

Cerebrate

Community management and tool orchestration the open-source way

Andras Iklody & Sami Mokaddem

Cerebrate Project

FIRSTCON22



WHO ARE WE ?



- 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

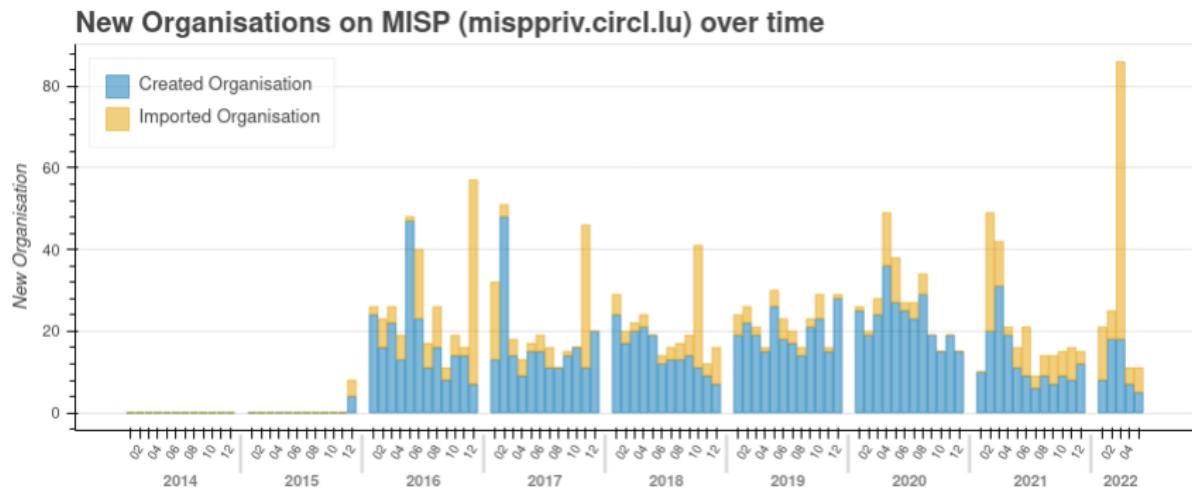
MELICERTES II: A QUICK RECAP OF THE MORNING SESSION

- 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)
 - **#FIRSTICON22** 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)

Hint:
Come to
the MISP
workshop
to learn
more!



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



A screenshot of a GitHub repository page for "cerebrate-project/cerebrate". The page shows the repository name, a "Public" badge, a "Notifications" button, a "Fork 11" button, a "Star 60" button, and a dropdown menu. The background of the screenshot is dark.

- 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

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API

★ MSP Graphman Sam Mokaddem Log out

Create Sync Config
List Servers
New Servers
Server overlap analysis matrix
List Communities

List Cerebrates
View Cerebrate **Edit Cerebrate** Add Cerebrate

Cerebrate view

Id 1
Name cerebrate.misp-project.org
URL <https://cerebrate.misp-project.org>
Owner Organisation CIRCL
Description
Organisations 
[← previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [next →](#) [last ▶](#)

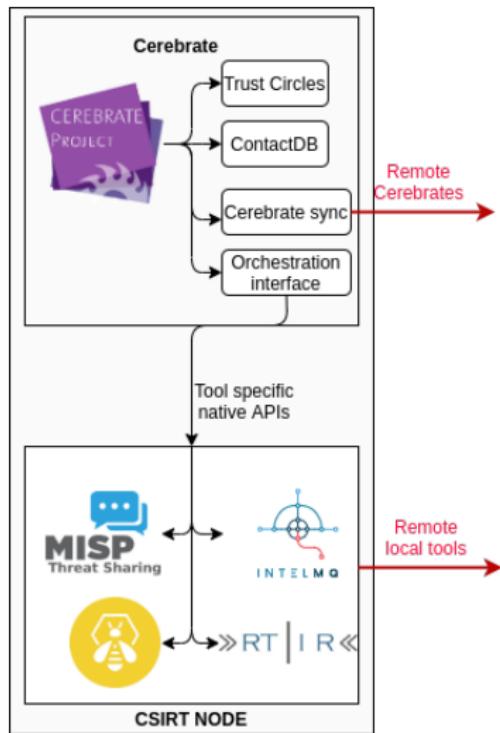
ID	Status	UUID	Name	Sector	Nationality	Actions
1	⌚	80058b479c-4fb8-4a29-73e9fbff02f6	CIRCL	Private	Luxembourg	
6	✗	b6587190-01b1-4a14-82b1-b6a7e53a0366	AKCEISKAECOS			
7	✗	a8c33501-38c2-4048-a6c5-d4d465130b	ASNET-CERT			
8	✓	e5b62a27-d827-7a1e5-4a93-d7913107310	CERT.AM			
9	✗	b659a505-0d05-4d54-a410-2e7820917214	ACOnet-CERT			
10	✗	3178207b-4385-4f59-baaf-5329522a4f7	AEC			
11	⌚	3110084-2307-46b1-8418-94a7e0333117	CERT.at		Austria	
12	✗	7cb00f5b-0ef9-4708-8100-257653005675	FREQUENTIS SIRT			
13	✗	b6b09520-da24-4e13-8561-71811e223235	GovCERT Austria			
14	✗	69830300-3000-4616-8936-20ab65709956	R-IT CERT			
15	✗	7d7e117e-9240-4199-8386-6d4126e24008	R-IT CSIRT			
16	✗	219980e0-8cc0-4376-1039-e14289953776	WienCERT			
17	✗	88277767-7531-4x66-be8b-0f897722e659	miCERT AT			
18	✗	c50ed65-c0b7-42b8-bb33-543e5c95499f	#CERT AT			
19	✗	a7054731-1761-4864-4761-903227070796	ArScienceCERT			
20	✗	19897449-256a-4234-ace1-75e9594e1c92	CERT AZ			

Could not locate the PGP public key.

Powered by [MISP 2.4.19](#) - 2022-09-29 03:03:44

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, ...

The screenshot shows the 'Organisation View' for the entry 'CIRCL'. The interface includes a navigation bar with 'Organisations index > CIRCL', a search bar 'Search in Cerebrate...', and buttons for 'View', 'Edit', and 'Actions'. The main content area displays the following data:

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	<ul style="list-style-type: none">[Core Team] sami.mokaddem@circl.lu[Core Team] alexandre.dulaunoy@circl.lu[Code Monkey] andras.iklody@circl.lu[Core Team] hugues.righetti@circl.lu Add individual
ENISA CSIRT Network	v3
CSIRT Constituency	v3
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

Organisations index Search in Cerebrate...   

ContactDB Organisation Index

Activity Past 7 days 

+ 0
of 0

Nationalities 

Sectors 

Previous Next

Add organisation		All	ENISA Accredited	ENISA not-Accredited	ENISA CSIRT Network (GOV)	circl	Search 				
#	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

Previous Next

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

FIRST Directory v1		ENISA CSIRT Network v3	CSIRT Constituency v1
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 Letzeburg" 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

The screenshot shows the Cerebrate interface for managing meta-templates. The top navigation bar includes 'MetaTemplates index' and 'FIRST Directory'. A search bar and a 'View Actions' button are also present. On the left, a sidebar lists various meta-template fields with their corresponding icons.

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

Previous Next

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

The screenshot shows a GitHub repository interface for the 'meta_fields' branch of the 'cerebrate' library. The commit history is displayed, showing various changes made by different users over time.

cerebrate / libraries / default / meta_fields /		
		Go to file
		Add file
...		...
	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

The screenshot shows the Cerebrate contact database interface for managing sharing groups. At the top, there is a navigation bar with icons for user, sharing group, and search, followed by a search bar labeled "Search in Cerebrate...". Below the navigation bar, the title "SharingGroup view" is displayed, along with a breadcrumb trail: "SharingGroups index > Sharing group for take-down". On the right side of the title bar are buttons for "View", "Edit", and "Actions".

The main content area displays a "SharingGroup view" for a group named "Sharing group for take-down" (ID: 4). The group is associated with the organization "CIRCL". The "Releasability" field indicates it is for incident #54912. The "Description" field is empty. The "Active" status is checked. The "local" setting is also checked.

Below the main view, there is a section titled "Organisations" with a sub-section "Add member". This section lists three organizations: "CERT POLSKA" (ID: 3), "CERT.at" (ID: 12), and "CIRCL" (ID: 17). Each organization entry includes its name, UUID, and two small action icons (one with a person and one with a trash can).

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

EncryptionKey view

ID	6
Type	pgp
Owner	Individual: (7) andras.iklody@circl.lu
Revoked	
Key	-----BEGIN PGP PUBLIC KEY BLOCK----- Comment: Hostname: openpgp.circl.lu Version: Hockeypuck ~unreleased xsBNBFt+7GBCAFDF8cZIm4IF2tXxfTakR3ztLIRnT8XmLrz0FS8t9zLxInIbT0I G8lUqKXm51Bf/S/1PPB5pg0bTnLQ7Vp4PgPsIaNYeG/143kj1g1guEh280ktrC 2X5qcndsqC0UjRjn1Rf0laG1BmdCexF3tGQ1x0r19TOp4VKw2YhGRYSS2QE/a vakZxb/mtAURkR9yLhPir/5wfME7jkbeN40CuF2d8GQpgos6knMgvwNvYTyVsieas XovW+9L7zegzhA9wC6/0gbGsn6n7a7epf+k5v6/Lzhg0Ew6y2gvrnVz3nJfQ17M 1eSnlKLehDgR0b1CNjEwygPjEXKCCTQfTKXABEBAAHNMUf2ZhJcyBja2xVhzKg KE1nb6gjzC2t1hSA8Y5KcmF2Lmrb69keUbjaXjBc5sd177wK1KEwE1ACMfAla0 RmACGwMHQwKwIBwMCAYQVCA1CgseFgIDAOtEAOjXgAACRC-o1Tx/wEt7CnB/96 Raqe-uwqfGTLOhW8TTQ03BU7RekLkogB110hnnoXkqZjKdCtz02+xS1H6/ds223 De2C451zr3xbTv7h8AgchPHtWkTV7v2x5G05tmgSJ7wb8VpbME4frJFEF7EFus3 wATqYfV9yq7oA1jRdyFgdJLjD2zio+74W20LYPukrQ9t6Kg5GbAu7gbHdgrEvk ERQR8LF/UKB4bG8Vt380tclgpbwB5k2c1LnS1B8918k1grg415tbi1MwNs1u5 45NzZ0V1LyDgzhIsIadvW4qrzB2jzpg2yvDnaEcx1Dr9sD30TJldztrRxwPAKXzg ZCBnc/SCBmc90sfewadzTJBmrRyXXMgSwts2R51ChJzzxvY3NrYSkgPGFu2HJh cySpa2xvZHLaZ21hawMwY29PsLAAeQTAAIAjgUCP7zA1bAwYLQ0gMwLGfQgC CQoLBByCAwECHjEFC4AACgkQvgTik8f7xE0w2aQf+L20vryk+sH4oQikbxkog+1EcV n2sW6bwcbg6fzeuytGLOXdsnMjNxuQy1JHNgxGLsP0DFyptZ2GhcT20uGuI So9s9W1/n00nKqmk7z2RMBLFDRnwlyRukTCV4eynqZ2Ef-4A1fGv9j9R2kz0M8txcXn 9kL/kzYTFFlu+riKX1P5y16d1uNckavqfQgDw40hd0pNHNUh0f0J0Se1gAfWf0 /D6PNuBULZUq5yxhQyS95UmTE7nCnK1kb1bpuynysjWCXu1Ngw7avp5OyL0f3f T9TfWhmpIdlbp1YR0FSvxYqRh+6Nz2adxF8B1crwTnfym8Jq6v5z9Pfpx+rMTA TQRu/ukkAQgqAoIb+8v0wbT/UN1J908su58f0fn8KStomhylgFvX79BcGTaoMs tBc1J7542zqq2YdJU/JB1eYnjK1IRE4wA1Lkomp9p+IauVwX4/M0qRvUdryS1Ru Rqfzr1nxgBg0IadxPU0DzK1-46n1ksVrsJmxv8u07/gp/CYLPrOsAHu0B2995Kz1g /ypZAN1ld4y+c+RULBcne100F6rR7t6RMSXPTq9RxnL1Q0NwEzP3k16Mw04 0wQ7PmUyQvh04LCEZFohsZ63a1m78KEx+VtBcBs+UKj4D4PwC59Xnkdk/avCe pMQuoQNEmAqPjDjYseVvMmXsY4eu+QARAAQAbw8FB8gBqAaBqJU/uxkahsM AAoJEL81JPh+GR0s0Qh/ZqmrShwshaxVYRt4Ftdn0sNu4jDftduL9mCc8veebqa omk9KMsG9WbHEBwR8tje1j1w5MgF88QfqzYCV1uyahOE3CaArbgRCRZ7UpPep2

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

The screenshot shows a web browser window titled "Cerebrate: Open/Organis..." with the URL "localhost:8080/open/organisations/index". The page is titled "Organisations index" and features a search bar "Search in Cerebrate...". At the top, there are three pie charts: "Activity" (Prod 7 days), "Nationalities", and "Sectors". Below the charts is a table header with columns: #, Name, Members, URL, Nationality, Sector, Tags, IPv4 address, IPv6 address, AS Number, Domain, and Actions. Two rows of data are listed: one for "CIRCL" (ID 17, 21 members, Luxembourg, private, 185.194.92.0/22, AS197869, Ju) and one for "CYBER CIRCLE CSIRT" (ID 316, 0 members, Public website not available). At the bottom, it says "Page 1 of 1, showing 2 organisations out of 2 total, starting on record 1, ending on 2".

#	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	Ju	
316	CYBER CIRCLE CSIRT	0	Public website not available								

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

The screenshot shows the 'Broods index' section of the Cerebrate application. At the top, there is a navigation bar with icons for user profile, search, notifications, and help. Below the navigation bar, the title 'Broods Index' is displayed, along with a summary of activity: '+ 0' and '0'.

Below the summary, there are buttons for 'Previous' and 'Next'. A filter bar includes 'Add brood', 'All', 'Pull: True', and 'Pull: False'. To the right of the filter bar is a search input field with placeholder 'Enter value to search' and a 'Search' button.

The main content area is a table titled 'Broods Index' with the following columns: '#', 'Name', 'Connection test', 'Url', 'Description', 'Owner Organisation', and 'Actions'. The table contains five rows of data:

#	Name	Connection test	Url	Description	Owner Organisation	Actions
1	cerebrate.misp-project.org	<button>Run</button> 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	<button>Run</button>	https://cerebrate.pilot.melicertes.eu	CSIRT SK		
3	Self	<button>Run</button>	http://172.19.0.5:80	CIRCL		
4	Pilot 2	<button>Run</button>	https://cerebrate.pilot.melicertes.eu/	CIRCL		
5	localhost-test	<button>Run</button>	http://localhost:8080/	CIRCL		

At the bottom of the table, there is a message: 'Page 1 of 1, showing 5 broods out of 5 total, starting on record 1, ending on 5'. Below this message are 'Previous' and 'Next' buttons.

DATA SHARING

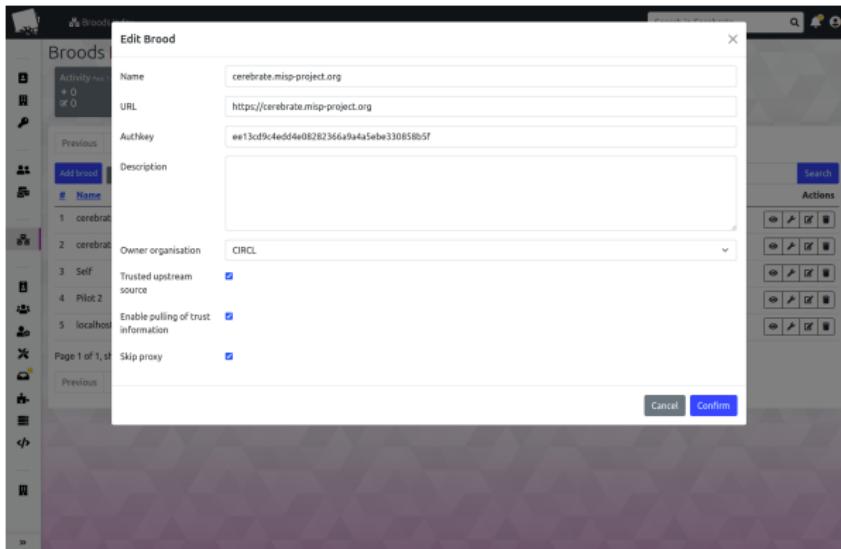
The screenshot shows the Cerebrate Brood View interface. At the top, there's a navigation bar with 'Broods index' and 'cerebrate.misp-project.org'. A search bar says 'Search in Cerebrate...'. On the right, there are 'View', 'Edit', 'Brood Tools', and 'Actions' buttons. Below the navigation is a section titled 'Cerate Brood View' with fields for ID (1), Name (cerebrate.misp-project.org), and Url (https://cerebrate.misp-project.org). Under 'Description', it lists 'Owner' as CIRCL. A sidebar on the left has icons for various brood types. A 'Organisations' tab is selected. Below it is an 'Organisation Index' with a table of 13 entries. The table columns are #, Name, UUID, URL, Nationality, Sector, Type, and Actions. The first entry is CIRCL.

#	Name	UUID	URL	Nationality	Sector	Type	Actions
1	CIRCL	B0658fac-879c-4a8b-8422-736a5f6fb2f6	http://www.circ.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-4383-4ff5-9baaf-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.at				

DATA SHARING: SYNCHRONISATION STRATEGIES

Two synchronisation strategies:

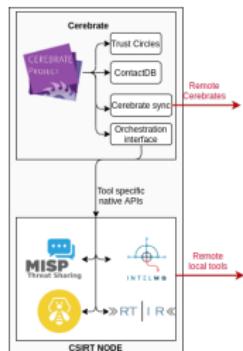
1. **Standard:** Only fetch and save new records
2. **Trusted upstream source:** Remote Cerebrate acts as an authoritative instance



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

The screenshot shows a GitHub repository interface for the 'cerebrate' project. The URL in the address bar is 'cerebrate / src / Lib / default / local_tool_connectors /'. The main content area displays a list of pull requests:

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

The screenshot shows a web-based control panel for the domain iglocska.eu, utilizing the MispConnector tool. The interface includes a navigation bar with 'LocalTools index' and 'iglocska.eu', a search bar, and a header with 'View', 'Edit', and 'Actions' buttons. The main content area displays the configuration for the 'iglocska.eu' connector, showing its ID (2), Name (iglocska.eu), Connector (MispConnector), and status (Exposed checked). It also shows the settings object containing the URL and authkey. Below this, there's a 'Description' section and two collapsed sections: 'ServerSettings' and 'Organisations'. A large table lists various entities with columns for Name, uuid, nationality, sector, and Actions.

Name	uuid	nationality	sector	Actions
A-FUNKY-HUNGARIAN-BANK.hu	5d8a16d4-0bdc-4c24-bc0b-3caa5e38e14	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-e94bcb8b8ee			
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

The screenshot shows a web application interface for managing local tool connectors. The top navigation bar includes a logo, the text "LocalTools index", a search bar with placeholder "Search in Cerebrate...", and several icons for filtering and sorting.

The main title is "Local tool connector index". Below it is a table with the following columns: Name, Connector, Version, Description, Connections, and Actions.

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.	<ul style="list-style-type: none">● Dev instance: Connection issue.● iglocska.eu: OK● covid-19.iglocska.eu: OK	

Below the table, a message indicates "Page 1 of 1, showing 1 organisations out of 1 total, starting on record 1, ending on 1".

The left sidebar contains a vertical list of icons representing different tools or components, with the "X" icon being the active tab.

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

The screenshot shows a web-based interface for managing local tools. At the top, there's a navigation bar with icons for 'Broods index' and 'https://cerebrate.iglocska.eu'. Below the navigation is a search bar labeled 'Search in Cerebrate...' and a toolbar with 'View', 'Edit', and 'Brood Tools' buttons.

The main content area displays a table titled 'Local tools made available by the remote Cerebrate'. The table has columns for 'Id', 'Name', 'Connector', 'Description', and 'Connected Local Tools'. There are two entries:

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

A vertical sidebar on the left contains various icons for different tool categories, such as file management, databases, and network monitoring. At the bottom left, there are navigation arrows for '»' and '<»'.

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



MISP INTERCONNECTION VIA CEREBRATE

Interconnection Request for MispConnector



Request Sent Request Accepted Connection Done

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

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"  
}
```

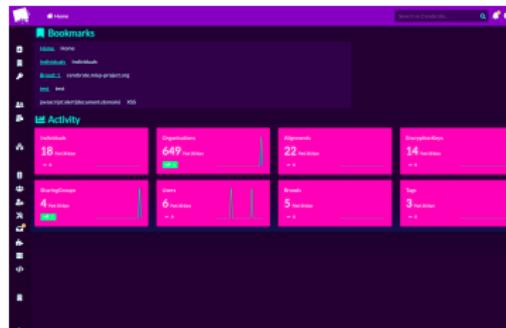
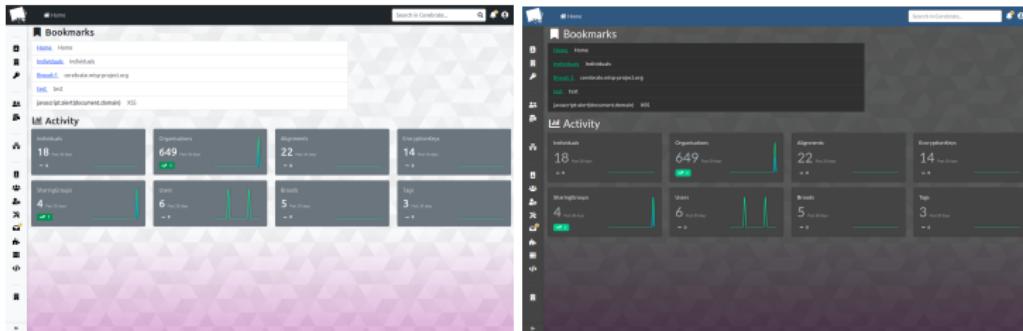
Cancel Decline Request Accept Request

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!**



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!