# MISP 3 - Teaching an Old Dog New Tricks Paving the way forward

Andras Iklody & Sami Mokaddem

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











#### 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 AN OUTDATED VERSION OF THE FRAMEWORK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
- CakePHP supports PHP version <=7.4</p>
  - 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

	Input Filters Global Actions	Sync Actions Ac		
Events	News My Profile My Settings Set Setting Organisations Role Permitsions			
	List Object Templ		-	
	List Sharing Grou Add Sharing Grou List Sharing Grou	1p		
 0* E	Add Sharing Gro Decaying Models	Tool		
0 × 4	List Decaying Mo User Guide	dels		
0.0	Categories & Typ Terms & Conditio Statistics			
0* 6	List Discussions Start Discussion			

#### > 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  $\rightarrow$  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

#### **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

## ① MISP 3.x

Task list Progress board 📼 E Timeline + New View = Filter by keyword or by field O In Progress 1 O Todo 9 O Done 8 This item hasn't been started This is actively being worked on This has been completed Ø MISP #8881 • MISP #8882 • MISP #8879 TagCollectionTag Sightingdb AdminSettings • MISP #8885 • MISP #8880 WarninglistEntry Inbox • MISP #8886 • MISP #8883 ObjectRelationship SharingGroups

• MISP #8887 NotificationLog

MISP #8890 GalaxyClusterBlocklist

• MISP #8891

EventLock

EventBlocklist

• MISP #8884

MISP #8889 AllowedList

Noticelists

ObjectTemplates

۲

۲

۲

#### 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

-0- C	ommits 333	E Files changed 2,467		🗓 5 contributors
	ommits on Jan 3	1, 2023		
	new: [3.x] initia	al skeleton added	Verified	35932db <>

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

Note         Note         Note           0         Independent of the sector of			
Impact         space         space <t< th=""><th>None</th><th>Last conmit message</th><th>Cast spread do</th></t<>	None	Last conmit message	Cast spread do
Best         Best         Best           Company         Best         Best         Best           Domany         Best         Best<	B.C.		
Bestamping         separational productional productintegemeterefeetee productional productintegemeterefeetee produc	E SellingPresident	The depreciation nutries	7 months ago
Bankary         quencharged         quencharged         quencharged           Bankary         approximation         quencharged         quencharged           Bankary         approximation         quencharged         quencharged           Bankary         approximation         quencharged         quencharged           Bankary         approximation         quencharged         quencharged           Bankary         quencharged         quencharged         quencharged           Bankary         quencharged         quencharged         quencharged           Bankary         quencharged         quencharged         quencharged         quencharged           Bankary         quencharged         quencharged         quencharged         quencharged         quencharged           Bankary         quencharged         quencharged <td< th=""><td>G 40000</td><td>new: [3.4] initial devictor-added</td><td>18 months ago</td></td<>	G 40000	new: [3.4] initial devictor-added	18 months ago
Bytespin         expeription         expeription         expeription         expeription           Bytespin         expeription         expeription         experip	dit elitargetiserieta []	next progratics) Administratings model mased	18 months ago
Bargency	d wiewodirzticke.ptp	drig reneme table for considency	6 months ago
Bayenergine         environment         environment         environment         environment           Comparationment         environment         environment         environment         environment           Comparation	C Appliation php	fic marga canflets	3 months age
Operational part of the second part of the seco	C Autoplatepp	new [3.4] initial skeleton-added	18 months age
Bestandige         National (Section Section S	C Autoryclassysp	add aptoral tests	á monite aga
Benomp         International Accession Acces	C Crystographic Crystole (19)	In us countrily	1 months ago
Parkange         Balange         <	C Investionalization pro	Sc ii	5 months ago
Braining         Springer	C teenahole.php	add, basic crud api teets for sharing groups	5 months ago
Optimization         improvementation         team           Optimization         improvementation         team           Optimization         Second         team           Optimization         team         team           Optimization	🗅 tratancefeble.php	add, add basic user tests, venove conduste tests, part code from car.,	7 months ago
Ownerspace         approximation         approximation         approximation	C pts/laticptp	thig reflector to use singleton	let month
Bandwardson         No         No           Destinationation of the second	C Lapiletepte	add: migrate: command its test jobs	list month
Behaviour (1996)         Applicationspring (1996)         Applicationspring (1996)           Behaviour (1996)         Behaviour (1996)         Behaviour (1996)         Behaviour (1996)	C hatodol/voresTable.php	add port suitedials	5 months age
Operationstation         Instrumentation         Instrumentation           Operationstation         Instrumentation         Instrumentation           Operationstation         Instrumentation         Instrumentation           Operationstation         Instrumentation         Instrumentation           Destingend         Instrumentation         Instrumentation	C tasonadateyry	The st	1 months ago
Bysequences         Appropriate         Provide State           Deschamithatige         Appropriate         Provide State           Deschamithatige         Appropriate         Appropriate	C celezanope-malezon tub	this property handle requirements	1 months ago
Bestinger         an instruction togy         Instruction           Destinger         an instruction         Construction           Destinger         Construction         Construction           Destinger         Construction         Construction         Construction           Destinger         Construction         Construction         Construction         Construction	C dejectemplatetenerozziole.php	news migrate object templates	a monthe ago
Andreaming of processional control of the sector of t	C thjeztengiaestabicphp	fic particip job values	2 months ago
Bendragen         registration on registration         Second Seco	C Organizations liable php	add more tests, fie bogs	5 months ago
Bestgeningebookser         Normage-shafter         Personagebookser           Bestgeningebookser         Normage-shafter         Personagebookser           Bestgeningebookser         Normage-shafter         Personagebookser           Bestgeningebookser         Personagebookser         Personagebookser	C RotesTablephp	new (3.4) initial skeleten added	18 months age
Despekpelpensentenspel     Sinseparation	C SevenSalephp	ship reflector to use singletion	Lest manife
Comparison for the second	C the regime ploy like play	his surge cardials.	1 months ago
Oppropheneury         org/paper/paper         Excelsion           Oppropheneury         org/paper/paper         Excelsion           Oppropheneury         org/paper/paper         Excelsion           Oppropheneury         etc/paper         Excelsion           Oppropheneury         etc/paper         Excelsion	C the region plane with the plan	the marge contract.	2 months age
Impolenting Makepte         Org Spoplecting/metal-added         Emotive spo           Interstanding type         odd (WII) por of Serutional Instance deduce departments         Lectrometal	C staningerouprating page	fic are reestricity) instead of constructor	3 90083 800
C General Sector and S	g signologitembleuhp	drug pightingthij models added	E monthe age
	1 TagloRectorNepTable.php	drig (tagcalections) model added	E monthe age
🗅 Namingkit Dates Table at p	C3 UserStaticphy	add; [###] port of SerdEmail tool and related docker adjustments	let meth
	3 Naminglation in Calify	new (naminglot entry) migration. But reaches, they #8888	Emonths age

# > CODEBASE MIGRATION: WHERE WE STAND II



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

	P 28 branches (	5 350 tags	Go to file	Add file *	O Code •
This branch is a	333 commits ahea	d, 914 commits be	ehind 2.4.	n	Contribute +

Even while supporting and improving 2.4

# LOOK AND FEEL

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



🖪 Organisations inde						Search MISP	۹ 🐥
Contact Organisation							
Organisation Ir	dexi						
vationalities o		Sectors 🕈 No dota					
Previous Next							
+ Addorganisation AL # Name	Local orgs External orgs Country: Luxe	mbourg	Members	URL Nationality	Sector	value to search	Search 🔻 🕱
1 ORGNAME	7e9251c8-3b15-417a	9#07-#500479r5h4d	2	Luxembourg	253.04	ADMIN	@ @ I
2 CERT-FR_1510	56bdf779-46f8-4353		8	France			
Page 1 of 1 showing 2 orga	nisations out of 2 total, starting on reco	ed 1 andios on 2					
Previous Next							

brganisation View	Organisation View       Image: Control of Contro	Organisation View         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0	Organisal		ONGINAME											_	ISP	۹
Image: control of the control of t	Image: control of the control of t	Image: control of the control of t	Delete															@ View
Image: Province of the control of the contr	teme         concluse           v         70/50156 Model Transact Substrational Substratin Substrational Substrate Substrational Substrate Substr	teme         concluse           v         70/50156 Model Transact Substrational Substratin Substrational Substrate Substrational Substrate Substr	rganisat	tion View														
000 \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	Valitation 10:4 472 4482 24824792344           Valitation 10:4 472 4482 2482792344           Valitation 10:4 472 4482 248279244           Valitation 10:4 472 4482 248279244           Valitation 10:4 472 4482 248279244           Valitation 10:4 472 4482 24827944           Valitation 10:4 472 4482 24827944           Valitation 10:4 472 4482 4482 4482           Valitation 10:4 472 4482 4482           Valitation 10:4 472	Valitation 10:4 472 4482 24824792344           Valitation 10:4 472 4482 2482792344           Valitation 10:4 472 4482 248279244           Valitation 10:4 472 4482 248279244           Valitation 10:4 472 4482 248279244           Valitation 10:4 472 4482 24827944           Valitation 10:4 472 4482 24827944           Valitation 10:4 472 4482 4482 4482           Valitation 10:4 472 4482 4482           Valitation 10:4 472			1													
N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N         N	Restant/         Catenology         Catenolog	Restant/         Catenology         Catenolog																
Nationality (all classes)         Na	National Description of the Carding on the	National Description of the Carding on the			7e9251	Ic8-3b15-417a-9e92-a508479c5	64d											
Interface         Interface <t< td=""><td>Instrumentation of the second of th</td><td>Instrumentation of the second of th</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	Instrumentation of the second of th	Instrumentation of the second of th																
Image: Control of the contro	Varianti Statisti         Addemini Statisti         Society         Soc	Varianti Statisti         Addemini Statisti         Society         Soc			Lucemi	bourg												
All	Control         Control <t< td=""><td>Control         Control         <t< td=""><td></td><td></td><td>ADMIN</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<></td></t<>	Control         Control <t< td=""><td></td><td></td><td>ADMIN</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>			ADMIN													
Versional ender 1 Previous Root Root Balan Bal	User index <sup>1</sup> Preitor Index   Preitor Index	User index <sup>1</sup> Preitor Index   Preitor Index			10111													
Versional ender 1 Previous Root Root Balan Bal	User index <sup>1</sup> Preitor Index   Preitor Index	User index <sup>1</sup> Preitor Index   Preitor Index																
Next         Entropy         All Action         All Action         All Action         Entropy	Previous         Next         Ender         Mark         Ender         Ender         Mark         Ender         Mark         Mark </td <td>Previous         Next         Entitie         B         De         A         A         SOB         A         Lest Login         Created         X         Devide         M           0         0         0         0         A         A         500         A         Lest Login         Created         X         Devide         M           1         0         0         A         X         400000         X         2022-0510         X         X         0           2         0         0         0         X         X         X         400000         X         2022-051710         X         X         0           Page 161         3.00161         X         X         X         3.00161         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X</td> <td>Users</td> <td></td>	Previous         Next         Entitie         B         De         A         A         SOB         A         Lest Login         Created         X         Devide         M           0         0         0         0         A         A         500         A         Lest Login         Created         X         Devide         M           1         0         0         A         X         400000         X         2022-0510         X         X         0           2         0         0         0         X         X         X         400000         X         2022-051710         X         X         0           Page 161         3.00161         X         X         X         3.00161         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X         X	Users															
Next         Entropy         All Action         All Action         All Action         Entropy	Previous         Next         Ender         Mark         Ender         Ender         Mark         Ender         Mark         Mark </td <td>Previous         Next         Ender         Mark         Ender         Ender         Mark         Ender         Mark         Mark<!--</td--><td>Lleastad</td><td>lev i</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td>	Previous         Next         Ender         Mark         Ender         Ender         Mark         Ender         Mark         Mark </td <td>Lleastad</td> <td>lev i</td> <td></td>	Lleastad	lev i														
Control         Control         Send         Send         Send         Send         Send         Send         Send         Send         Model         Mod	Alterne         Alterne         Alterne         Alterne         Alterne         Enternalistic transmit         Sende         Y           1         10         Org         Brit         Sende         A         500         A         Lext.tealm         Created         Image: Sender Sender         A         A           1         10         Org         Brit         Sender         X         X         A         400000         X         2021-0540713514         Image: Sender Sender         A         A           2         Obstable         Sender Sender         X         X         X         332164         V         Image: Sender Sender         Image: Sender Sender Sender Sender Sender Sender         Image: Sender Sen	Alterne         Alterne         Alterne         Alterne         Alterne         Enternalistic transmit         Sendo V           1         10         Org         Brite         Sendo         A         500         A         Lext.team         Created         Image: Sendo V         A         M           1         10         Org         Brite         Sendo V         X         X         A         400000         X         2021-0540713514         Image: Sendo V         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A         A	oser ind	lex.														
Control         Control         Send         Send         Send         Send         Send         Send         Send         Send         Model         Mod	Attem         Max         Distance         Marce         Max         Distance         Marce         <	Attem         Max         Distance         Marce         Max         Distance         Marce         <	Previous	Next														
0         10         6m         East         98         0         2         500         2         Lettleph         Created         ✓         X         X         Mail           1         1         000000000000000000000000000000000000	D         D0         D0         D0         D0         P         D0         P         D0         P         D0         D0         D0<	D         D0         D0         D0         D0         P         D0         P         D0         P         D0         D0         D0<																
1         CR62005         adminipaleministrat         X         X         X         4000000         X         2022/04/01/01/01         X         X           2         2         CR620055         Services         sprc/abelinistrat         X         X         X         3807661         V         0         2022/01/17/01/9480         V         C           Nage 1 of 1, showing 2 uses as of 2 facts, starting on record 1, ending on 2          X         X         X         3807661         V         0         2022/01/17/01/9480         V         C	1       1       Seconds       admini developministes       X       X       X       400000       X       201243-001011544       X       X       I         2       2       Seconds       Seconds       specifiedministes       X       X       X       3307841       V       0       2002401-171011940       V       V       R         Raps 1 of 1, showing 2 cares and of 2 tabul, stating on record 1, ending an 2       V       X       X       3307841       V       0       2002401-171011940       V       V       0	1         0522MMS         selmin         edmin@4dmin.text         X         X         4000000         X         2022.01-01.0175.11         X         X         X           2         2         0522MMS         Sent user         gengl@4min.text         X         X         3307861         ✓         0         2022.01-01.0175.11         ✓         0         2022.01-01.0175.11         ✓         0         2022.01-01.0175.11         ✓         0         2022.01-01.0175.11         ✓         0         2022.01-01.0175.11         ✓         0         2022.01-01.0175.11         ✓         0         2022.01-01.0175.11         ✓         0         2022.01-01.0175.11         ✓         0         2022.01-01.0175.11         ✓         0         2022.01-01.0175.11         ✓         0         2022.01-01.0175.11         ✓         0         2022.01-01.0175.11         ✓         0         2022.01-01.0175.11         ✓         Ø         Ø         Ø </td <td></td> <td>Enter valu</td> <td>e to searc</td> <td>1 5</td> <td>arch 🔻</td>													Enter valu	e to searc	1 5	arch 🔻
2         California         Sections         specified         X         X         3567861         ©         202245-171819-40          ©         Ø           Page 1 of 1, showing 2 uses out of 2 table, tasking on record 1, ending on 2          X         X         3567861         ©         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø         Ø <td< td=""><td>2         2. 2002/04/2         Sinclustry:         Ny mpdgedminitest:         X         X         3387/861         -         0         2002/05/17/857840         -         ID           Page 1 of 1, dowing 2 conv.out of 2 blad, stating on mound 4, wedragen 2         -         -         -         ID</td><td>□ 2 <u>06/20455</u> <u>50/2007</u> sprc@edmin.text X X X 3347161 ✓ 0 202243-1715/15460 □ ✓ 0 Page 1 of 1, 30-anleg 2 users out of 2 total, starting on record 1, ending on 2</td><td>+ Add User</td><td>All Active Dis</td><td>abled 🚦 Roles -</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>	2         2. 2002/04/2         Sinclustry:         Ny mpdgedminitest:         X         X         3387/861         -         0         2002/05/17/857840         -         ID           Page 1 of 1, dowing 2 conv.out of 2 blad, stating on mound 4, wedragen 2         -         -         -         ID	□ 2 <u>06/20455</u> <u>50/2007</u> sprc@edmin.text X X X 3347161 ✓ 0 202243-1715/15460 □ ✓ 0 Page 1 of 1, 30-anleg 2 users out of 2 total, starting on record 1, ending on 2	+ Add User	All Active Dis	abled 🚦 Roles -													
Page 1 of 1, showing 2 users out of 2 totals, starting on neorod 1, anding on 2	Page 1 of 1, showing 2 users out of 2 total, starting on record 1, ending on 2	Page 1 of 1, dissing 2 users out of 2 total, starting on record 1, ending on 2				Email			2	۵	SID	2	Last Login	Created			Disabled	Ac
Page 1 of 1, showing 2 users out of 2 totals, starting on neorod 1, anding on 2	Page 1 of 1, showing 2 users out of 2 total, starting on record 1, ending on 2	Page 1 of 1, dissing 2 users out of 2 total, starting on record 1, ending on 2	0 10	Org	Role			٩						Created		×		Ac
			□ <u>I</u> □ 1 □ 2	Org Organame Organame	Role admin Sync.user	admin@admin.test sync@admin.test	×	9	×	×	4000000	×	2023-03-08 07:15:14			* *		
			ID     1     2     Page 1 of 1, sh	Org ORGNAME ORGNAME howing 2 users out	Role admin Sync.user	admin@admin.test sync@admin.test	×	۰	×	×	4000000	×	2023-03-08 07:15:14			* *		A
			ID     1     2     Page 1 of 1, sh	Org ORGNAME ORGNAME howing 2 users out	Role admin Sync.user	admin@admin.test sync@admin.test	×	•	×	×	4000000	×	2023-03-08 07:15:14			* *		Ac
			ID     1     2     Page 1 of 1, sh	Org ORGNAME ORGNAME howing 2 users out	Role admin Sync.user	admin@admin.test sync@admin.test	×	•	×	×	4000000	×	2023-03-08 07:15:14			* *		Ac
			ID     1     2     Page 1 of 1, sh	Org ORGNAME ORGNAME howing 2 users out	Role admin Sync.user	admin@admin.test sync@admin.test	×	0	×	×	4000000	×	2023-03-08 07:15:14			* *		Ac
			ID     1     2     Page 1 of 1, sh	Org ORGNAME ORGNAME howing 2 users out	Role admin Sync.user	admin@admin.test sync@admin.test	×	•	×	×	4000000	×	2023-03-08 07:15:14			* *		Ac
			ID     1     2     Page 1 of 1, sh	Org ORGNAME ORGNAME howing 2 users out	Role admin Sync.user	admin@admin.test sync@admin.test	×	•	×	×	4000000	×	2023-03-08 07:15:14			* *		Ac
			ID     1     2     Page 1 of 1, sh	Org ORGNAME ORGNAME howing 2 users out	Role admin Sync.user	admin@admin.test sync@admin.test	×	•	×	×	4000000	×	2023-03-08 07:15:14			* *		Ac
			ID     1     2     Page 1 of 1, sh	Org ORGNAME ORGNAME howing 2 users out	Role admin Sync.user	admin@admin.test sync@admin.test	×	9	×	×	4000000	×	2023-03-08 07:15:14			* *		Ac
			ID     1     2     Page 1 of 1, sh	Org ORGNAME ORGNAME howing 2 users out	Role admin Sync.user	admin@admin.test sync@admin.test	×	9	×	×	4000000	×	2023-03-08 07:15:14			* *		Ac
			ID     1     2     Page 1 of 1, sh	Org ORGNAME ORGNAME howing 2 users out	Role admin Sync.user	admin@admin.test sync@admin.test	×	<b>Q</b>	×	×	4000000	×	2023-03-08 07:15:14			* *		Ac
			ID     1     2     Page 1 of 1, sh	Org ORGNAME ORGNAME howing 2 users out	Role admin Sync.user	admin@admin.test sync@admin.test	×	•	×	×	4000000	×	2023-03-08 07:15:14			* *		Ac
			ID     1     2     Page 1 of 1, sh	Org ORGNAME ORGNAME howing 2 users out	Role admin Sync.user	admin@admin.test sync@admin.test	×	0	×	×	4000000	×	2023-03-08 07:15:14			* *		Ac
			ID     1     2     Page 1 of 1, sh	Org ORGNAME ORGNAME howing 2 users out	Role admin Sync.user	admin@admin.test sync@admin.test	×		×	×	4000000	×	2023-03-08 07:15:14			* *		Ac
			ID     1     2     Page 1 of 1, sh	Org ORGNAME ORGNAME howing 2 users out	Role admin Sync.user	admin@admin.test sync@admin.test	×		×	×	4000000	×	2023-03-08 07:15:14			* *		Ac
			ID     1     2     Page 1 of 1, sh	Org ORGNAME ORGNAME howing 2 users out	Role admin Sync.user	admin@admin.test sync@admin.test	×	0	×	×	4000000	×	2023-03-08 07:15:14			* *		
			ID     1     2     Page 1 of 1, sh	Org ORGNAME ORGNAME howing 2 users out	Role admin Sync.user	admin@admin.test sync@admin.test	×	•	×	×	4000000	×	2023-03-08 07:15:14			* *		Ac
			ID     1     2     Page 1 of 1, sh	Org ORGNAME ORGNAME howing 2 users out	Role admin Sync.user	admin@admin.test sync@admin.test	×	•	×	×	4000000	×	2023-03-08 07:15:14			* *		

MISP	🖶 Users Index 🔸 admin@admin.te	st	Search MISP Q 🔺 🖨
	1 Delete		
0	User admin@admin.test		
Ľ	ID	1	
	Email	admin@admin.test	
	Organisation	ORCNAME	
	Role	admin	
	Email notifications	Exet publicled notification S Dely notification S Weekly notification S Monthy notification S	
	Contact alert enabled		
8	NIDS Start SID	400000	
8	Terms accepted	<b>0</b>	
1	Must change password		
	PGP key	NA	
	S/MIME Public certificate		
8	Disabled		
ф			
*	Authentication keys		
50	Events		
◎ ★ B ◎ @ O ♡ O O O O O O O O O O O O O O O O O			
*			E

	📟 SharingGroups 🛙	ndex 🔸 Test edil	G	Search MISP	۹ 🜲 ۹
_	+ Create SharingGroups				⊖ View 🕑 Edit
٥	New Sharing C	Group			
	General Organisati	ions Instances	Summary & Save		
8	Local Organisations		Select a local organisation		~
8	Remote Organisations		Select a remote organisation		~
•	Type	Name	FR		
	local	ORGNAME	CERT-FR_1510		
○●◎目☆ ◎ ≫ ※ - ~ ~ ~ ~ ~					
3					\$

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



	-	Maurana I ummumman		👷 🖉 Marcolan S. antiquentar	The state of the s
			When they is many the second		the first between building
	•	Users a dealer Chadrade as at			
	•	Oser adminigradminicesc			
				a fault designed and	
	•	Taxada Incidente		typetate Dictor	
		Enalmethodow East additional and a second and a second additional and a second additional addit		Conjustice on Co	
		Net-refuter		- Independenting	
	٠	Hotershalm		• United the matched	
				B BANKER STORE	
		NUMBER OF CONTRACTOR OF CONTRA		E transfer E	
	1	Pad / ang served		A state part of the state p	
		Networks and the second s		<u>i</u>	
	Π.			Ŧ	
	*			• anti-anti-anti-	
	1.2				
				*	
	1.5				
				•	
	2			2	
	12			2	
	Π.				
	1.00			13	
				±	
Image: space of space	× 1			2	
Image: space of space					
Image: space of space					
Image: space of space					
Image: space of space					
Image: space of space					_
Image: marked biology of the state of th					
Image: marked biology of the state of th					
Image: Section of the section of t		Microsoft F. administration	Gardineth, R & O	u∰ (unvision ) anticipational	Augusta 🔹 🔹 🖉
<pre></pre>					tarrente. 🔬 🛎 🔍
					tarrente. 🔬 🛎 🔍
	:	Uper admin/2 admin text			tarrente. 🔬 🛎 🔍
	1	Uper admin/2 admin text			tarrente. 🔬 🛎 🔍
Note:     Note:     Note:     Note:       Note:     Note:     Note:     Note:       Note:     Note:     Note:       Note:     Note:     Note:       Note:     Note:     Note:       Note:     Note:     Note:       Note:     Note:     Note:       Note:     Note:     Note:	0 1 0	Uper admin/2 admin text		User schningbadminstert	tarrente. 🔬 🛎 🔍
Note:     Note:     Note:     Note:       Note:     Note:     Note:     Note:       Note:     Note:     Note:       Note:     Note:     Note:       Note:     Note:     Note:       Note:     Note:     Note:       Note:     Note:     Note:       Note:     Note:     Note:	0120	User administration		User administrativest	tarrente. 🔬 🛎 🔍
		User administration		Core administrativest	tarrente. 🔬 🛎 🔍
	8 0100	User administration		Core administrativest	tarrente. 🔬 🛎 🔍
	0000			Cover administrativity:     Cover administrativity:     Cover administrativity:     Cover administrative     Cover a	tarrente. 🔬 🛎 🔍
	- 81 0 1 0 0			Cover administrativity:     Cover administrativity:     Cover administrativity:     Cover administrative     Cover a	tarrente. 🔬 🛎 🔍
				Cover administrativity:     Cover administrativity:     Cover administrativity:     Cover administrative     Cover a	tarrente. 🔬 🛎 🔍
	1001 Ba 0100			Ver winddokhitott	tarrente. 🔬 🛎 🔍
				Eventselaadsaktaatt     Eventselaadsaktaatt     Eventselaadsaktaatt     Eventselaadsaktaatt     Eventselaadsaktaattaattaattaattaattaattaattaattaatt	tarrente. 🔬 🛎 🔍
	e vane Sa onso	Regarding data to the second s		Eventselaadsaktaatt     Eventselaadsaktaatt     Eventselaadsaktaatt     Eventselaadsaktaatt     Eventselaadsaktaattaattaattaattaattaattaattaattaatt	tarrente. 🔬 🛎 🔍
	Pe van 8a 0100	Regarding data to the second s		Eventselaadsaktaatt     Eventselaadsaktaatt     Eventselaadsaktaatt     Eventselaadsaktaatt     Eventselaadsaktaattaattaattaattaattaattaattaattaatt	tarrente. 🔬 🛎 🔍
	1498 X004 88 8100	Regarding data to the second s		Eventselaadsaktaatt     Eventselaadsaktaatt     Eventselaadsaktaatt     Eventselaadsaktaatt     Eventselaadsaktaattaattaattaattaattaattaattaattaatt	tarrente. 🔬 🛎 🔍
	4498 NOR4 88 8780	Region general set of the set of		A Constraint of the second sec	tarrente. 🔬 🛎 🔍
	- 449.8 X02.4 ER BABD	Region general set of the set of		Variabilitària de la construcción de la constr	tarrente. 🔬 🛎 🔍
	20 4468 X084 88 8180	Region general set of the set of		Varianteenteenteenteenteenteenteenteenteente	tarrente. 🔬 🛎 🔍
	125 1458 X084 BB 0100	Region general set of the set of		Varianteenteenteenteenteenteenteenteenteente	tarrente. 🔬 🛎 🔍
	125 445# X084 BH B120	Region general set of the set of		All and a second s	tarrente. 🔬 🛎 🔍
	6 110 1400 VODA BN 0100	Region general set of the set of		All and a second s	tarrente. 🔬 🛎 🔍
	0010 KB 4005 #455 475 50.	Region general set of the set of		All and a second s	tarrente. 🔬 🛎 🔍
	1200 110 4468 1004 88 8180 8	Region general set of the set of		All and a second s	tarrente. 🔬 🛎 🔍
	***** 125 4*** ×*** 8* 8*80	Region general set of the set of		All and a second s	tarrente. 🔬 🛎 🔍
	008200 115 4458 X084 88 8180	Region general set of the set of		All and a second s	tarrente. 🔬 🛎 🔍
	Buubted in debe vone Ba brau	Region general set of the set of		All and a second s	tarrente. 🔬 🛎 🔍
	sbusstad inb dete van Bu bran	Region general set of the set of		All and a second s	tarrente. 🔬 🛎 🔍
	studefas ire dete vane Ba bran	Region general set of the set of			tarrente. 🔬 🛎 🔍
	1 10000000 100 1400 1400 000 000 000 000	Region general set of the set of			tarrente. 🔬 🛎 🔍
	-10 sbostad (25 dete van 2n 2020	Regarding and the second secon			tarrente. 🔬 🛎 🔍
	vest shoostad typ depe vane Bu Snao	Regarding and the second secon			tarrente. 🔬 🛎 🔍
	vest sbuseres ive depe vone Ba Bran	Regarding and the second secon			tarrente. 🔬 🛎 🔍
-	vezo elecerative del delle vale la bran	Regarding and the second secon			tarrente. 🔬 🛎 🔍
	vest shoostad top deve vane Ba anan	Regarding and the second secon			tarrente. 🔬 🛎 🔍
	anne an sans the detail and the set	Regarding and the second secon			tarrente. 🔬 🛎 🔍
	vest shorefor the deter and Sa and	Regarding and the second secon			tarrente. 🔬 🛎 🔍

# **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						
			In automatically prevaler appearance for interaction details in spatiane. To reader appearance prevalence for a prevalentiation for a strategiest reaction encode the action from and addition types are named, core appearance, and hash the prevalent for IRDESDAL values of the articles. Explore for more attribute types a planeted.	e applicative fo	r opulare presid	lar, carrendy we arity	oppot/NDS opposize
	Simply click or	ary of the billow	ing buttors to download the appropriate data.				
	Tope .	Last Update	Description	Outsided	Filmin	Program	Actions
	3504	144	Only this to disarritual all overity and altributes that pus have access to in MIDP 2000 format. Altachments are enabled on this instance.	100	144	NA	Described Dr
	XM.	505	City Bits to Elevisional ad events and addicates that you have access to in MEP IM, format Allachimetis are evalued on this relation.	104	104	NMA.	Download De
-	C87,59	101	City this to diversion an attributes that are indicates and that you have access to (except the attachments) in City format.	78	505	NA.	Download Ge
9	C94,44	104	Orice this to download all attributes that you have access to jurcept lie attractments) in CSV format.	700	506	NRA.	Deuriced Ge
	Seriota	144.	Dick this to developed all retreacts unlessed attributes that you have access to under the Sarcosa rule format. Only published events and attributes marked as IOS Signature are ampriled. Administration to able to maintain a advandat containing host, domain name and Procedures to exclude hom the NOS export.	<b>**</b>	101	NA.	Deariesd Co
	Seat	NK.	Dick this to download all retrack valued attributes that you have access to under the Seret rule format, Only published avents and attributes marked as IDS Signature are experted. Administration is able to maintain a advandar containing heat, domain name and IP numbers to exclude from the NEOS export.	<b>**</b>	144	NeA.	Courses Co
	010	NR.	Dick this to deviced all retrieves valued attributes that you have access to under the Bio-six format. Only published revents and attributes marked as DS Signature are experted. Administration is able to market in advandat containing hast, domain name and IP numbers to include that the HOS expert.		100	NeA.	Courses Ge
	5%X	104	Click this to download a STUX document containing the STUX version of all-events and attributes that you have access to. Attachments are enabled on this instance.	768	506	NRA.	Coursions Ge
	5702	NR.	On the to developed a \$7102 decement containing the \$702 vestion of all events and attributes that you have access to. Attachments are analysed on this instance.	700	NR.	NRA	Described Ge
	neg	NR.	Disk this to dominant an IDV2 (one like generated from all is unaly units interance, domain administers. This can be useful for DISS level forwalling: Delypublished events and administers and administers. This can be useful for DISS level forwalling. Delypublished events and administers and administers.	100	No.	NeA.	Download G
	тра	NR.	Dick on one of the bottom below to download all the attributes with the maching space. This hat can be used to found towards software when searching for subprises likes. Delypoinheld events and attributes maked as ICS Signature are required. Attochments are employed on the instance.	<b>1</b>	100	NA	Generalie
	Yara	NH.	Click this to described frama ndex perventised from all relevant attributes.	<b>30</b>	506	NA	Download Co
	Yana	New.	Dick this to download' functions prevaied from all relevant altitudes. Roles are returned in a 2004 format with internation altered regim (generated or parsen) and validly.	**	144	NA	Desrived De
			ana 201 Marangani Marangani, Marangani 1923, 2023, 2024, Marana Amali Amali Amala Amala (Marang Marangani Marangani Amala Amala (Marangani Marangani Mar				
	mine-you	ionay cart-ru	tor 2000 when the process and the process of the second second second second second second second second second	chine tapp	org tapa com	of target-status	
	bark appare	in darin	ten in nunder gein glowe mander break alter Geraky-sume sampligs if makeurige or Administratio shall under Inghad Administratio shall been and and and and and and and and and an	shalled sha	400 44410034	shat13556 www	0.224 sha0.236 wa
	1003552	In onen I	heanquitestan heanquitat heanquitat heanquitat heanquitat heanquitat heanquitat heanquitat heanquitat	throng the	111156 Berarie	Ind-224 Norone	0Ab226 Terumph
	filmani(sha	MIZ Norm	(b) whiles shelded led whites series and white series diging are white right and and in right and place of the rig		wallon date w50	Ingeprissial of	SIS Improvint met
	x000 https://	01-01-070 OT	narmat larenges cause later per priper proper between manager maater manager ended and data	angy 6	materialed an	ut-metoaday	anat timat rack
	enalmessa	geld giften	emene gehub-separates gehub-separates jatos is setto is den generate feat same matte same fut same fut same fut same fut same fut same fut same	nt-number   p	coport-country	cerent expirator	abesirunter hale
	stanurber	sar-dard	te-ena prinary-materiae sculty-or-materiae special-servate-request terupent tyre-sculter. Sour-assistic paperet artists place-port-or-organi-enclositation place-port-or-materiae p	la epitatu	wad tongs and	utor possegere	ane excito locator eur
			application-di concentration-de concel accomptinget				

#### 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	
٥	Add Object + Pablish - Cases Spear-phishing atte	mpt targeting telco	sector			Ø View	🧭 Edit 🧐 View History 🔥 Explore
2	critical notice like delegation reque	sts, tag conflicts,					×
	Event ID	46	Threat Level	2			
8	UUID	c516b000-740b-4e3b-8bb5-2f4562b1167e	Analysis	1			
	Creator org	ORGNAME	Tags		echniquess"email speafing" phishing distributions" spe	earghidding" phishing states" active" phishing pro	chological acceptability-"medium"
9	Owner org	ORGNAME		estimative language. Wallhood probab			
_	Contributors		Galaxies		mbourg" [ misp-gelexycountry="luxenboarg" ] misp-g		with melicious ettachments - T1367"
•	Creator user	admin@admin.test		misp-galexymitre-attack-pattern="5p	earphishing Attachment - T1566.001"   misp-galaxy.mitr	erelleckrpettern-"Phishing - T1564"	
8	Protected Event		Extends				
8	Date	2023-02-07	Extended by	46			
1	Distribution	1	Related Events	6 related hits			
	Published	No	Feed Hits	1.feed hits			
Ð			Server Hits Warninglist Hits	0 server hits 1 warninglist hits			
\$ \$ \$ \$	27 Oct 29 Oct 31 Oct 62 New	O PROPOSALS 2 SEGNITIVE O EXTENSIONS O DELETED 1 FEED HTS 1 WARNING 6 RELATIONSHIPS 175556 KOC	Distribution	6 Attributes	Recent sightings           1         2         1           2         3         3           27 Οα         28 Οα         31 Θα	Relevant correlations go here - Events with some contaxt overlap - Events created by other orgs	
높 B	notice for empty event,						×
°0	💩 Objects 🚺	🕄 Attributes 🛐	🖥 Reports 🔫	😭 Event Graph	AgA Event Timeline	ATT&OK®	💁 Discussion 🧿
∰ © ு ∰ ∰ ♣ ≁	ağıets						
>>							5

# **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



- 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 $\rightarrow$ 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 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



#### Model migration timeline

	2023 H1		
Preparation phase	✓ Users	✓ Settings	Inbox
Refactoring	<ul> <li>Organisations</li> </ul>	✓ Warninglists	Correlation values
Extraction to Libraries	✓ Roles	✓ Noticelists & Allowlists	Taxonomy
	<ul> <li>Authkeys</li> </ul>	<ul> <li>Sharing groups</li> </ul>	User Settings
	<ul> <li>Cryptographic keys</li> </ul>	<ul> <li>Object Templates</li> </ul>	Tags
		<ul> <li>SightingDB</li> </ul>	AuditLogs
		✓ Event blocklists	Jobs
		Object relationships	Cerebrate
		Galaxy	Dashboard
*	*	Galaxy Clusters	

#### 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?
  - <sup>₽</sup> 3.x → 3-x branch MISP/MISP/tree/3.x
  - Project for migration github.com/orgs/MISP/projects/2