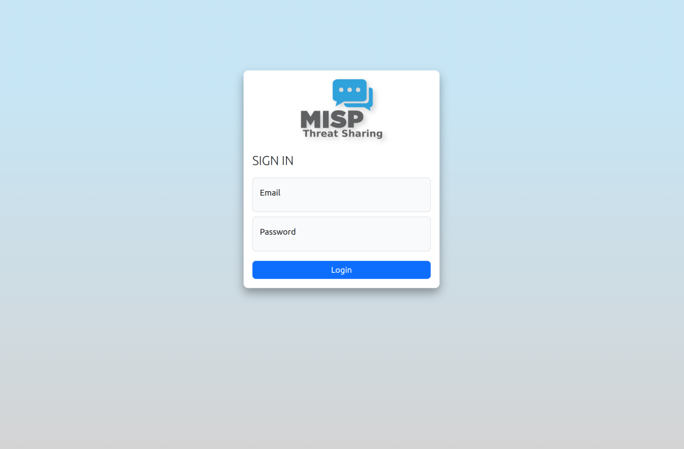
This branch is 333 commits ahead, 914 commits behind 2.4.

- 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



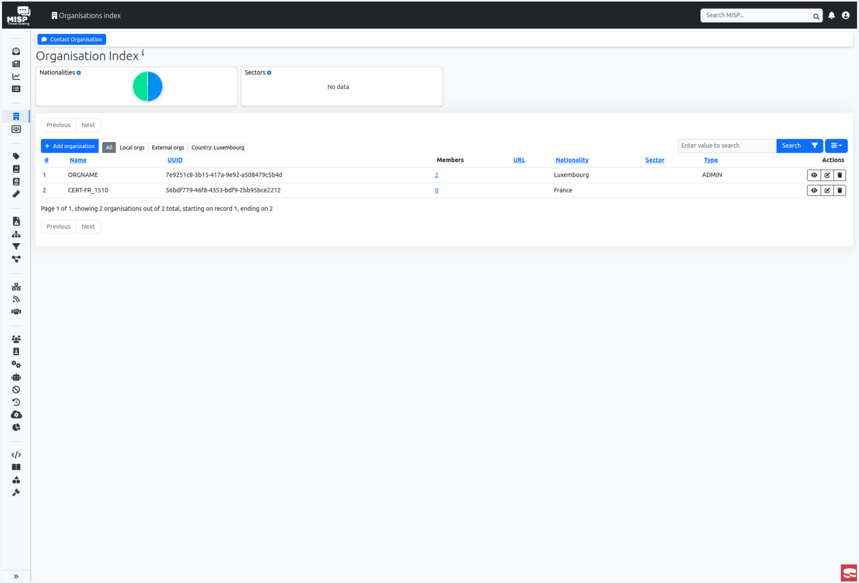
MISP Threat Sharing

SIGN IN

Email

Password

Codebase Migration: Look and Feel II

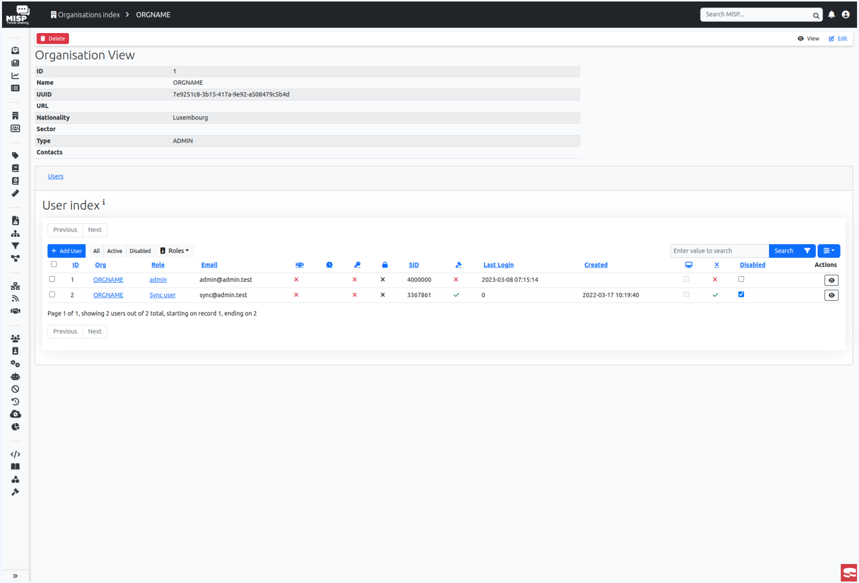


Organisation Index ℹ

#	Name	UUID	Members	URL	Nationality	Sector	Type	Actions
1	ORGNAME	7e9251c8-3b15-417a-9e92-a508479c5b4d	2		Luxembourg		ADMIN	
2	CERT-FR_1510	56bdf779-46f8-4353-bdf9-2bb95bce2212	0		France			

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

Codebase Migration: Look and Feel II



Organisation View

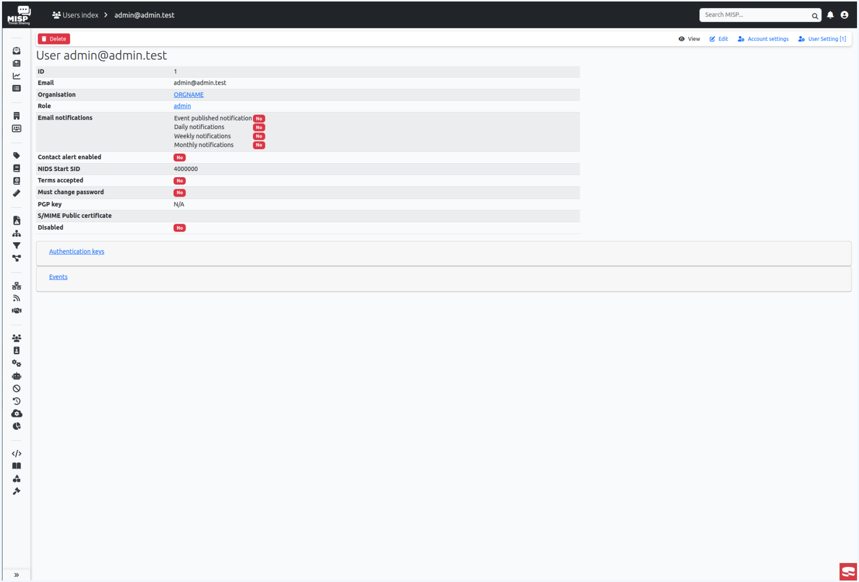
ID	1
Name	ORGNAME
UUID	7e9251c8-3b15-417a-9e92-a508479c5b4d
URL	
Nationality	Luxembourg
Sector	
Type	ADMIN
Contacts	

User index i

☐	ID	Org	Role	Email					SID		Last Login	Created		✕	Disabled	Actions
☐	1	ORGNAME	admin	admin@admin.test	✗		✗	✗	4000000	✗	2023-03-08 07:15:14		☐	✗	☐	👁
☐	2	ORGNAME	Sync user	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

Codebase Migration: Look and Feel II



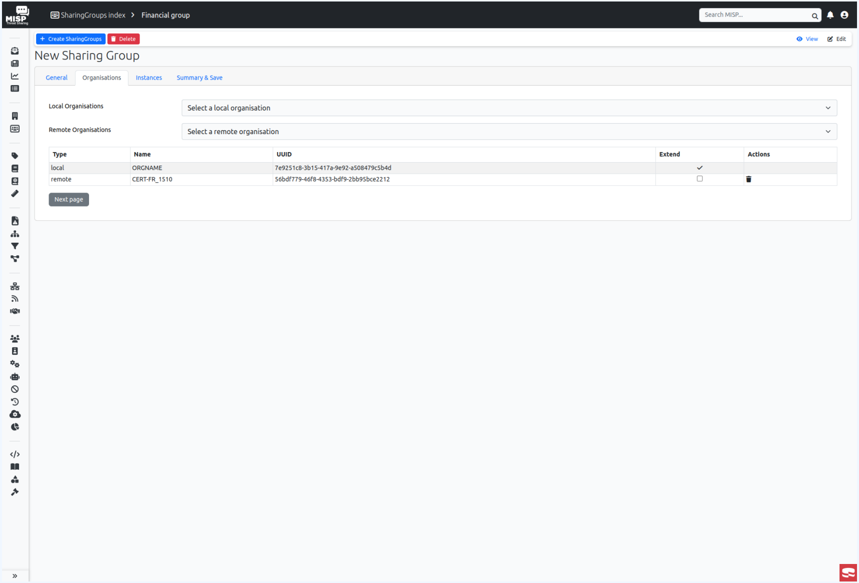
User admin@admin.test

ID	1
Email	admin@admin.test
Organisation	ORGNAME
Role	admin
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



New Sharing Group

Local Organisations: Select a local organisation

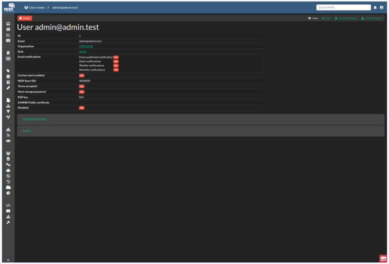
Remote Organisations: Select a remote organisation

Type	Name	UUID	Extend	Actions
local	ORGNAME	7e9251c8-3b15-417a-9e92-a508479c5b4d	✓	
remote	CERT-FR_1510	56bdf779-46f8-4353-bdf9-2bb95bce2212	□	🗑

Codebase Migration: Look and Feel II

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

Codebase Migration: Look and Feel II

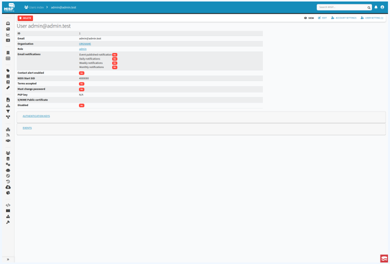


User admin@admin.test

ID	1
Email	admin@admin.test
Organisation	ORGNAME
Role	admin
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

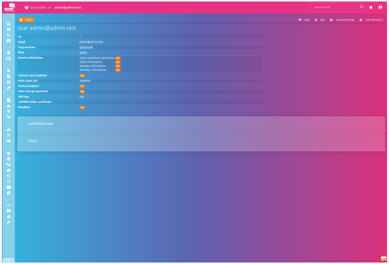


User admin@admin.test

ID	1
Email	admin@admin.test
Organisation	ORGNAME
Role	admin
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

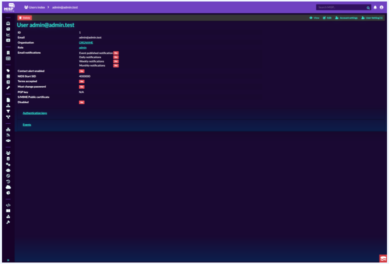


User admin@admin.test

ID	1
Email	admin@admin.test
Organisation	ORGNAME
Role	admin
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



User admin@admin.test

ID	1
Email	admin@admin.test
Organisation	ORGNAME
Role	admin
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

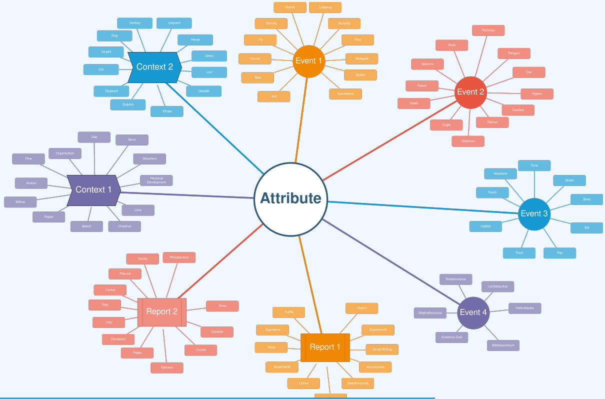
Authentication keys

Events

Step III - The TODOs

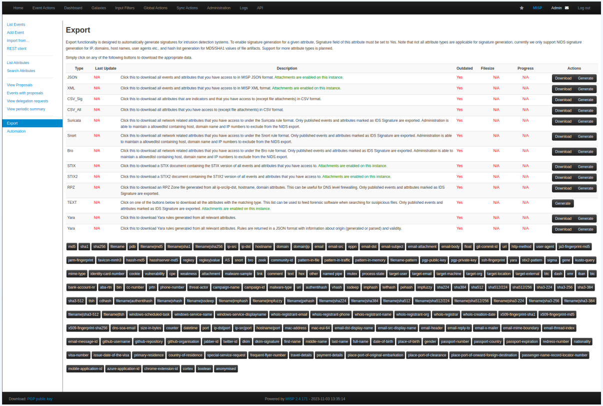
> Redefine how we interact with data I

- 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 intrusion detection systems. To enable signature generation for a given attribute, 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 NIDS signature generation for IP, domains, host names, user agents etc., and hash list generation for MD5/SHA1 values of file artifacts. Support for more attribute types is planned.

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

Type	Last Update	Description	Outdated	Filesize	Progress	Actions
JSON	N/A	Click this to download all events and attributes that you have access to in MISP JSON format. Attachments are enabled on this instance.	Yes	N/A	N/A	Download Generate
XML	N/A	Click this to download all events and attributes that you have access to in MISP XML format. Attachments are enabled on this instance.	Yes	N/A	N/A	Download Generate
CSV_Sig	N/A	Click this to download all attributes that are indicators and that you have access to (except file attachments) in CSV format.	Yes	N/A	N/A	Download Generate
CSV_All	N/A	Click this to download all attributes that you have access to (except file attachments) in CSV format.	Yes	N/A	N/A	Download Generate
Suricata	N/A	Click this to download all network related attributes that you have access to under the Suricata rule format. Only published events and attributes marked as IDS Signature are exported. Administration is able to maintain a allowedlist containing host, domain name and IP numbers to exclude from the NIDS export.	Yes	N/A	N/A	Download Generate
Snort	N/A	Click this to download all network related attributes that you have access to under the Snort rule format. Only published events and attributes marked as IDS Signature are exported. Administration is able to maintain a allowedlist containing host, domain name and IP numbers to exclude from the NIDS export.	Yes	N/A	N/A	Download Generate
Bro	N/A	Click this to download all network related attributes that you have access to under the Bro rule format. Only published events and attributes marked as IDS Signature are exported. Administration is able to maintain a allowedlist containing host, domain name and IP numbers to exclude from the NIDS export.	Yes	N/A	N/A	Download Generate
STIX	N/A	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	N/A	N/A	Download Generate
STIX2	N/A	Click this to download a STIX2 document containing the STIX2 version of all events and attributes that you have access to. Attachments are enabled on this instance.	Yes	N/A	N/A	Download Generate
RPZ	N/A	Click this to download an RPZ Zone file generated from all ip-src/ip-dst, hostname, domain attributes. This can be useful for DNS level firewalling. Only published events and attributes marked as IDS Signature are exported.	Yes	N/A	N/A	Download Generate
TEXT	N/A	Click on one of the buttons below to download all the attributes with the matching type. This list can be used to feed forensic software when searching for susipicious files. Only published events and attributes marked as IDS Signature are exported. Attachments are enabled on this instance.	Yes	N/A	N/A	Generate
Yara	N/A	Click this to download Yara rules generated from all relevant attributes.	Yes	N/A	N/A	Download Generate
Yara	N/A	Click this to download Yara rules generated from all relevant attributes. Rules are returned in a JSON format with information about origin (generated or parsed) and validity.	Yes	N/A	N/A	Download Generate

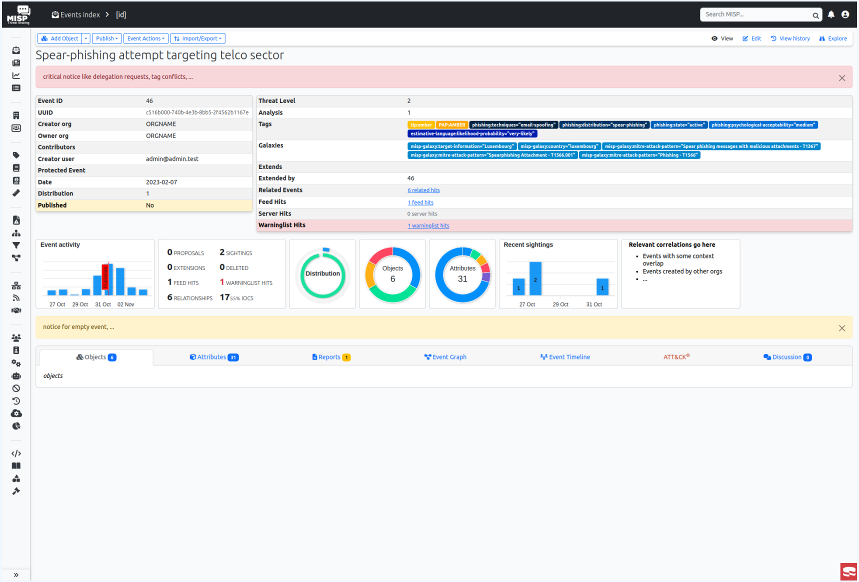
Download: PGP public key

Powered by MISP 2.4.171 - 2023-11-03 13:35:14

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



Spear-phishing attempt targeting telco sector

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

Event ID	46
UUID	c516b000-740b-4e3b-8bb5-2f4562b1167e
Creator org	ORGNAME
Owner org	ORGNAME
Contributors	
Creator user	admin@admin.test
Protected Event	
Date	2023-02-07
Distribution	1
Published	No

Threat Level	2
Analysis	1
Tags	tlp:amber PAP:AMBER phishing:techniques="email-spoofing" phishing:distribution="spear-phishing" phishing:state="active" phishing:psychological-acceptability="medium" estimative-language:likelihood-probability="very-likely"
Galaxies	misp-galaxy:target-information="Luxembourg" misp-galaxy:country="luxembourg" misp-galaxy:mitre-attack-pattern="Spear phishing messages with malicious attachments - T1367" misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" misp-galaxy:mitre-attack-pattern="Phishing - T1566"
Extends	
Extended by	46
Related Events	6 related hits
Feed Hits	1 feed hits
Server Hits	0 server hits
Warninglist Hits	1 warninglist hits

0 PROPOSALS
2 SIGHTINGS
0 EXTENSIONS
0 DELETED
1 FEED HITS
1 WARNINGLIST HITS
6 RELATIONSHIPS
17 55% IOCS

Relevant correlations go here

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

notice for empty event, ...

objects

Considerations

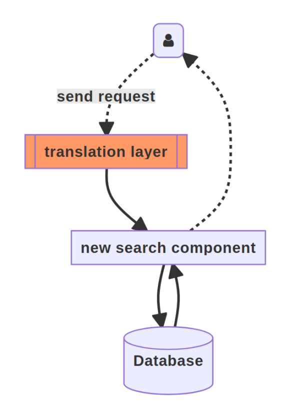
> MISP Core format

MISP
STANDARD
collaborative intelligence

- 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

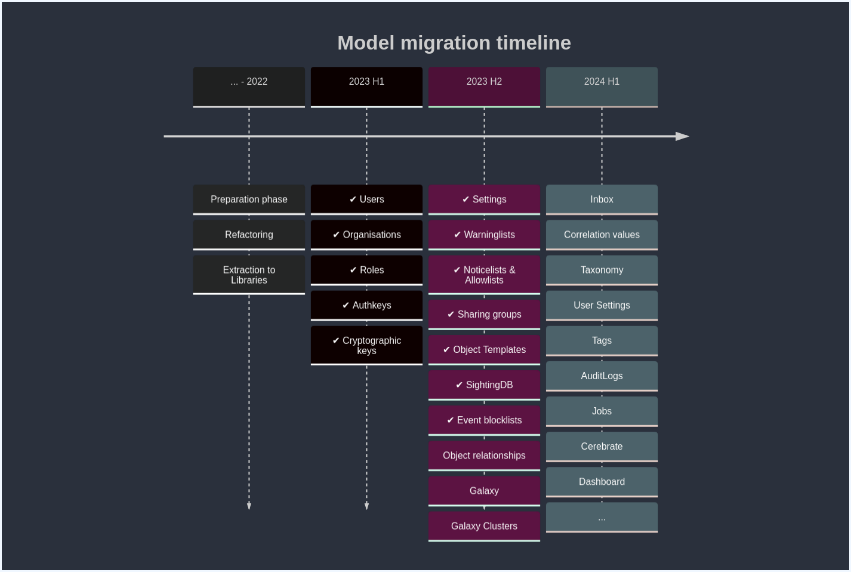
SO, HOW DO WE UPDATE OUR MISP?
THAT'S THE NEAT PART, YOU DON'T
imgflip.com

- No one-click update; manual script execution required
- Migration tools will be included in MISP 3 to help you
- This allows us to make underlaying 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 targerts: **Ubuntu** and **RHEL**

Alright gentlemen, we need a new idea
For installation of new instances
Native installation, Docker installer
Simplified native installation, Upstream Docker installer
imgflip.com



Model migration timeline

... - 2022

- Preparation phase
- Refactoring
- Extraction to Libraries

2023 H1

- ✔ Users
- ✔ Organisations
- ✔ Roles
- ✔ Authkeys
- ✔ Cryptographic keys

2023 H2

- ✔ Settings
- ✔ Warninglists
- ✔ Noticelists & Allowlists
- ✔ Sharing groups
- ✔ Object Templates
- ✔ SightingDB
- ✔ Event blocklists
- Object relationships
- Galaxy
- Galaxy Clusters

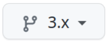
2024 H1

- Inbox
- Correlation values
- Taxonomy
- User Settings
- Tags
- AuditLogs
- Jobs
- Cerebrate
- Dashboard
- ...

> 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 lauching 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`