

MANAGING INFORMATION SHARING COMMUNITIES

E.103

CIRCL COMPUTER INCIDENT RESPONSE CENTER LUXEMBOURG

MISP PROJECT

<https://www.misp-project.org/>

MARCH 24, 2022



OBJECTIVES OF THIS MODULE

- Tips for joining information sharing communities
- Tips for being a good member in a sharing community
- Tips for building your own sharing community
- Tool for managing a sharing community
 - ▶ Managing organisations and contacts
 - ▶ Maintaining distribution lists (aka sharing groups)
 - ▶ Managing a large cluster of MISPs

BEING PART OF AN INFORMATION SHARING COMMUNITY

There is a wide range of MISP communities type:

- Private sector communities
 - ▶ Private organisations, researchers, central hub
- ISACs communities
 - ▶ Central hub for sectorial or geographical Communities
 - ▶ Examples: GSMA, FIRST.org, CSIRT Network, Banking, etc
- Ad-hoc communities
 - ▶ Often use for exercises such as ENISA or LockedShield

Considerations before joining a sharing community:

- Understand the community's objectives
 - ▶ Defense, prevention, collaboration, research, specific reporting duties
- Make sure the use-cases are not conflicting
 - ▶ False-positive appetite, maturity levels, topical interests
 - ▶ Detection rules VS threat intelligence VS prevention

TIPS FOR BEING A GOOD MEMBER OF A SHARING COMMUNITY

- As explained extensively in course e.206, Context is king:
 - ▶ You should try to contextualise as best as you can using:
 - ▶ Normalized vocab: Taxonomies, Galaxies & MITRE ATT&CK
 - ▶ Connected graph using MISP Objects and relationships
 - ▶ Add timeliness with Sightings and `first_seen` / `last_seen`
- Sharing results and reports
- Sharing enhancements or proposals to existing data
- Validating data (sightings) or flagging false positives
- Asking for support from the community

- Different models for your constituents
 - ▶ **Having an account** on a MISP instance
 - ▶ **Hosting** their own instance and connecting to a peer
 - ▶ **Becoming member** of a sectorial MISP community that is connected to multiple peers
- Planning ahead for future growth
 - ▶ Estimating requirements (workforce, hardware requirements)
 - ▶ Deciding early on common vocabularies (i.e. taxonomies)
 - ▶ Offering services through MISP to promote adhesion

TIPS FOR BUILDING YOUR OWN SHARING COMMUNITY

- **Lead by example** - the power of imitation
- Don't block sharing with unrealistic quality controls
 - ▶ You might lose organisations that might turn into valuable contributors
 - ▶ Organisations will start sharing junk to stay above the thresholds
- Encourage **improving by doing**
 - ▶ What should the information look like?
 - ▶ How should it be contextualised
 - ▶ What do you consider as useful information?
 - ▶ What tools did you use to get your conclusions?
- Side effect is that you will end up **raising the capabilities of your constituents**

- Convert the passive organisations into actively sharing ones
 - ▶ Help them increase their capabilities
 - ▶ Lead by example
 - ▶ **Give credit where credit is due**
 - Never steal the contribution of your community
 - ▶ Offers the possibility to take over their data via **delegation**
 - Anonymity of organisations might help them building confidence at the beginning

TIPS FOR BUILDING YOUR OWN SHARING COMMUNITY

- Encourage sharing of supporting materials, scripts or guidance for protection
- Raise awareness about the benefits of a well modelled, graph-based information
- Again, **context is king!** If possible, make contextualisation a requirement
 - ▶ Users can then filter based on their needs
 - ▶ Classification help your peers to understand why the data is important
 - ▶ And also, why this data can be useful to them

DISPELLING THE MYTHS AROUND BLOCKERS WHEN IT COMES TO INFORMATION SHARING

- Sharing difficulties are not really technical issues but often it's a matter of **social interactions** (e.g. **trust**).
 - ▶ You can play a role here: organise regular workshops, conferences, have face to face meetings
- Legal restrictions
 - ▶ "Our legal framework doesn't allow us to share information."
 - ▶ "Risk of information leak is too high and it's too risky for our organization or partners."
- Practical restrictions
 - ▶ "We don't have information to share."
 - ▶ "We don't have time to process or contribute indicators."
 - ▶ "Our model of classification doesn't fit your model."
 - ▶ "Tools for sharing information are tied to a specific format, we use a different one."

- Often within a community, **smaller bubbles** of information sharing will form
 - ▶ e.g: Within a national private sector community, a dedicated community for financial institutions
 - ▶ If an incident involves multiple organisations
- MISP's sharing group serve this purpose mainly
- If you are building your own community, consider bootstrapping these specific sharing community
 - ▶ Organisations can self-organise, but you are probably the ones with the know-how to get them started

COMMUNITY MANAGEMENT AND OR- CHESTRATION TOOL

- MISP is just one part of the puzzle
- Information sharing presumes knowledge of contacts
- Creating reusable community-specific distribution list need to be maintained
- Fleet management for larger organisations needs additional work

Cerebrate is an open-source tool meant to address these challenges

WHAT IS CEREBRATE?



- Open source **community management and orchestration** tool
- Central tool for the Melicertes 2 project (Co-funded by the EU as a CEF project)
 - ▶ Project for the CSIRT network building a common set of tools and services for the national CSIRTs
 - ▶ Flexible to support a wide range of communities
- Tight **integration** with various open-source tools
- Planned as the primary MISP management tool

WHY DO WE NEED CEREBRATE FROM A MISP PERSPECTIVE

■ **Deficiencies** in our current tool chain

- ▶ Do I really have to jump through hoops and long e-mail chains to **onboard new members**?
- ▶ How do I **find trusted information** on who an organisation is in MISP?
- ▶ How can I **manage a large cluster of MISPs** without tedious manual labour?
- ▶ If I run a community through MISP, how can I reuse my member information for other community tasks such as mailing lists?
- ▶ Information signing has been on the MISP roadmap for a long time - where do we get ground truths for a community from?

WHAT ISSUES IS CEREBRATE TRYING TO TACKLE?

■ Community management

- ▶ **Repository** of organisations and individuals
- ▶ Management of **sharing groups**
- ▶ **Exchange** of contact and sharing group information
- ▶ Cryptographic key lookup for **information signing**

■ Local tool management

- ▶ Instrumentation of **local tool interconnections**
- ▶ Local tool **fleet management**
- ▶ **Feeding** the local tools with Cerebrate data

CEREBRATE: WHAT IS AVAILABLE CURRENTLY?

- A set of Common functionalities
- Contact Database
- Sharing group management
- Cerebrate to Cerebrate synchronisation
- Mailing list management
- Local tool orchestration - integration modules
- Inbox system
- Local tool fleet management

- Index of Organisations and Individuals
- Flexible meta-data model (community specific, constituency, etc)
- Content aware search functionalities

CEREBRATE: CONTACT DATABASE

Flexible meta-data model to include community specific data point

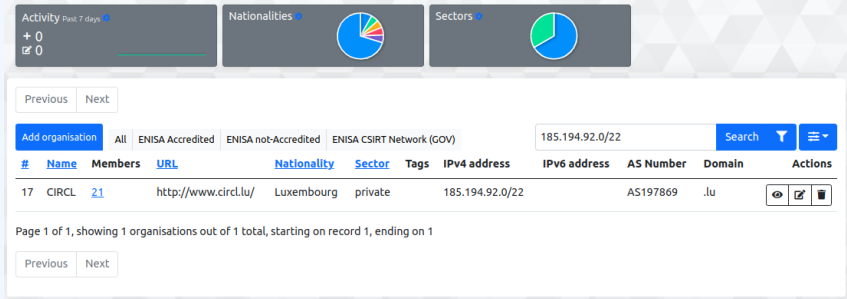
The screenshot displays the Cerebrate web application interface. At the top, a dark navigation bar contains the 'Organisations Index > CIRCL' breadcrumb, a search bar with the placeholder 'Search in Cerebrate...', and notification and user icons. The main content area is titled 'Organisation View' and includes 'View', 'Edit', and 'Actions' buttons. A left sidebar contains various icons for navigation. The central panel shows the details for the 'CIRCL' organisation, including its ID (17), UUID, URL, Nationality (Luxembourg), Sector (private), Type, Contacts (info@circl.lu), and Tags (+). The 'Alignments' section lists roles and email addresses: [Developer] sami.mokaddem@circl.lu, [Core Team] sami.mokaddem@circl.lu, [Core Team] cedric.bonhomme@circl.lu, and [Core Team] steve.clement@circl.lu. Below this, a table displays additional metadata for the 'ENISA CSIRT Network' and 'CSIRT Constituency'.

Metadata	Value
ISO 3166-1 Code	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: CONTACT DATABASE

Content aware search functionalities: CIDR block search

ContactDB Organisation Index



CEREBRATE: CONTACT DATABASE

Global searches on a large variety of data point

The screenshot displays a search interface with a search bar at the top containing the text 'mokaddem' and a magnifying glass icon. Below the search bar, the results are categorized into three sections: METAFIELDS, INDIVIDUALS, and USERS. Each section has a horizontal line and a count on the right. The METAFIELDS section lists two alternate email addresses. The INDIVIDUALS section lists one email address. The USERS section lists one user name. At the bottom of the results area, there is a magnifying glass icon followed by the text 'View all results'.

Category	Count
METAFIELDS	2
INDIVIDUALS	1
USERS	1

View all results

CEREBRATE: SHARING GROUP MANAGEMENT

Allow to define sharing groups composed of organisations that can be download from another Cerebrate or from MISP

The screenshot shows the 'SharingGroups Index' page for 'Test Sharinggroup'. The interface includes a search bar, navigation icons, and a detailed view of the sharing group. The group details show it is active and local. Below, the 'Organisations' section lists members with their IDs, names, UUIDs, and actions (view/delete).

SharingGroups Index > Test Sharinggroup

Search in Cerebrate...

SharingGroup view

View Edit Actions

ID	1
UUID	ee19cb12-531b-463d-87d6-b37df6b3e730
Name	Test Sharinggroup
Organisation	CIRCL
Releasability	
Description	
Active	✓
local	✓

Organisations

Add member

#	Name	UUID	Actions
13	CERT.be	acd27f7f-3dae-4481-b431-807431259c30	
17	CIRCL	55f6ea5e-2c60-40e5-964f-47a8950d210f	

CEREBRATE: SHARING GROUP MANAGEMENT

Sharing groups can also be generated based on filters via the reusable blueprints

#19: Non-sanctioned financial organisations 

```
{  
  "AND": {  
    "OR": {  
      "org_sector": "Financial",  
      "sharing_group_id": 127  
    },  
    "NOT": {  
      "org_nationality": [  
        "Russia",  
        "Russian Federation",  
        "Belarus",  
        "Republic of Belarus"  
      ]  
    }  
  }  
}
```



Mechanism to exchange contact data via synchronisation

The screenshot displays the 'Broods Index' interface. At the top, there's a dark header with the 'Broods Index' logo, a search bar labeled 'Search in Cerebrate...', and notification icons. Below the header, the 'Broods Index' title is followed by an 'Activity' summary box showing '+ 0' and '0' with a 'Past: 7 days' filter. The main content area features a table of broods. The table has columns for '#', 'Name', 'Connection test', 'Url', 'Description', 'Owner Organisation', and 'Actions'. A single brood is listed with the name 'cerebrate.misp-project.org'. The 'Connection test' column contains a 'Run' button and status details: 'Status: OK (243 ms)', 'Remote: Cerebrate v1.4', 'User: GraphMan (admin)', and 'Sync permission: Yes'. The 'Url' column shows 'https://cerebrate.misp-project.org'. The 'Owner Organisation' column shows 'CIRCL'. The 'Actions' column contains icons for view, edit, and delete. Navigation buttons for 'Previous' and 'Next' are present above and below the table. A footer bar at the bottom indicates 'Page 1 of 1, showing 1 broods out of 1 total, starting on record 1, ending on 1'.

Broods Indexⁱ

Activity Past: 7 days
+ 0
0

Previous Next

Add brood All Pull: True Pull: False

Enter value to search Search

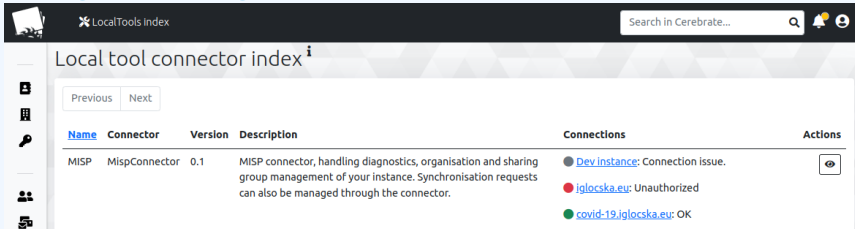
#	Name	Connection test	Url	Description	Owner Organisation	Actions
1	cerebrate.misp-project.org	Run Status: OK (243 ms) Remote: Cerebrate v1.4 User: GraphMan (admin) Sync permission: Yes	https://cerebrate.misp-project.org		CIRCL	View Edit Delete

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

Previous Next

CEREBRATE: LOCAL TOOL ORCHESTRATION

Manage and configure local tools (such as MISP) via Cerebrate




The screenshot displays the 'LocalTools Index' interface. At the top, there is a search bar labeled 'Search in Cerebrate...' and a notification bell icon. The main heading is 'Local tool connector index'. Below this, there are 'Previous' and 'Next' navigation buttons. A table lists the connectors, with the 'MISP' connector selected. The table has columns for Name, Connector, Version, Description, Connections, and Actions. The 'Connections' column for the MISP connector shows three entries: 'Dev instance: Connection issue.' (grey dot), 'iglocska.eu: Unauthorized' (red dot), and 'covid-19.iglocska.eu: OK' (green dot). An 'Actions' column with an eye icon is also present.

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: Unauthorized● covid-19.iglocska.eu: OK	


CEREBRATE: LOCAL TOOL ORCHESTRATION

Inter-connect local tools (such as a MISP instance) to another through 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.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"}
```

Cancel Decline Request Accept Request

USE CASE SPECIFIC TO LAW ENFORCEMENT

- Budapest convention allowed us to have a public inventory of contact information
- Once this data is ingested in Cerebrate, we can make use of the search functionalities to quickly get the information we need

TODO: Include picture of data stored in Cerebrate