Cerebrate

Community management and tool orchestration the open-source way

Andras Iklody & Sami Mokaddem

Cerebrate Project

FIRSTCON22

CEREBRATE PROJECT

#FIRSTCON22 SPEAKER

DUBLIN IRELAND 2022

34th ANNUAL FIRST CONFERENCE

JUNE 26 – JULY 1

Who are we ?

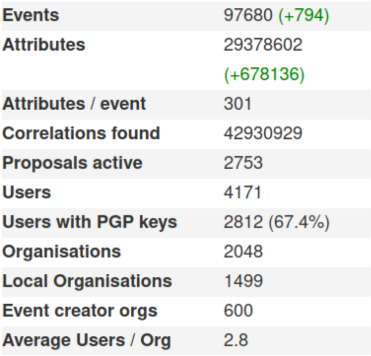
circl.lu
Computer Incident
Response Center
LUXEMBOURG

- The Computer Incident Response Center Luxembourg (CIRCL)
- CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg
- CIRCL leads the development of the open-source MISP threat intelligence platform
  - As well as running multiple large MISP communities performain active daily threat-intelligence sharing

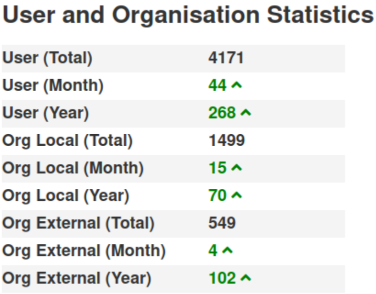
MeliCERTes II: a quick recap of the morning session

- MeliCERTes
- Common tooling for CSIRTs
- Cerebrate a central component of the new tooling
- Takes care of:
  - Contact management
  - orchestration
  - Sharing group distribution and management

Some stats about one of our MISP instance: MISPPriv (1)



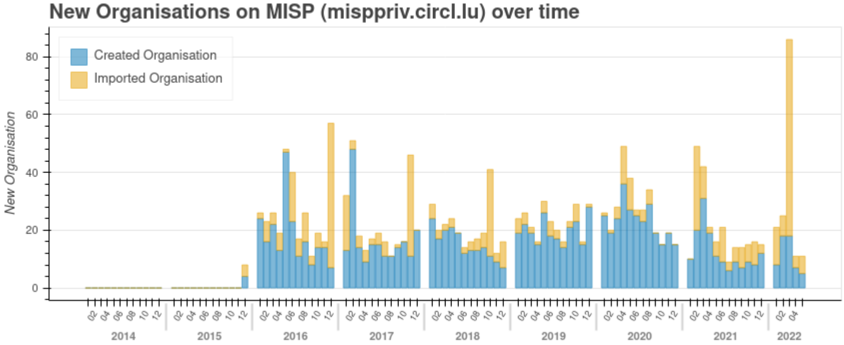
Events	97680 (+794)
Attributes	29378602 (+678136)
Attributes / event	301
Correlations found	42930929
Proposals active	2753
Users	4171
Users with PGP keys	2812 (67.4%)
Organisations	2048
Local Organisations	1499
Event creator orgs	600
Average Users / Org	2.8



User and Organisation Statistics

User (Total)	4171
User (Month)	44 ^
User (Year)	268 ^
Org Local (Total)	1499
Org Local (Month)	15 ^
Org Local (Year)	70 ^
Org External (Total)	549
Org External (Month)	4 ^
Org External (Year)	102 ^

Some stats about one of our MISP instance: MISPPriv (2)



Issues we're trying to solve

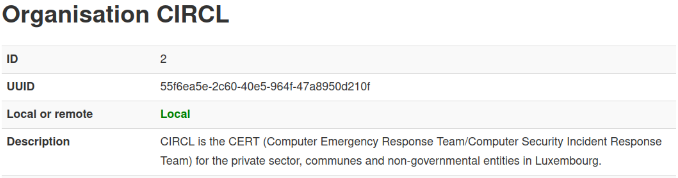
Rising number of communities is great!

- **Bridge the gap** between between communities
- Sharing with peers that face **similar threats**
- **Reuse** of TTPs across sectors
- **Hybrid threats** How seemingly unrelated things may be interesting to correlate
- **Spread the love**, as our field is ahead of several other sectors when it comes to information sharing

Issues we're trying to solve

However, broader and more diverse communities lead to more issues

- Non-technical issues
  - Sharing difficulties in terms of social interactions (e.g trust)
    - #FIRSTCON22 greatly helps in that aspect!
  - Lots of points of contacts
- Technical issues
  - Centralised identity management
  - Data might change or evolve over time
  - Loads of UUIDs to manually process
  - Distribution list management is difficult across communities



Organisation CIRCL

ID	2
UUID	55f6ea5e-2c60-40e5-964f-47a8950d210f
Local or remote	**Local**
Description	CIRCL is the CERT (Computer Emergency Response Team/Computer Security Incident Response Team) for the private sector, communes and non-governmental entities in Luxembourg.

Issues we're trying to solve with Cerebrate

- Constituencies of organisations
  - Geographic & sectorial
  - But also technical: CIDR blocks & AS Numbers
- Cryptographic key lookup for information signing
  - MISP's protected event feature (New since MISP v2.4.156)

Issues we're trying to solve with Cerebrate

- Constituencies of organisations
  - Geographic & sectorial
  - But also technical: CIDR blocks & AS Numbers
- Cryptographic key lookup for information signing
  - MISP's protected event feature (New since MISP v2.4.156)

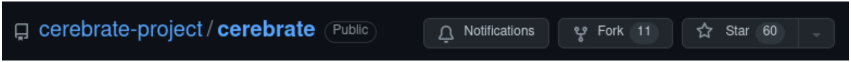
Issues we're trying to solve with Cerebrate

- Customisable data model adaptable to each community
    - Based on the sheer amount of different types of communities, **it's a must**
- Sharing group management
- Synchronisation and lookup system

Our attempt at solving them: Cerebrate

- Open source community management and orchestration tool

CEREBRATE PROJECT



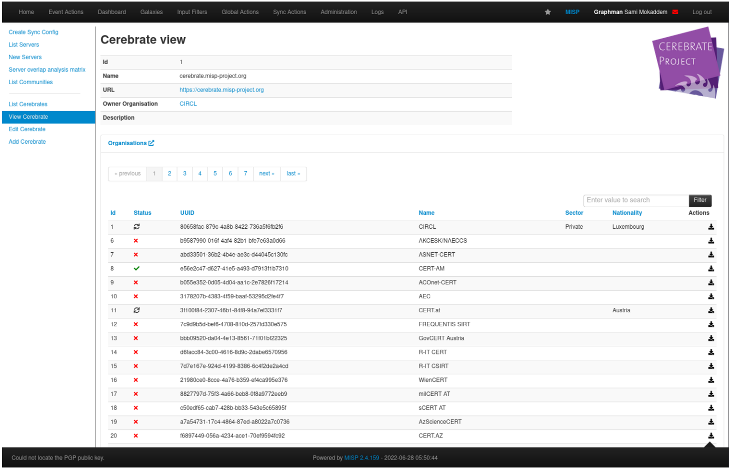
- Central tool for the **Melicertes 2 project** (Co-funded by the EU as a CEF project - SMART 2018/1024)
- Rich **Contact Database**
- Tightly coupled management system and companion for MISP (and other tools)
  - Get in touch with us if you need help building integrations!
- Planned as the primary MISP **fleet management** tool

Goals and design

- Goals: Simplicity, lightweight and open-source
- Technologies used: PHP, cakephp4, BS5, ...
    - (almost) the same as in MISP for easier **maintainability** and **code re-use**
- IAM centric design
    - Tightly integrated with Keycloak
- Core functionalities: Auditing, API
    - Any changes should be easily accessible to counter errors or foul plays
    - From our perspective, automation and integration is essential and should be as easy as possible

GOALS AND DESIGN

- Built with tool integration in mind, acting as a contact database



Cerebrate view

Id	1
Name	cerebrate.misp-project.org
URL	https://cerebrate.misp-project.org
Owner Organisation	CIRCL
Description	

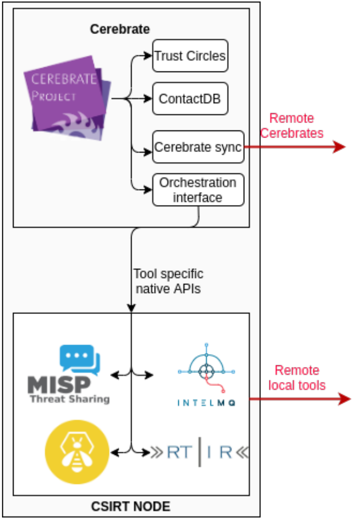
Id	Status	UUID	Name	Sector	Nationality	Actions
1	↻	80658fac-879c-4a8b-8422-736a5f6fb2f6	CIRCL	Private	Luxembourg	⤓
6	✗	b9587990-016f-4af4-82b1-bfe7e63a0d66	AKCESK/NAECCS			⤓
7	✗	abd33501-36b2-4b4e-ae3c-d44045c130fc	ASNET-CERT			⤓
8	✓	e56e2c47-d627-41e5-a493-d7913f1b7310	CERT-AM			⤓
9	✗	b055e352-0d05-4d04-aa1c-2e7826f17214	ACOnet-CERT			⤓
10	✗	3178207b-4383-4f59-baaf-53295d2fe4f7	AEC			⤓
11	↻	3f100f84-2307-46b1-84f8-94a7ef3331f7	CERT.at		Austria	⤓
12	✗	7c9d9b5d-bef6-4708-810d-257fd330e575	FREQUENTIS SIRT			⤓
13	✗	bbb09520-da04-4e13-8561-71f01bf22325	GovCERT Austria			⤓
14	✗	d6facc84-3c00-4616-8d9c-2dabe6570956	R-IT CERT			⤓
15	✗	7d7e167e-924d-4199-8386-6c4f2de2a4cd	R-IT CSIRT			⤓
16	✗	21980ce0-8cce-4a76-b359-ef4ca995e376	WienCERT			⤓
17	✗	8827797d-75f3-4a66-beb8-0f8a9772eeb9	milCERT AT			⤓
18	✗	c50edf65-cab7-428b-bb33-543e5c65895f	sCERT AT			⤓
19	✗	a7a54731-17c4-4864-87ed-a8022a7c0736	AzScienceCERT			⤓
20	✗	f6897449-056a-4234-ace1-70ef9594fc92	CERT.AZ			⤓

Could not locate the PGP public key.

Powered by MISP 2.4.159 - 2022-06-28 05:50:44

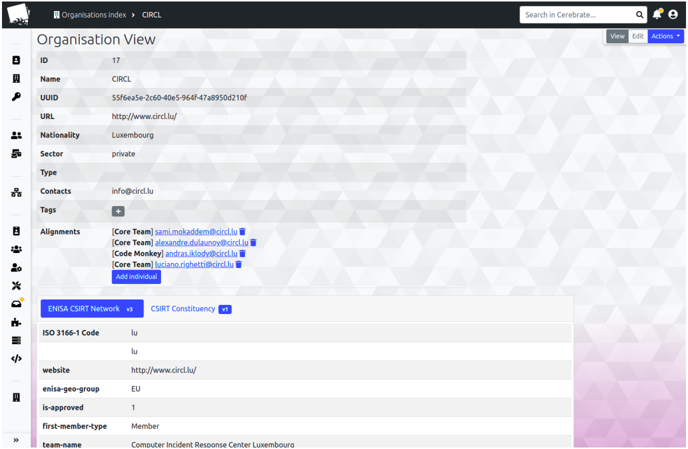
MISP is able to look up Organisations & Sharing Group in Cerebrate

Cerebrate's place in a typical CSIRT software stack



Cerebrate's contact database

- Contact database for the CSIRT network
  - Common contact fields such as `UUID`, `name`, `contact email address`, `nationality`, `URL`, ...

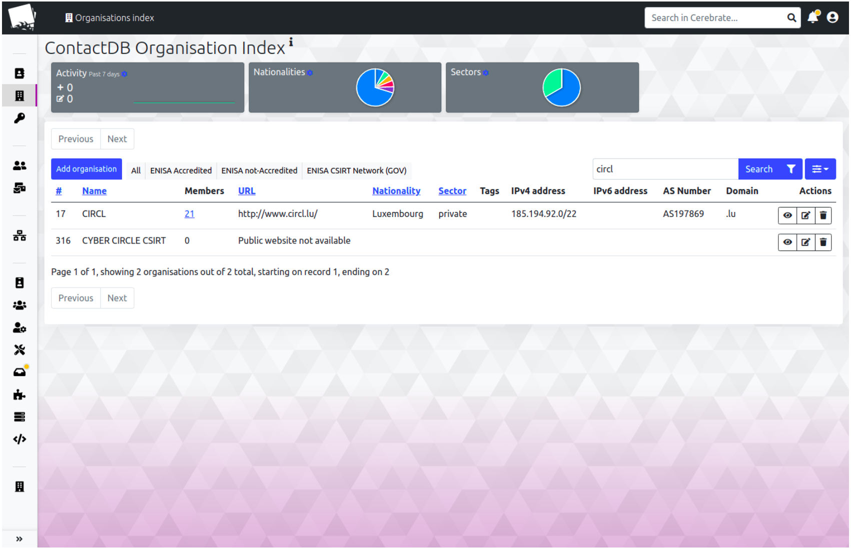


Organisation View

ID	17
Name	CIRCL
UUID	55f6ea5e-2c60-40e5-964f-47a8950d210f
URL	http://www.circl.lu/
Nationality	Luxembourg
Sector	private
Type	
Contacts	info@circl.lu
Tags	+
Alignments	**[Core Team]** sami.mokaddem@circl.lu **[Core Team]** alexandre.dulaunoy@circl.lu **[Code Monkey]** andras.iklody@circl.lu **[Core Team]** luciano.righetti@circl.lu Add individual

ISO 3166-1 Code	lu
	lu
website	http://www.circl.lu/
enisa-geo-group	EU
is-approved	1
first-member-type	Member
team-name	Computer Incident Response Center Luxembourg

Cerebrate's contact database



ContactDB Organisation Index

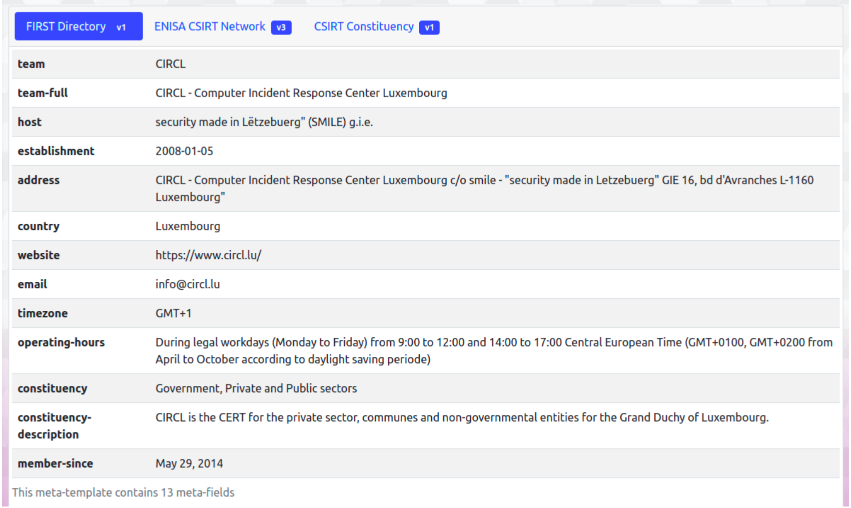
#	Name	Members	URL	Nationality	Sector	Tags	IPv4 address	IPv6 address	AS Number	Domain	Actions
17	CIRCL	21	http://www.circl.lu/	Luxembourg	private		185.194.92.0/22		AS197869	.lu	
316	CYBER CIRCLE CSIRT	0	Public website not available								

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

Cerebrate's contact database: Meta-fields

- Flexible system to store additional information: `meta-fields` (KV-store)
- These `meta-fields` are part of a larger structure called `meta-templates`
- Support of multiple templates used by various entities out there
    - **FIRST Directory**
    - ENISA CSIRT inventory
    - CSIRT Constituency (CIDR blocks, AS Numbers, ...)

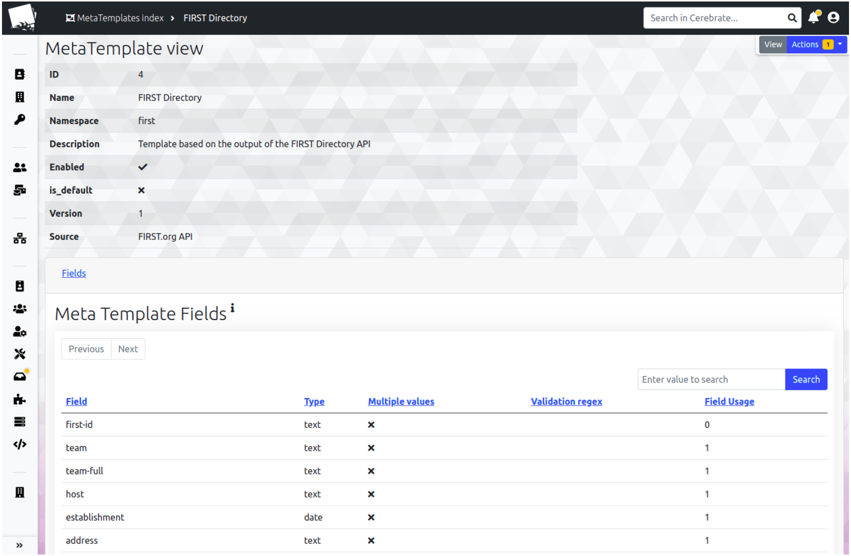
Cerebrate's contact database: Meta-fields



team	CIRCL
team-full	CIRCL - Computer Incident Response Center Luxembourg
host	security made in Lëtzebuerg" (SMILE) g.i.e.
establishment	2008-01-05
address	CIRCL - Computer Incident Response Center Luxembourg c/o smile - "security made in Letzebuerg" GIE 16, bd d'Avranches L-1160 Luxembourg"
country	Luxembourg
website	https://www.circl.lu/
email	info@circl.lu
timezone	GMT+1
operating-hours	During legal workdays (Monday to Friday) from 9:00 to 12:00 and 14:00 to 17:00 Central European Time (GMT+0100, GMT+0200 from April to October according to daylight saving periode)
constituency	Government, Private and Public sectors
constituency-description	CIRCL is the CERT for the private sector, communes and non-governmental entities for the Grand Duchy of Luxembourg.
member-since	May 29, 2014

This meta-template contains 13 meta-fields

Cerebrate's contact database: Meta-fields



MetaTemplate view

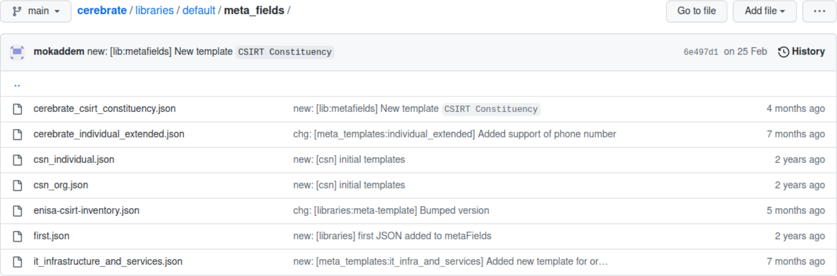
ID	4
Name	FIRST Directory
Namespace	first
Description	Template based on the output of the FIRST Directory API
Enabled	✓
is_default	✗
Version	1
Source	FIRST.org API

Fields

Meta Template Fields i

Field	Type	Multiple values	Validation regex	Field Usage
first-id	text	✗		0
team	text	✗		1
team-full	text	✗		1
host	text	✗		1
establishment	date	✗		1
address	text	✗		1

Cerebrate's contact database: Meta-fields



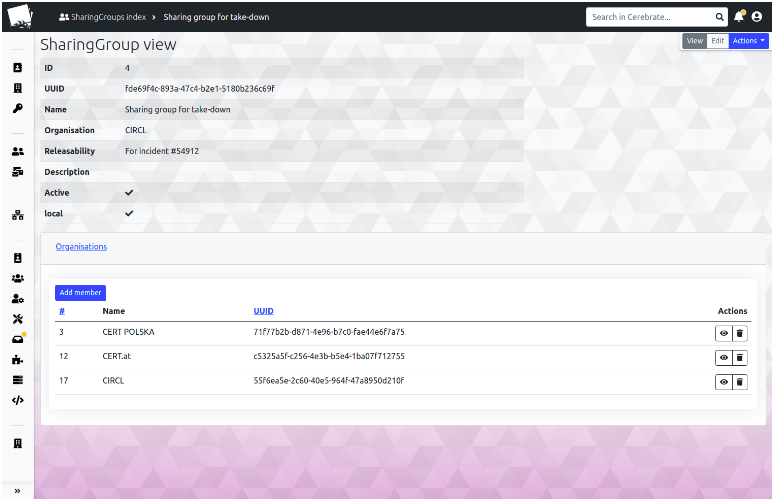
mokaddem new: [lib:metafields] New template `CSIRT Constituency` 6e497d1 on 25 Feb

cerebrate_csirt_constituency.json	new: [lib:metafields] New template `CSIRT Constituency`	4 months ago
cerebrate_individual_extended.json	chg: [meta_templates:individual_extended] Added support of phone number	7 months ago
csn_individual.json	new: [csn] initial templates	2 years ago
csn_org.json	new: [csn] initial templates	2 years ago
enisa-csirt-inventory.json	chg: [libraries:meta-template] Bumped version	5 months ago
first.json	new: [libraries] first JSON added to metaFields	2 years ago
it_infrastructure_and_services.json	new: [meta_templates:it_infra_and_services] Added new template for or…	7 months ago

Cerebrate's contact database: Sharing group management

- Easy way to **create** and **share** distribution lists
- Allow sharing groups to be **reusable**
- Circumvent limitations of traditional Threat Intelligence Sharing Platform
  - The exchange of sharing groups on creation / modification rather than on data exchange
  - Avoids the duplication of similar sharing groups

Cerebrate's contact database: Sharing group management



SharingGroup view

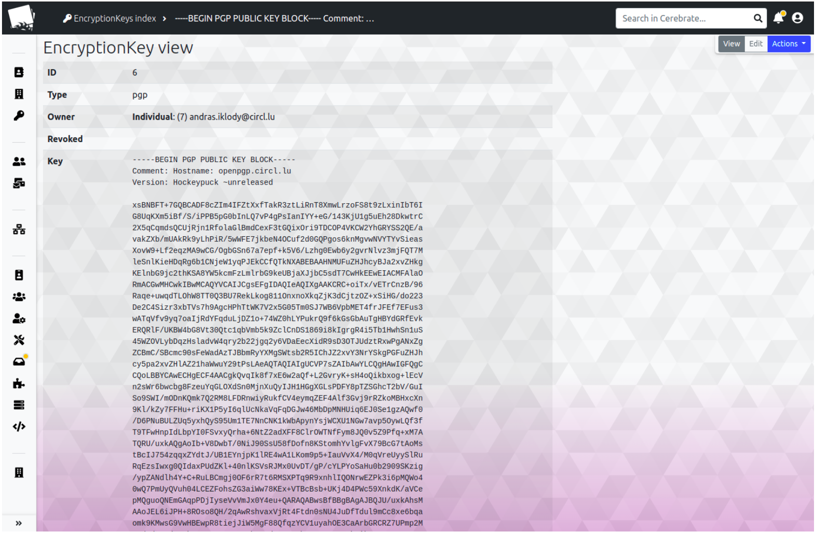
ID	4
UUID	fde69f4c-893a-47c4-b2e1-5180b236c69f
Name	Sharing group for take-down
Organisation	CIRCL
Releasability	For incident #54912
Description	
Active	✓
local	✓

#	Name	UUID	Actions
3	CERT POLSKA	71f77b2b-d871-4e96-b7c0-fae44e6f7a75	
12	CERT.at	c5325a5f-c256-4e3b-b5e4-1ba07f712755	
17	CIRCL	55f6ea5e-2c60-40e5-964f-47a8950d210f	

Cerebrate's contact database: Identity and Signing

- Cerebrate can act as a trusted contact database containing cryptographic keys (PGP, S/MIME)
- Which can be used by other application to sign and validate information
  - See MISP's protected Event feature

Cerebrate's contact database: Identity and Signing



EncryptionKeys index › -----BEGIN PGP PUBLIC KEY BLOCK----- Comment: ...
Search in Cerebrate...
View
Edit
Actions

EncryptionKey view

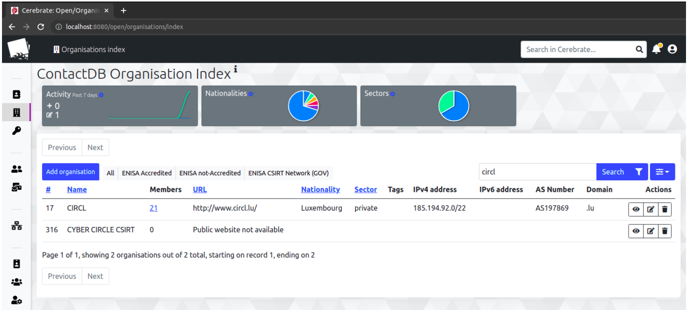
ID	6
Type	pgp
Owner	**Individual**: (7) andras.iklody@circl.lu
Revoked	
Key	see below

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: Hostname: openpgp.circl.lu
Version: Hockeypuck ~unreleased

xsBNBFT+7GQBCADF8cZIm4IFZtXxfTakR3ztLiRnT8XmwLrzoFS8t9zLxinIbT6I
G8UqKXm5iBf/S/iPPB5pG0bInLQ7vP4gPsIanIYY+eG/143KjU1g5uEh28DkwtrC
2X5qCqmdsQCUjRjn1RfolaGlBmdCexF3tGQixOri9TDCOP4VKCW2YhGRYSS2QE/a
vakZXb/mUAkRk9yLhPiR/5wWFE7jkbeN4OCuf2d0GQPgos6knMgvwNVYTYvSieas
XovW9+Lf2eqzMA9wCG/OgbGSn67a7epf+k5V6/Lzhg0Ewb6y2gvrNlvz3mjFQT7M
leSnlKieHDqRg6b1CNjeW1yqPJEkCCfQTkNXABEBAAHNMUFuZHJhcyBJa2xvZHkg
KElnbG9jc2thKSA8YW5kcmFzLmlrbG9keUBjaXJjbC5sdT7CwHkEEwEIACMFAlaO
RmACGwMHCwkIBwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRC+oiTx/vETrCnzB/96
Raqe+uwqdTLOhW8TT0Q3BU7RekLkog811OnxnoXkqZjK3dCjtzOZ+xSiHG/do223
De2C4Sizr3xbTVs7h9AgcHPhTtWK7V2x5G05Tm0SJ7WB6VpbMET4frJFEf7EFus3
wATqVfv9yq7oaIjRdYFqduLjDZ1o+74WZ0hLYPukrQ9f6kGsGbAuTgHBYdGRfEvk
ERQRlF/UKBW4bG8Vt30Qtc1qbVmb5k9ZclCnDS1869i8kIgrgR4i5Tb1HwhSn1uS
45WZOVLybDqzHsladvW4qry2b22jgq2y6VDaEecXidR9sD3OTJUdztRxwPgANxZg
ZCBmC/SBcmc90sFeWadAzTJBbmRyYXMgSWtsb2R5IChJZ2xvY3NrYSkgPGFuZHJh
cy5pa2xvZHlAZ21haWwuY29tPsLAeAQTAQIAIgUCVP7sZAIbAwYLCQgHAwIGFQgC
CQoLBBYCAwECHgECF4AACgkQvqIk8f7xE6w2aQf+L2GvryK+sH4oQikbxog+lEcV
n2sWr6bwcbg8FzeuYqGLOXdSn0MjnXuQyIJH1HGgXGLsPDFY8pTZSGhcT2bV/GuI
So9SWI/mODnKQmk7Q2RM8LFDRnwiyRukfCV4eymqZEF4Alf3Gvj9rRZkoMBHxcXn
9Kl/kZy7FFHu+riKX1P5yI6qlUcNkaVqFqDGJw46MbDpMNHUiq6EJ0Se1gzAQwf0
/D6PNuBULZUq5yxhQyS95Um1TE7NnCNK1kWbApynYsjWCXU1NGw7avp5OywLQf3f
T9TFwHnpIdLbpYI0FSvxyQrha+6NtZ2adXFF8ClrOWTNfFym8JQ0v5Z9Pfq+xM7A
TQRU/uxkAQgAoIb+V8DwbT/0NiJ90SsU58fDofn8KStomhYvlgFvX79BcG7tAoMs
tBcIJ754zqqxZYdtJ/UB1EYnjpK1lRE4wA1LKom9p5+IauVvX4/M0qVreUyySlRu
RqEzsIwxg0QIdaxPUdZKl+40nlKSVsRJMx0UvDT/gP/cYLPYoSaHu0b2909SKzig
/ypZANdlh4Y+C+RuLBCmgj0OF6rR7t6RMSXPTq9R9xnhlIQONrwEZPk3i6pMQWo4
0wQ7PmUyQVuh04LCEZFohsZG3aiWw78KEx+VTBcBsb+UKj4D4PWc59XnkdK/aVCe
pMQguoQNEmGAqpPDjIyseVvVmJx0Y4eu+QARAQABwsBfBBgBAgAJBQJU/uxkAhsM
AAoJEL6iJPH+8ROso8QH/2qAwRshvaxVjRt4Ftdn0sNU4JuDfTdul9mCc8xe6bqa
omk9KMwsG9VwHBEwpR8tiejJiW5MgF88QfqzYCV1uyahOE3CaArbGRCRZ7UPmp2M
```

Cerebrate's contact database: Open Directory

- Cerebrate can be configured to act as an **open** directory of contact information
- Other tools (including other Cerebrate nodes) can use this directory
- Allows for information and information source validation



ContactDB Organisation Index

#	Name	Members	URL	Nationality	Sector	Tags	IPv4 address	IPv6 address	AS Number	Domain	Actions
17	CIRCL	21	http://www.circl.lu/	Luxembourg	private		185.194.92.0/22		AS197869	.lu	
316	CYBER CIRCLE CSIRT	0	Public website not available								

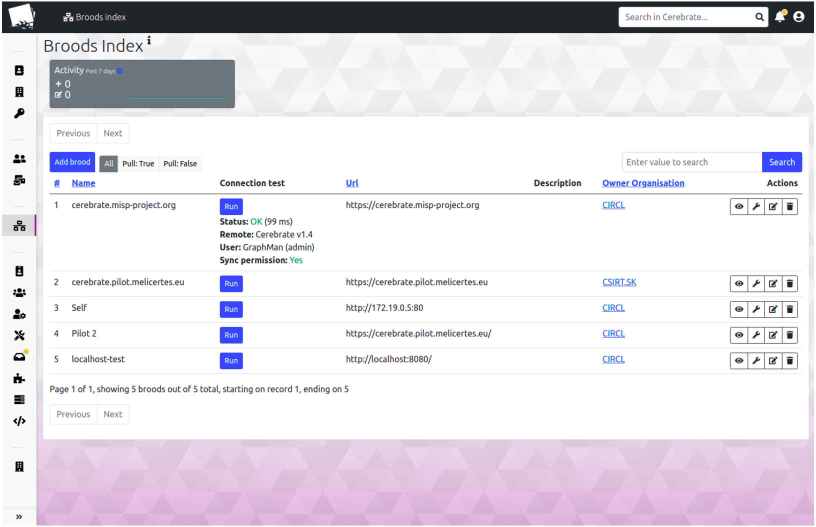
Page 1 of 1, showing 2 organisations out of 2 total, starting on record 1, ending on 2

Data sharing

Basically the same strategy as the one used in MISP:

- **Connect** with other Cerebrate nodes
- **Diagnose** connectivity issues
- Remotely **browse** data of the other node
- **Fetch and save** organisation, individual, sharing-group data

DATA SHARING

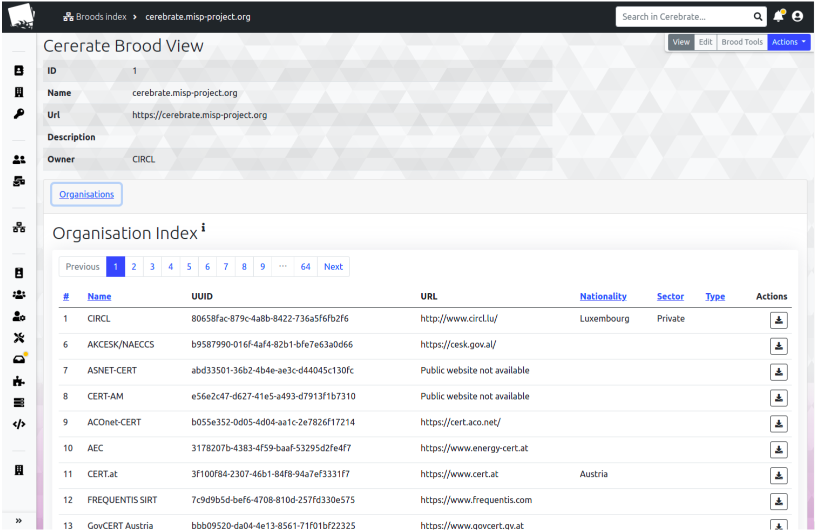


Broods Index

#	Name	Connection test	Url	Description	Owner Organisation	Actions
1	cerebrate.misp-project.org	Run **Status:** OK (99 ms) **Remote:** Cerebrate v1.4 **User:** GraphMan (admin) **Sync permission:** Yes	https://cerebrate.misp-project.org		CIRCL	
2	cerebrate.pilot.melicertes.eu	Run	https://cerebrate.pilot.melicertes.eu		CSIRT.SK	
3	Self	Run	http://172.19.0.5:80		CIRCL	
4	Pilot 2	Run	https://cerebrate.pilot.melicertes.eu/		CIRCL	
5	localhost-test	Run	http://localhost:8080/		CIRCL	

Page 1 of 1, showing 5 broods out of 5 total, starting on record 1, ending on 5

Data sharing



Broods index › cerebrate.misp-project.org
Search in Cerebrate...
View
Edit
Brood Tools
Actions

Cerate Brood View

ID	1
Name	cerebrate.misp-project.org
Url	https://cerebrate.misp-project.org
Description	
Owner	CIRCL

Organisation Index i

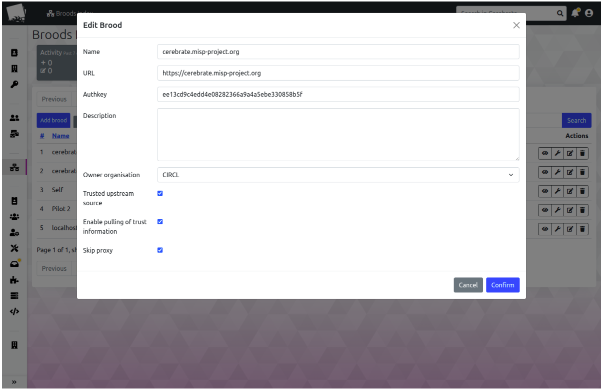
Previous 1 2 3 4 5 6 7 8 9 … 64 Next

#	Name	UUID	URL	Nationality	Sector	Type	Actions
1	CIRCL	80658fac-879c-4a8b-8422-736a5f6fb2f6	http://www.circl.lu/	Luxembourg	Private		
6	AKCESK/NAECCS	b9587990-016f-4af4-82b1-bfe7e63a0d66	https://cesk.gov.al/				
7	ASNET-CERT	abd33501-36b2-4b4e-ae3c-d44045c130fc	Public website not available				
8	CERT-AM	e56e2c47-d627-41e5-a493-d7913f1b7310	Public website not available				
9	ACOnet-CERT	b055e352-0d05-4d04-aa1c-2e7826f17214	https://cert.aco.net/				
10	AEC	3178207b-4383-4f59-baaf-53295d2fe4f7	https://www.energy-cert.at				
11	CERT.at	3f100f84-2307-46b1-84f8-94a7ef3331f7	https://www.cert.at	Austria			
12	FREQUENTIS SIRT	7c9d9b5d-bef6-4708-810d-257fd330e575	https://www.frequentis.com				
13	GovCERT Austria	bbb09520-da04-4e13-8561-71f01bf22325	https://www.govcert.gv.at				

Data sharing: Synchronisation strategies

Two synchronisation strategies:

1. **Standard**: Only fetch and save new records
2. **Trusted upstream source**: Remote Cerebrate acts as an authoritative instance



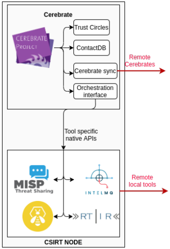
Edit Brood

Name	cerebrate.misp-project.org
URL	https://cerebrate.misp-project.org
Authkey	ee13cd9c4edd4e08282366a9a4a5ebe330858b5f
Description	
Owner organisation	CIRCL
Trusted upstream source	☑
Enable pulling of trust information	☑
Skip proxy	☑

MANAGING LOCAL TOOLS

Why would Cerebrate have integration with other tools?

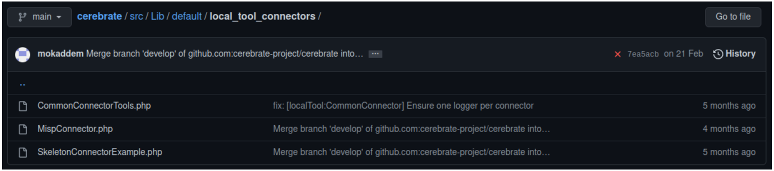
- To support information sharing, being able to validate information sources is crucial
- Traditional information sharing software stacks have to have their own organisation database
- Why re-invent the wheel everytime?



Managing local tools

There will inevitably be integration between local tools and Cerebrate. Why not go a step further?

- Cerebrate exposes a modular system to manage these local tools
- Based on a configuration file, user interfaces can be created to visualise data and instruct local tools to perform operations



main ▾ cerebrate / src / Lib / default / **local_tool_connectors** /

Go to file

mokaddem Merge branch 'develop' of github.com:cerebrate-project/cerebrate into… ··· × 7ea5acb on 21 Feb **History**

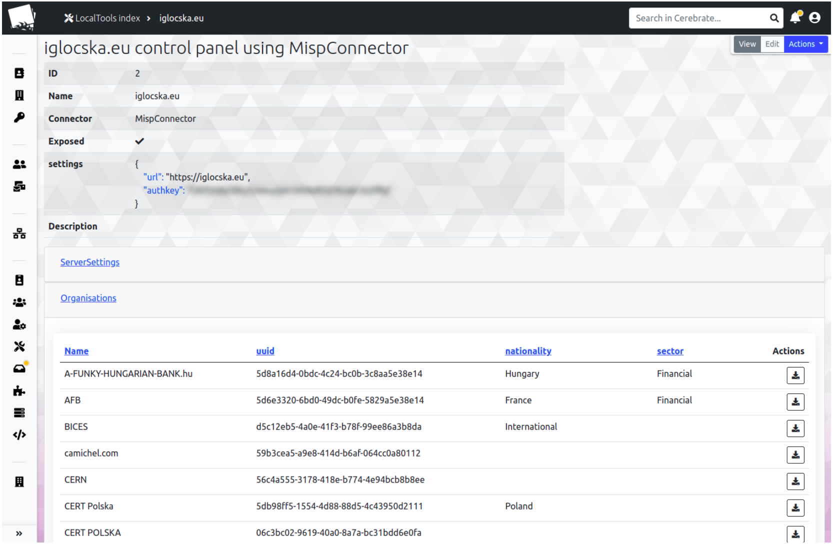
..

CommonConnectorTools.php	fix: [localTool:CommonConnector] Ensure one logger per connector	5 months ago
MispConnector.php	Merge branch 'develop' of github.com:cerebrate-project/cerebrate into…	4 months ago
SkeletonConnectorExample.php	Merge branch 'develop' of github.com:cerebrate-project/cerebrate into…	5 months ago

Local tool: MISP Connector capabilities

- **Configure** a MISP instances via server settings
- **Fetch** Organisations & Sharing Groups
- **Diagnose** other connected MISP servers
- **Manage** users, ...

LOCAL TOOL: MISP CONNECTOR CAPABILITIES



iglocska.eu control panel using MispConnector

ID	2
Name	iglocska.eu
Connector	MispConnector
Exposed	✓
settings	{ "url": "https://iglocska.eu", "authkey": [redacted] }
Description	

ServerSettings

Organisations

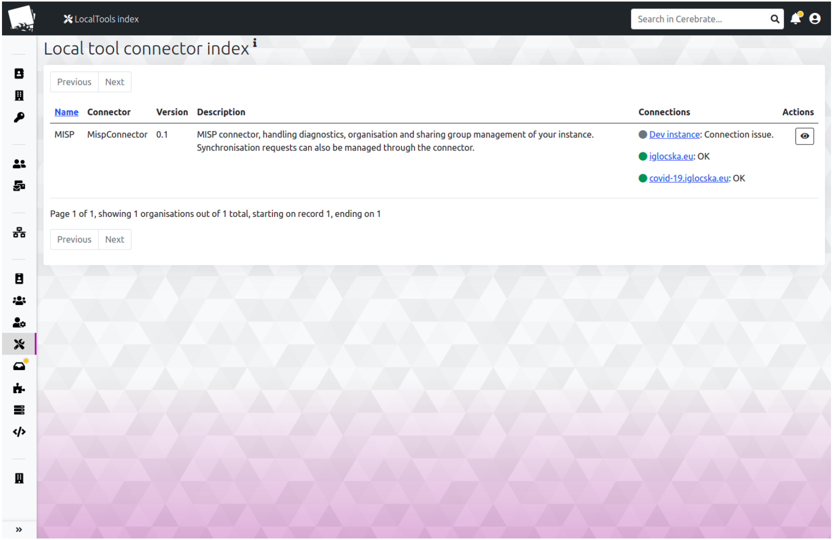
Name	uuid	nationality	sector	Actions
A-FUNKY-HUNGARIAN-BANK.hu	5d8a16d4-0bdc-4c24-bc0b-3c8aa5e38e14	Hungary	Financial	
AFB	5d6e3320-6bd0-49dc-b0fe-5829a5e38e14	France	Financial	
BICES	d5c12eb5-4a0e-41f3-b78f-99ee86a3b8da	International		
camichel.com	59b3cea5-a9e8-414d-b6af-064cc0a80112			
CERN	56c4a555-3178-418e-b774-4e94bcb8b8ee			
CERT Polska	5db98ff5-1554-4d88-88d5-4c43950d2111	Poland		
CERT POLSKA	06c3bc02-9619-40a0-8a7a-bc31bdd6e0fa			

Local tool: MISP Connector capabilities

Why do one when we can do many?

- Cerebrate can connect to multiple tools via its associated connector
- Allowing local tool fleet management
  - MISP fleet management!

Local tool: MISP Fleet management



Local tool connector index

Previous Next

Name	Connector	Version	Description	Connections	Actions
MISP	MispConnector	0.1	MISP connector, handling diagnostics, organisation and sharing group management of your instance. Synchronisation requests can also be managed through the connector.	● Dev instance: Connection issue. ● iglocska.eu: OK ● covid-19.iglocska.eu: OK	👁

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

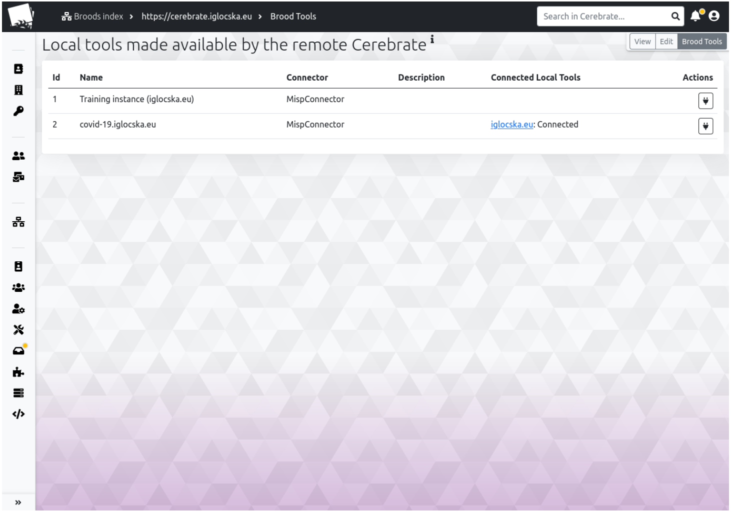
Previous Next

Local tool interconnection via Cerebrate

- Cerebrate's main goal is to **ease community management**
- Select which local tools are meant to be exposed to the community for requests
- Open dialogues to community members to request tool-to-tool interconnections

Local tool interconnection via Cerebrate

Cerebrate can leverage its access to local tool to reach out to tools from other Cerebrate nodes



Local tools made available by the remote Cerebrate

Id	Name	Connector	Description	Connected Local Tools	Actions
1	Training instance (iglocska.eu)	MispConnector			
2	covid-19.iglocska.eu	MispConnector		iglocska.eu: Connected	

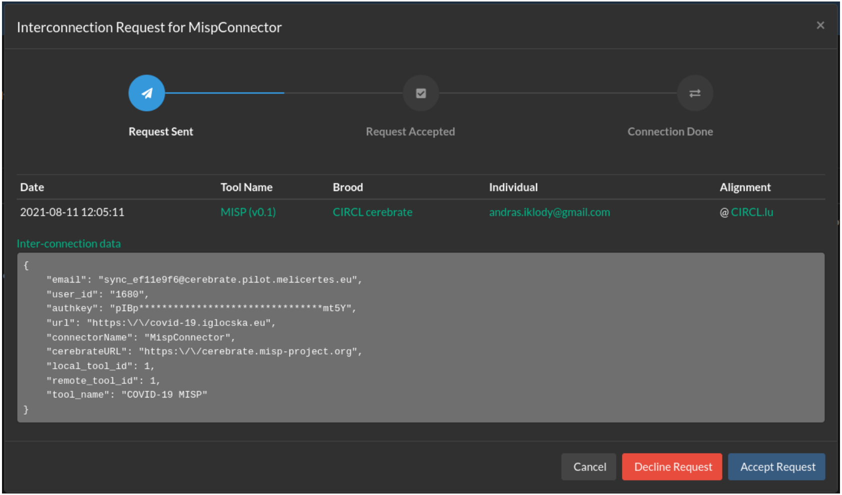
Local tool interconnection via Cerebrate

- Local tools can be **exposed** to other Cerebrate nodes
- **Inter-connection requests** can be issued from one node to another
- Following a 3-way handshake protocol, inter-connections can be:
    - Issued
    - Accepted
    - Finalised

Local tool interconnection via Cerebrate

MY DEAR, COULD YOU PROVIDE ME WITH ACCESS TO YOUR MISP?
IT WOULD BE MY PLEASURE. HERE YOU GO.
MUCH APPRECIATED.

MISP interconnection via Cerebrate



Interconnection Request for MispConnector

Date	Tool Name	Brood	Individual	Alignment
2021-08-11 12:05:11	MISP (v0.1)	CIRCL cerebrate	andras.iklody@gmail.com	@ CIRCL.lu

Inter-connection data

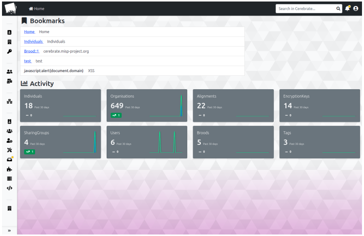
```
{
    "email": "sync_ef11e9f6@cerebrate.pilot.melicertes.eu",
    "user_id": "1680",
    "authkey": "pIBp********************************mt5Y",
    "url": "https:\/\/covid-19.iglocska.eu",
    "connectorName": "MispConnector",
    "cerebrateURL": "https:\/\/cerebrate.misp-project.org",
    "local_tool_id": 1,
    "remote_tool_id": 1,
    "tool_name": "COVID-19 MISP"
}
```

What else does Cerebrate have?

- Mailing list management
- ACL system
- Inbox system
  - Inter-connection requests, enrolment requests
- Tagging
- Update system
- Audit logs
- Open API

What else does Cerebrate have?

Cerebrate has `dark theme` and **more**!

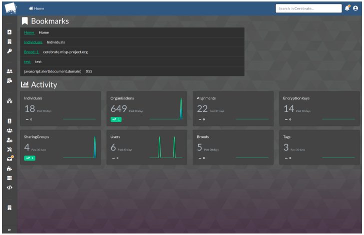


Bookmarks

Home Home
Individuals Individuals
Brood::1 cerebrate.misp-project.org
test test
javascript:alert(document.domain) XSS

Activity

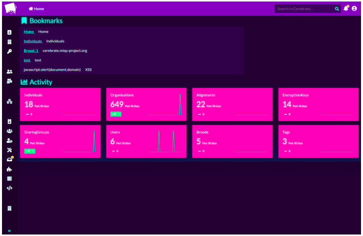
Individuals 18 Past 30 days — 0
Organisations 649 Past 30 days 1
Alignments 22 Past 30 days — 0
EncryptionKeys 14 Past 30 days — 0
SharingGroups 4 Past 30 days 1
Users 6 Past 30 days — 0
Broods 5 Past 30 days — 0
Tags 3 Past 30 days — 0


Bookmarks

Home Home
Individuals Individuals
Brood::1 cerebrate.misp-project.org
test test
javascript:alert(document.domain) XSS

Activity

Individuals 18 Past 30 days — 0
Organisations 649 Past 30 days 1
Alignments 22 Past 30 days — 0
EncryptionKeys 14 Past 30 days — 0
SharingGroups 4 Past 30 days 1
Users 6 Past 30 days — 0
Broods 5 Past 30 days — 0
Tags 3 Past 30 days — 0


Bookmarks

Home Home
Individuals Individuals
Brood::1 cerebrate.misp-project.org
test test
javascript:alert(document.domain) XSS

Activity

Individuals 18 Past 30 days — 0
Organisations 649 Past 30 days 1
Alignments 22 Past 30 days — 0
EncryptionKeys 14 Past 30 days — 0
SharingGroups 4 Past 30 days 1
Users 6 Past 30 days — 0
Broods 5 Past 30 days — 0
Tags 3 Past 30 days — 0

Current roadmap

- Data signing / validation
  - Community centric PKI
  - Enable data validation services for tools such as MISP
- Integration with other tools
  - Ticketing systems
  - Tighter Mailing list integration (Mailman)
  - Messaging App (Mattermost)

Thanks!

- Want to integrate your tool with Cerebrate?

  → Get in touch!
- Want to have a live demo?

  → Get in touch!
- Want to suggest features or integrations?

  That’s right → Get in touch!