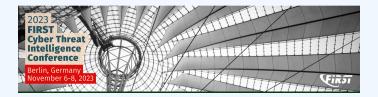
MISP 3 - Teaching an Old Dog New Tricks Paving the way forward

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 AN OUTDATED VERSION OF THE FRAMEWORK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

				Global Actions	Sync Actions		
	Event			News My Profile My Settings Set Setting			
				Organisations Role Permission	15		
			_	List Object Temp	plates	-	
				List Sharing Gro Add Sharing Gro	oup		
				List Sharing Gro Add Sharing Gro			
-		£		Decaying Model List Decaying M			
	0.4	-	-	User Guide			
		1		Categories & Ty Terms & Conditi			
	0.4	6		Statistics List Discussions			
	0.4			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

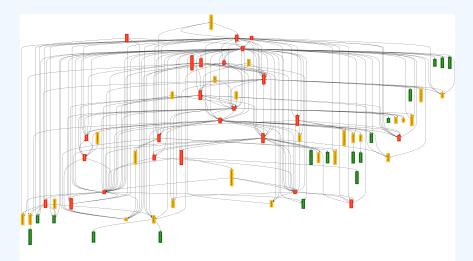


Setting the stage with Cerebrate

- 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 This item hasn't been started This is actively being worked on MISP #8881 • MISP #8882 TagCollectionTag Sightingdb • MISP #8885 Inbox • MISP #8886 ObjectRelationship • MISP #8887 NotificationLog MISP #8890 GalaxyClusterBlocklist

• MISP #8891

EventBlocklist

EventLock

O Done 8 This has been completed ۲ • MISP #8879 AdminSettings ۲ • MISP #8880 WarninglistEntry • MISP #8883 SharingGroups • MISP #8884 ObjectTemplates Noticelists ۲ MISP #8889 AllowedList CryptographicKey Authkeys

Ø

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

-o- Commits 3	33 主 Files changed 2,467	🗓 5 contributors
-o- Commits on	Jan 31, 2023	
] initial skeleton added … ka committed on Jan 31	Verified C 35932db ()

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

Name	Last conmit message	Cost commit da
No.		
Edited Antiparties	This depresables nations	7 months age
C .gooog	news (study initial elements-added	18 months age
q4q.eiterzenintee []	next progration Administratings model mesed	18 months ago
C) eliseolization php	drig reneme table for canalitency	6 months ago
C Applialisation	fic maps confirm	3 months ago
C Audit.opTable.php	new [1.4] initial skeleter-added	18 months age
C Automyclasicycle	add apt and tests	á montra aga
C Cypeographic Cepting and	In or controlly	3 months age
C neetBookazakazakere	Sc ii	5 months age
C trentstable.php	add basic coul api tests for sharing groups	5 months ago
🗅 tritanosfabik.php	add, add basic user texts, remove combrate texts, part code from car	7 months ago
[] pitvlikticptp	dag selecter to use singleton	let month
C usplatiophp	add migrate command its test jobs	let meeth
C hatocistroneslatie.php	add port restories	5 months age
C tastoria/tastyry	he st	3 months age
C CEpezzaelow-strapizzone ange	This property handle requirements	a northe age
C céjectempérentementation php	new: migrate-object templates.	a months ago
C Objectionplatectable.php	fic parting job values	a monthe age
C Organizational lable php	add more texts. fie buge	5 months ago
C RotsTablephp	now (3.) initial skeleton added	18 months age
C Sevenializingto	dag reflecter te use singleten	let month
C Dangtrophychileyty	his swept coefficie.	3 minibaaga
C thangcropterwritikeupp	The margar cardiate.	3 months age
C sharingoroupctativ.php	fic are restrictly initial af contractor	3 weeks ago
🗇 sightingdomoleuhp	the sighting the models added	a months ago
C TagloRetterTagrTable.php	the Jogcoliscient) model added	8 months ago
C UsesTablephp	add (WP) port of SendEmail tool and related dodien adjustments	let month
3 NaminghatheriesTable.php	non (suminglot only) migration. But reading, free #1888	8 months 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



MISP	Crganisations index							Search MISP	۹ 🔶 פ
۵	Contact Departmention Organisation Index ⁱ								
	Nationalities 0	Sectors 0	No data						
;	Previous Next								
	+ Add organisation All Local orgs E	xternal orgs Country: Luxembourg		Members	URL	Nationality	Sector	Enter value to search	Search 🔻 🗮 - Actions
8	I ORGNAME	7e9251c8-3b15-417a-9e92-a508479c5b4d		Members 2	<u>ORL</u>	Luxembourg	sector	ADMIN	Actions
8	2 CERT-FR_1510	56bdf779-46f8-4353-bdf9-2bb95bce2212		2		France		PROPERTY	
1		of 2 total, starting on record 1, ending on 2		-					
Đ	Previous Next	or 2 total, starting on record 1, ending on 2							
ф	Previous Next								
× .									
8									
3									
121									
8									
••									
e 0									
Э									
۵									
¢									
\$									
88									
4									
*									
39									S

Organisation View 0 ADDILATE	Organisation View organisation View 0	Organisation View	Horganis	actions index 2	ORGNAME											Junon	15P	۹
0 1 Second 2 Adden 1/2 Second 2/2 Secon	0 1 0	0 1 0	Delete															Ø View
0 1 Note 000000000000000000000000000000000000	0 1 000000000000000000000000000000000000	0 1 000000000000000000000000000000000000	Organisa	ation View														
come 7 #031310 2015 4175 4002 20050F7525840 Water Manage Status 20050F7525840 Water Manage Status 20050F7525840 Water Manage Status 20050F7525840 Water Manage Status 20050F7525840 Colspan="4">Colspan="4"Colspan="4">Colspan="4"Colspan="4">Colspan="4"Colspan="4">Colspan="4"Colspan="4"Colspan="4">Colspan="4"Colspa	come 7 #12110 3016 4176 4692 3056475.0540 4 We work work work work work work work work	come 7 #12110 3016 4176 4692 3056475.0540 4 We work work work work work work work work																
originality Lawritory Lawritory <thlawritory< th=""> <thlawritory< th=""></thlawritory<></thlawritory<>	One Lawellow Lawellow </td <td>One Lawellow Lawellow <!--</td--><td></td><td></td><td>ORCA</td><td>LAME</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>	One Lawellow Lawellow </td <td></td> <td></td> <td>ORCA</td> <td>LAME</td> <td></td>			ORCA	LAME												
teambory teambory team At Ann type Attant team Attant te	National Control 1	National Control 1	JUID		76925	51c8-3b15-417a-9e92-a508479c5	b4d											
Statute ADMM Tetra ADMM Central:	Status Status<	Status Status<																
Index Addem Control Description	Total Addamini Construint	Total Addamini Construint			Luxer	nbourg												
Contract Contract Contract User	Contract Contract Contract User	Contract Contract Contract User																
User User Index ¹ Index ¹	User User Index ¹ Index ¹	User User Index ¹ Index ¹			ADMI	N												
User Index ¹ Pretron Ref. Pretron All Active Stander D Refer. It Construction and Active Stander D Refer.	User Index ¹ Pretron Ref. Pretron All Active Stander D Refer. It Construction and Active Stander D Refer.	User Index ¹ Pretron Ref. Pretron All Active Stander D Refer. It Construction and Active Stander D Refer.	oncects															
Previous Institution All Acone Description Entert Entert Entert Entert Entert Control of the second Control of the second o	Previous Institution All Acone Description Entert Entert Entert Entert Entert Control of the second Control of the second o	Previous Institution All Acone Description Entert Entert Entert Entert Entert Control of the second Control of the second o	Users															
Previous Next Ender <	Previous Next Ender <	Previous Next Ender <	Licor inc	dovi														
Attem Attem <th< td=""><td>Attem Attem <th< td=""><td>Attem Attem <th< td=""><td>User int</td><td>uex</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></th<></td></th<></td></th<>	Attem Attem <th< td=""><td>Attem Attem <th< td=""><td>User int</td><td>uex</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></th<></td></th<>	Attem Attem <th< td=""><td>User int</td><td>uex</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></th<>	User int	uex														
Little All Acone Deside Final See 0 A A SE0 A LotaLize Created X X Deside M 0 0 99 Bitel Enail 99 0 A A 500 A LotaLize Created V X Deside M M M C 1 Concentry X Deside M M C 1 Concentry X Deside M M C X C C X C C X C C X C C X C C X C C X C C X C C X C C X C C X C X C X C X C X C X C X C X C X C X C X C	Little All Acone Deside Final See 0 A A SE0 A LotaLize Created X X Deside M 0 0 99 Bitel Enail 99 0 A A 500 A LotaLize Created V X Deside M M M C 1 Concentry X Deside M M C 1 Concentry X Deside M M C X C C X C C X C C X C C X C C X C C X C C X C C X C C X C C X C X C X C X C X C X C X C X C X C X C X C	Little All Acone Deside Final See 0 A A SE0 A LotaLize Created X X Deside M 0 0 99 Bitel Enail 99 0 A A 500 A LotaLize Created V X Deside M M M C 1 Concentry X Deside M M C 1 Concentry X Deside M M C X C C X C C X C C X C C X C C X C C X C C X C C X C C X C C X C X C X C X C X C X C X C X C X C X C X C	Previous	Next														
ID Drag Pail Examile Her Sea A Sea	ID Drag Pail Examile Her Sea A Sea	ID Drag Pail Examile Her Sea A Sea																
1 0522MMS selmin edmini@edmini.text X X 4000000 X 2022-01-01 (21):14 X X 2 2 0522MMS Sets core spro@dmini.text X X 3607841 ✓ 0 2022-01-17 (51):940 ✓ Ø Page 1 of 1, dowing 2 coars out of 2 table, starting on nexce 5, ending on 2	1 0622MHX sdmin edmin@vedmin.text X X 4000000 X 2023-01-01 071514 X X 2 2 0620MHX Sector spen@vemin.text X X 3307641 ✓ 0 2022-01-17 151940 ✓ ✓ Ø Page 10 ⁴ 1, dewing 2 cares out of 2 table, kateling on neces 4, inding on 2	1 0622MHX sdmin edmin@vedmin.text X X 4000000 X 2023-01-01 071514 X X 2 2 0620MHX Sector spen@vemin.text X X 3307641 ✓ 0 2022-01-17 151940 ✓ ✓ Ø Page 10 ⁴ 1, dewing 2 cares out of 2 table, kateling on neces 4, inding on 2	+ Add User	All Active D	isabled 🚦 Roles •										Enter val	ue to seard	h S	sarch 🔻
□ 2 <u>04CMMM</u> Spreamer syndlyddminthet X X X 3307841 ✓ 0 202243-1711c11540 □ ✓ 0 Page 1 of 1, dowleg 2 caan out of 2 blob, Kathig on nearet 1, mding on 2	□ 2 <u>ORCHANE</u> Secure syndpolinit.tes X X X 3367611 ✓ 0 202243-1715:1540 □ ✓ 0 Rage 1 of 1, boxing 2 users out of 2 table, duating on record 1, inding on 2	□ 2 <u>ORCHANE</u> Secure syndpolinit.tes X X X 3367611 ✓ 0 202243-1715:1540 □ ✓ 0 Rage 1 of 1, boxing 2 users out of 2 table, duating on record 1, inding on 2					-				CID		t and t and a	Created	-	~	Disabled	Ac
Page 1 of 1, showing 2 users out of 2 total, starting on record 1, ending on 2	Page 1 of 1, showing 2 users out of 2 total, starting on record 1, ending on 2	Page 1 of 1, showing 2 users out of 2 total, starting on record 1, ending on 2	D 10	Org	Role	Email							LOSS LOSSI					
Page 1 of 1, showing 2 users out of 2 total, starting on record 1, ending on 2	Page 1 of 1, showing 2 users out of 2 total, starting on record 1, ending on 2	Page 1 of 1, showing 2 users out of 2 total, starting on record 1, ending on 2																
			1 2 Page 1 of 1,1	ORGNAME ORGNAME showing 2 users ou	admin Svinc user	admin@admin.test sync@admin.test	×	-	×	×	4000000	×	2023-03-08 07:15:14			×		
			1 2 Page 1 of 1,1	ORGNAME ORGNAME showing 2 users ou	admin Svinc user	admin@admin.test sync@admin.test	×		×	×	4000000	×	2023-03-08 07:15:14			×		
			1 2 Page 1 of 1,1	ORGNAME ORGNAME showing 2 users ou	admin Svinc user	admin@admin.test sync@admin.test	×		×	×	4000000	×	2023-03-08 07:15:14			×		
			1 2 Page 1 of 1,1	ORGNAME ORGNAME showing 2 users ou	admin Svinc user	admin@admin.test sync@admin.test	×		×	×	4000000	×	2023-03-08 07:15:14			×		
			1 2 Page 1 of 1,1	ORGNAME ORGNAME showing 2 users ou	admin Svinc user	admin@admin.test sync@admin.test	×		×	×	4000000	×	2023-03-08 07:15:14			×		
			1 2 Page 1 of 1,1	ORGNAME ORGNAME showing 2 users ou	admin Svinc user	admin@admin.test sync@admin.test	×		×	×	4000000	×	2023-03-08 07:15:14			×		
			1 2 Page 1 of 1,1	ORGNAME ORGNAME showing 2 users ou	admin Svinc user	admin@admin.test sync@admin.test	×		×	×	4000000	×	2023-03-08 07:15:14			×		
			1 2 Page 1 of 1,1	ORGNAME ORGNAME showing 2 users ou	admin Svinc user	admin@admin.test sync@admin.test	×		×	×	4000000	×	2023-03-08 07:15:14			×		
			1 2 Page 1 of 1,1	ORGNAME ORGNAME showing 2 users ou	admin Svinc user	admin@admin.test sync@admin.test	×		×	×	4000000	×	2023-03-08 07:15:14			×		
			1 2 Page 1 of 1,1	ORGNAME ORGNAME showing 2 users ou	admin Svinc user	admin@admin.test sync@admin.test	×		×	×	4000000	×	2023-03-08 07:15:14			×		
			1 2 Page 1 of 1,1	ORGNAME ORGNAME showing 2 users ou	admin Svinc user	admin@admin.test sync@admin.test	×		×	×	4000000	×	2023-03-08 07:15:14			×		
			1 2 Page 1 of 1,1	ORGNAME ORGNAME showing 2 users ou	admin Svinc user	admin@admin.test sync@admin.test	×		×	×	4000000	×	2023-03-08 07:15:14			×		
			1 2 Page 1 of 1,1	ORGNAME ORGNAME showing 2 users ou	admin Svinc user	admin@admin.test sync@admin.test	×		×	×	4000000	×	2023-03-08 07:15:14			×		
			1 2 Page 1 of 1,1	ORGNAME ORGNAME showing 2 users ou	admin Svinc user	admin@admin.test sync@admin.test	×		×	×	4000000	×	2023-03-08 07:15:14			×		
			1 2 Page 1 of 1,1	ORGNAME ORGNAME showing 2 users ou	admin Svinc user	admin@admin.test sync@admin.test	×		×	×	4000000	×	2023-03-08 07:15:14			×		
			1 2 Page 1 of 1,1	ORGNAME ORGNAME showing 2 users ou	admin Svinc user	admin@admin.test sync@admin.test	×		×	×	4000000	×	2023-03-08 07:15:14			×		

MISP	볼 Users index 🔸 adming/admin.te	st		Search MISP	Q 🗍 🤂
	Telete		Ø View	😢 Edit 🏻 🍰 Account settings	20 User Setting [1]
0	User admin@admin.test				
2	ID	1			
2	Email	admin@admin.test			
8	Organisation	ORGNAME			
	Role	admin			
	Email notifications	Event publicade notification University and University and			
	Contact alert enabled	83			
8	NIDS Start SID	400000			
8	Terms accepted	83			
1	Must change password				
•	PGP key	N(A			
	S/MIME Public certificate				
B	Disabled	80			
ф		—			
*	Authentication keys				
	Events				
ري ال					
불					
*0					
ě.					
0					
5					
0					
¢					
$\langle \rangle$					
88					
4					
2					
»					S

MISP	SharingGroups index	> Financial gr	oup				Search MISP		۹ 🐥 و
۵	+ Create SharingGroups								⊖ View & Edit
8	New Sharing Gro	up							
≝	General Organisations	Instances	Summary & Save						
	Local Organisations		Select a local organisation	n					~
	Remote Organisations		Select a remote organisa	ation					~
	Туре	Name		UUID		Extend		Actions	
	local	ORGNAME		7e9251c8-3b15-417a-9e92-a508479c5b4d			~		
8	remote	CERT-FR_1510		56bdf779-46f8-4353-bdf9-2bb95bce2212					
1	Next page								
6									
4									
•									
4									
-									
28									
iĝi S									
1621									
분									
е ••									
è									
õ									
5									
ŏ									
e									
$\langle \rangle$									
-									
*									
»									

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



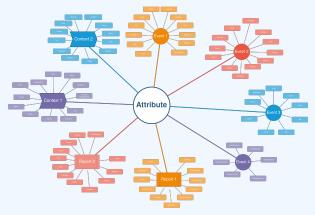
	Wearan I amena	we design of the second s	No. 0	-B	¥10000 X 400040044		100000, R & O
			where where is many real is recorded.		Part I		the part & control & montes
•	User admin@ad v v v v v v v v v v v v v	win toot					
164	oper auminigati	minicest		a 05			
				÷		and the second	
	Typester			- 24	-	acoust	
	Indextudent	for a function of the second s				Construitation of Kalance Data walkanian antigen akalanian Sanata ya Sanata	
		Wadpick Value 🗧				metratular o	
•		Herlanshalan			test dari andrikel		
H	and back	-		1 E	Low BR	and a second	
					n anglat Anglangana		
						0	
					ACCOUNTS OF A		
*				¥ .			
1.2							
10							
1.2				2			
19				•			
18				0			
18				0			
**** *********							
1.30				49			
				-			
				÷.			
				*			
-							
-	🖢 🗑 Carrolis V. amagan			н В	********		arrente
				н В			Anna anna 💽 🛎 O
-	-		Gardenili, 9 a O	н В			And a gran grant grant and grant and grant grant grant grant grant grant grant grant grant and grant g
-	user adminikadmin te			н В			Anna anna 💽 🛎 O
-	user adminikadmin te			н В			Anna anna 💽 🛎 O
	user adminikadmin te			- 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1	er admin@admin.test		Anna anna 💽 🛎 O
0.00	user adminikadmin te			111 1 1 1 1 1 1 1 1 1 1 1 1	er admin@admin.test	s Annotation Marka	Anna anna 💽 🛎 O
	user adminikadmin te				er admin@admin.test	s Annotation Marka	Anna anna 💽 🛎 O
8= 8788	-			111 1 1 1 1 1 1 1 1 1 1 1 1	ser admin@admin.test	• enterna ente	Anna anna 💽 🛎 O
8 0×20	User solmingkodmin.te User solmingkodmin.te San San San San			108.1881 108.1881 108.1881	ser admin@admin.test	• enterna ente	Anna anna 💽 🛎 O
. 8. 01.00 S	User solmingkodmin.te User solmingkodmin.te San San San San			108.1881 108.1881 108.1881	ser admin@admin.test	• enterna ente	Anna anna 💽 🛎 O
an 8 aran 8	User solmingkodmin.te User solmingkodmin.te San San San San			108.1881 108.1881 108.1881	ser admin@admin.test	• enterna ente	Anna anna 💽 🛎 O
vans Ba bran 🖁	User solmingkodmin.te User solmingkodmin.te San San San San			100018-1001	ser admin@admin.test	• enterna ente	Anna anna 💽 🛎 O
· vas 8x stat	Uper administration for for for mainteen mainteen mainteen Maintee				ser admin@admin.test	• enterna ente	Anna anna 💽 🛎 O
84 8750	Uper administration for for for mainteen mainteen mainteen Maintee				ser admin@admin.test	• enterna ente	Anna anna 💽 🛎 O
<pre>41. VODA BH BTED BH </pre>	User solmingkodmin.te User solmingkodmin.te San San San San				eer admini@admin.test a manane	s Annotation Marka	Anna anna 💽 🛎 O
dete vane Bi bran	Verración de la companya de la compa				ser admin@admin.test	• enterna ente	Anna anna 💽 🛎 O
debe kone Be bran 🚦	Uper administration for for for mainteen mainteen mainteen Maintee			449€ ×000€ 85 860 <mark>8</mark> 5582562 [522562 [5226 2	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O
1 1458 1004 88 8180 8	Verración de la companya de la compa			449€ ×000€ 85 860 <mark>8</mark> 5582562 [522562 [5226 2	eer admini@admin.test a manane	• enterna ente	Anna anna 💽 🛎 O
ve dete vane Ba bran	User administration was a second and a second and a second a seco			29-1449€ ×000+ 85 850 86 2532552 [532]	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O
tre dete vare Ba anan 🔒	Verración de la companya de la compa			449€ ×000€ 85 860 <mark>8</mark> 5582562 [522562 [5226 2	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O
125 depe tane Be bran	User administration was a second and a second and a second a seco			+ * * 4 + * * * * * * * * * * * * * * * * * *	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O
is tro dependente de ondo 🔒	User administration was a second and a second and a second a seco			+ * * 4 + * * * * * * * * * * * * * * * * * *	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O
rat tup daha kana Ba anan 🔒	User administration was a second and a second and a second a seco			+ * * 4 + * * * * * * * * * * * * * * * * * *	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O
8/06 175 1458 1000 Ba Brac 🔒	User administration was a second and a second and a second a seco			+ * * 4 + * * * * * * * * * * * * * * * * * *	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O
sefat tob debe vane Be anno 🚦	User administration was a second and a second and a second a seco			+ * * 4 + * * * * * * * * * * * * * * * * * *	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O
osedas tub debe vane Ba anao 🔒	User administration was a second and a second and a second a seco			+ * * 4 + * * * * * * * * * * * * * * * * * *	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O
Buoktas irb debe vane Be Bran 🤱	User administration was a second and a second and a second a seco			+ * * 4 + * * * * * * * * * * * * * * * * * *	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O
sbussies irs date tans Ba anan 🚦	User administration was a second and a second and a second a seco			29-1449€ ×000+ 85 850 86 2532552 [532]	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O
· abustat ive dete vase Ba Bran 8	User administration was a second and a second and a second a seco			🙀 3128 48 482 447 447 447 354 407 40	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O
15 sbostad (75 dete vans 82 state 🚦	User administration was a second and a second and a second a seco			🙀 3128 48 482 447 447 447 354 407 40	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O
ati abootat iyo dabe yana Ba buan 🚦	User administration was a second and a second and a second a seco			🙀 3128 48 482 447 447 447 354 407 40	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O
1910 1001206 120 1400 1400 80 80 80 80 8	User administration was a second and a second and a second a seco			+ * * 4 + * * * * * * * * * * * * * * * * * *	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O
vest abusedat dvb debe vane Bu snap 🚦	User administration was a second and a second and a second a seco			🙀 3128 48 482 447 447 447 354 407 40	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O
vest abusedant dvb dvbe vane Ba anau 🚦	User administration was a second and a second and a second a seco			🙀 3128 48 482 447 447 447 354 407 40	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O
vest abuseras tre deter vane Bu bran 🚦	User administration was a second and a second and a second a seco			🙀 3128 48 482 447 447 447 354 407 40	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O
vest søvsedas tve dete vase Sa state 🚦	User administration was a second and a second and a second a seco			🙀 3128 48 482 447 447 447 354 407 40	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O
vest abutedas jub debe vane Be Brate 🚦	User administration was a second and a second and a second a seco			🙀 3128 48 482 447 447 447 354 407 40	er administradmin test annen menten	• enterna ente	Anna anna 💽 🛎 O

STEP III - THE TODOS

> Redefine how we interact with data I

Indicator centric perspective

- 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 addrabidity provide signalants for information spatients. To enable signature prevaluto for a pieve addision, Topolate field of the addision exact the sector tree, Note that soil ad addision types are names, your agents etc., and leads to prevalents for 1000/5042, values of the addision. Expension for more advisoring types is planned.	e applicative fo	r alinans lisina	lar, carrently we only	upper ND1 upper v
	Simply click o	ary of the billow	ing buttors to download the appropriate data.				
	204	Last Update	Description	Outsided	Filesier	Program	Actions
	3504	144	Clock this to described all overtis and abrilation that pro-baser access to in MEP 2020 format. All adverses are modeled on this instance.	100	144	NMA.	Doorstaal Dee
	XML	505	CitA fini to disertical all events and all bases for its faces access to its MIDP TML format. All addresses are evaded as finit restance.	W6	104	NPA.	Download Der
-	C34,59	505	Click this to developed all attributes that are indicates and that you have access to (except the attachments) in Clie format.	766	506	186	Download Gen
	694,A4	NH.	Ock this to download all ambutes that you have access to prompt like attachments) in CSV format.	30	506.	NA	Deuricad Car
	Soricata	Nex.	Dick this to download all network valued attributes that you have access to under the Sanoda rule format. Only published ownes and attributes marked as DS Signature are appreted. Administration is able to maintain a alloweditz containing host, domain name and IP numbers to excise how the HOS export.	30 C	100	NeA.	Described Cer
	Seat.	NR.	Dick this to develop all retreats related attributes that you have access to under the Sever use terms. Only published events and attributes marked as IDS Signature are experted. Administration is able to maintain a attributes containing host, domain name and IP numbers to exclude from the NEOS export.		No.	NA	Download Ger
	0 e	104	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	NA.	Download Ger
	5%X	506	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.	Download Gen
	5702	N9.	Dick this to download a \$T312 document containing the \$T312 version of all events and attributes that you have access to. Attachments are availed at this instance.	30	505	NA	Deuricad Ce
	neg	Nex.	Disk this to developed an ISV2 Save like generated from all proceduce, hereixane, domain advitutes. This can be useful iter DVS level inervaling. Oxypatibleset events and advitutes marked as DS Signature are expensed.	100	144	NeA.	Desrived Ce
	TEAT	104	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.	1	100	NA	Generale
	Yana	NR.	Click this to described frama ndex perventised from all relevant attributes.	100	NPR.	NRA.	Dewniced Cen
	Yana	Non.	Dick this to download frame new prevaled from all indexant altributes. Bules are returned in a 2024 terms with information almost edge (prevaled or parsen), and salidly	100	No.	NeA.	Desrived G
	per la per	el Trabarren contry card-to ter also rit		gy private tary chine target athatite the	sah tagaquasi org tagan kocati att2 sinatt22223	yana attad yadam 19 (19 yat estatutut 19 attad 13 (19 atta	signa gene had
	figname(she		(01) whites scheduled and a scheduled and a schedule scheduled and a scheduled schedu	_			
			non-mark phon-septe Guardie Salettier part product proceed functionager incontained producted datasyonant inter-order pare-strate incontained phon- ement geno-september period segmenter parts and the generative segment to the second backness functions generated period period				when one of the
			terna privy mateux sunty chroates apoint wave repeti Tepel by sunter Surradial paymitatati plan port cispat estatatio plan port cispat estatatio				are ward to do not
	_	_	aggicator-iti ovena-cannianid conex bosiani acovaniani				

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
- Sneak peak ? 🙂

SNEAK PEAK OF THE NEW EVENT VIEW - WIP

MISP	🖨 Events index 🔸 [id]					Search MISP	ે ૧ ૧
۵	& Add Object	empt targeting telco				View	🖉 Edit 🧐 Viewhistory 🗰 Explore
8			sector				
	critical notice like delegation req	uests, tag conflicts,					×
	Event ID	46	Threat Level	2			
8	UUID	c516b000-740b-4e3b-8bb5-2f4562b1167e	Analysis	1			
-	Creator org	ORGNAME	Tags		chriquess "email speafing" phishing distributions" sp	earghiching" phishing states "active" phishing pry	chological-acceptability+"medium"
_	Owner org	ORGNAME		estimative-language/likelihood-probability			
	Contributors		Galaxies	misp-galaxytarget-information="Laxer	nbourg" [misp-galaxy.country="kusambourg" [misp-g arphibling Attachment - T1566.001" [misp-galaxy.mitr	gelaxymikre-ettack-pattern-"Spear phishing messages	with malicious attachments - T1367*
	Creator user	admin@admin.test	Extends	with the state and a state and a state	adversed surfaces () () () () () () () () () (e attorpational money 11504	
8	Protected Event		Extended by	46			
8	Date	2023-02-07	Related Events	40 6 related hits			
	Distribution	1	Feed Hits				
	Published	No		1 feed hits			
Ð			Server Hits Warninglist Hits	0 server hits			
di la			warningascriics	1 warninglist hits			
8 8 8	27 Oct 29 Oct 31 Oct 62 Nov	1 PEED HITS 1 WARRING 6 RELATIONSHIPS 17 SYN KOC		6 3	2 27 Οστ 28 Οστ 31.Οστ	•	×
분 8 00 48	& Objects	😪 Attributes 🔢	🖥 Reports 🥵	🐨 Event Graph	As ^a Event Timeline	ATT&OX [®]	Ciscussion
00000000000000000000000000000000000000							
»							5

CONSIDERATIONS

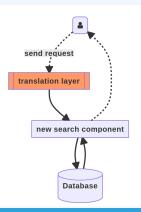
> MISP CORE FORMAT



- 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	 Organisations 	✓ Warninglists	Correlation values
Extraction to Libraries	✓ Roles	✓ Noticelists & Allowlists	: Taxonomy
	✓ Authkeys	 Sharing groups 	User Settings
	 Cryptographic keys 	✓ Object Templates	Tags
		 SightingDB 	AuditLogs
		✓ Event blocklists	Jobs
		Object relationships	Cerebrate
		Galaxy	Dashboard
*	*	Galaxy Clusters	

> 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 → 3-x branch MISP/MISP/tree/3.x
 - Project for migration github.com/orgs/MISP/projects/2