

MANAGING INFORMATION SHARING COMMUNITIES

E.103

CIRCL COMPUTER INCIDENT RESPONSE CENTER LUXEMBOURG

MISP PROJECT

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

MARCH 21, 2022



OBJECTIVES OF THIS MODULE

- Joining an information sharing communities
- Tips for being a good member of a sharing community
- Tips for building your own sharing community
- Managing sub-sharing communities
 - ▶ Managing organisations and contacts
 - ▶ Maintaining distribution lists (aka sharing groups)
 - ▶ Manage large cluster of MISPs

BEING PART OF AN INFORMATION SHARING COMMUNITY

Wide range of MISP communities:

- 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:
 - ▶ Taxonomies & Galaxies
 - ▶ MITRE ATT&CK
 - ▶ MISP Objects and relationships
 - ▶ Sightings and `first_seen` / `last_seen`
- Sharing results or reports
- Sharing enhancements or proposals to existing data
- Validating data (sightings) or flagging false positives
- Asking for support from the community

- Different models for 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
- Raise awareness about the benefits of a well modelled, graph based information sharing
- 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 it 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
 - ▶ 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 in any sharing community
- 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 the new 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

The logo for the CEREBRATE Project is displayed on a purple, tilted rectangular background. The text "CEREBRATE" is on the top line and "PROJECT" is on the bottom line, both in white, uppercase, sans-serif font. Below the text, there is a faint, stylized graphic of a brain or a network of nodes.

CEREBRATE
PROJECT

■ **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 IT 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 contact database interface. At the top, there is a navigation bar with "Organisations index" and "CIRCL". A search bar on the right contains the text "Search in Cerebrate...". Below the navigation bar, the "Organisation View" for "CIRCL" is shown. The view includes a sidebar with icons for various data points and a main content area with a table of metadata. The table lists fields such as ID, Name, UUID, URL, Nationality, Sector, Type, Contacts, Tags, and Alignments. The "Alignments" section shows a list of roles and associated email addresses. Below the table, there are two tabs: "ENISA CSIRT Network v3" and "CSIRT Constituency v1". The "CSIRT Constituency v1" tab is active, showing a list of fields and their values.

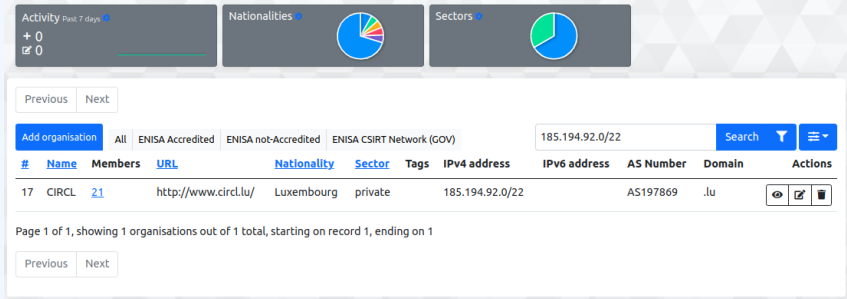
Field	Value
ID	17
Name	CIRCL
UUID	55f6ea5e-2c60-40e5-964f-47a8950d210f
URL	http://www.circl.lu/
Nationality	Luxembourg
Sector	private
Type	
Contacts	info@circl.lu
Tags	+
Alignments	<ul style="list-style-type: none">[Developer] sami.mokaddem@circl.lu[Core Team] sami.mokaddem@circl.lu[Core Team] cedric.bonhomme@circl.lu[Core Team] steve.clement@circl.lu

ENISA CSIRT Network v3 CSIRT Constituency v1

Field	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

Content aware search functionalities: CIDR block search

ContactDB Organisation Indexⁱ



CEREBRATE: CONTACT DATABASE

Global searches on a large variety of data point

The screenshot shows 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 email addresses with their corresponding field names in parentheses. The INDIVIDUALS section lists one email address. The USERS section lists one username. 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

Results:

- sami.mokaddem@circl.lu (individual::alternate_email)
- sami.mokaddem@securitymadein.lu (individual::alternate_email)
- sami.mokaddem@circl.lu
- mokaddem

[View all results](#)

CEREBRATE: SHARING GROUP MANAGEMENT

Allow to defined sharing groups composed of organisation that can be download from another Cerebrate or from MISP

The screenshot shows the 'SharingGroup view' in Cerebrate. The top navigation bar includes 'SharingGroups index > Test Sharinggroup', a search bar, and notification icons. The main content area displays the details of a sharing group with the following fields:

- ID: 1
- UUID: ee19cb12-531b-463d-87d6-b37df5b3e730
- Name: Test Sharinggroup
- Organisation: CIRCL
- Releasability: (empty)
- Description: (empty)
- Active: ☒
- Local: ☒

Below these details is a section titled 'Organisations' with an 'Add member' button. It contains a table with two members:

#	Name	UUID	Actions
13	CERT.be	acd2777f-3dae-4481-b431-807431259c30	
17	CIRCL	55f6ea5e-2c60-40e5-964f-47a8950d210f	

Sharing group blueprints to define reusable blueprints for generating sharing

```
#10: 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

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 main content area has a light gray geometric pattern background. On the left, a sidebar contains icons for various functions. The main panel shows an 'Activity' summary for the last 7 days with '+ 0' and '0' counts. Below this is 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 shows a 'Run' button and details: 'Status: OK (243 ms)', 'Remote: Cerebrate v1.4', 'User: GraphMan (admin)', and 'Sync permission: Yes'. The 'Url' column contains 'https://cerebrate.misp-project.org'. The 'Owner Organisation' column has a link 'CIRCL'. The 'Actions' column contains icons for view, edit, and delete. At the bottom, a pagination bar 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

Inter-connect local tools (such as a MISP instance) to another through Cerebrate

The screenshot displays the Cerebrate LocalTools Index interface. At the top, there's a search bar labeled "Search in Cerebrate...". Below it, the "Local tool connector index" is shown with a table of connectors. The table has columns for Name, Connector, Version, Description, Connections, and Actions. A single entry for "MISP" is visible, using the "MispConnector" (version 0.1). The description states it handles diagnostics, organization, and sharing of group management. The "Connections" column shows three entries: "Dev instance" (Connection issue), "iglocska.eu" (Unauthorized), and "covid-19.iglocska.eu" (OK). An "Interconnection Request for MispConnector" modal is open, showing a progress bar with three stages: "Request Sent" (completed), "Request Accepted" (in progress), and "Connection Done" (pending). Below the progress bar is a table of interconnection requests with columns for Date, Tool Name, Brood, Individual, and Alignment. A single request is listed for "MISP (v0.1)" on "2021-08-11 12:05:11", associated with "CIRCL cerebrate" and "andras.klody@gmail.com", aligned with "@ CIRCL.lu". At the bottom, the "Inter-connection data" is shown as a JSON object.

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: Unauthorizedcovid-19.iglocska.eu: OK	

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

```
{  "email": "sync_ef11e9f6@cerebrate.pilot.melicertes.eu",  "password": "XXXXXXXXXX"}
```

USE CASE SPECIFIC TO LE

- 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

The logo for the Cerebrate Project is displayed on a light blue background. It features a large, tilted purple rectangle containing the word "CEREBRATE" in white, uppercase, sans-serif font. Below it, the word "PROJECT" is also in white, uppercase, sans-serif font, but it is partially cut off by the bottom edge of the image. To the right of the main purple rectangle, there are two smaller, overlapping geometric shapes: a dark purple rectangle and a lighter purple trapezoid.

CEREBRATE
PROJECT