

MANAGING INFORMATION SHARING COMMUNITIES

E.103

CIRCL COMPUTER INCIDENT RESPONSE CENTER LUXEMBOURG

MISP PROJECT

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

MARCH 21, 2022



2022-03-21

Managing information sharing communities

MANAGING INFORMATION SHARING
COMMUNITIES

E.103

CIRCL COMPUTER INCIDENT RESPONSE CENTER LUXEMBOURG

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

MARCH 21, 2022



- 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

2022-03-21

Managing information sharing communities

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

2022-03-21

Managing information sharing communities

└ Being part of an information sharing community

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

Managing information sharing communities

- └ Being part of an information sharing community
- └ Joining an information sharing communities

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

Managing information sharing communities

- └ Being part of an information sharing community
 - └ Joining an information sharing communities

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

2022-03-21

Managing information sharing communities

- └ Being part of an information sharing community
 - └ 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

Managing information sharing communities

└ Being part of an information sharing community

└ Tips for building your own sharing 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**

Managing information sharing communities

- └ Being part of an information sharing community
 - └ 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

└ Being part of an information sharing community

└ Tips for building your own sharing community

- 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

- 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

Managing information sharing communities

└ Being part of an information sharing community

└ 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."

2022-03-21

Managing information sharing communities

- └ Being part of an information sharing community
- └ 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

Managing information sharing communities

- └ Being part of an information sharing community
 - └ Managing sub-sharing communities

- 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 ORCHESTRATION TOOL

2022-03-21

Managing information sharing communities

└ Community management and orchestration tool

COMMUNITY MANAGEMENT AND ORCHESTRATION 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

2022-03-21

Managing information sharing communities

└ Community management and orchestration tool

└ Additional challenges of community management

- 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

CEREBRATE
PROJECT

2022-03-21

Managing information sharing communities

└ Community management and orchestration tool

└ What is Cerebrate?

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



■ 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?

Managing information sharing communities

└ Community management and orchestration tool

└ Motivations 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 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

2022-03-21

Managing information sharing communities

└ Community management and orchestration tool

└ 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

2022-03-21

Managing information sharing communities

└ Community management and orchestration tool

└ 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

2022-03-21

- Managing information sharing communities
 - └ Community management and orchestration tool
 - └ Cerebrate: Contact database

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

CEREBRATE: CONTACT DATABASE

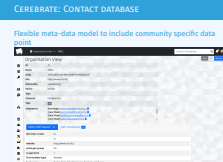
Flexible meta-data model to include community specific data point

The screenshot displays the Cerebrate web application interface. At the top, there's a navigation bar with 'Organisations index' and 'CIRCL'. A search bar is present with the text 'Search in Cerebrate...'. The main content area is titled 'Organisation View' and shows details for the 'CIRCL' organization. The details are organized into sections: 'Basic Information' (ID, Name, UUID, URL, Nationality, Sector, Type), 'Contacts' (info@circl.lu), 'Tags' (a plus button), and 'Alignments' (a list of roles and email addresses). Below these, there's a section for 'ENISA CSIRT Network' and 'CSIRT Constituency' with a table of attributes like 'ISO 3166-1 Code', 'website', 'enisa-geo-group', 'is-approved', 'first-member-type', and 'team-name'.

Attribute	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	[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
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

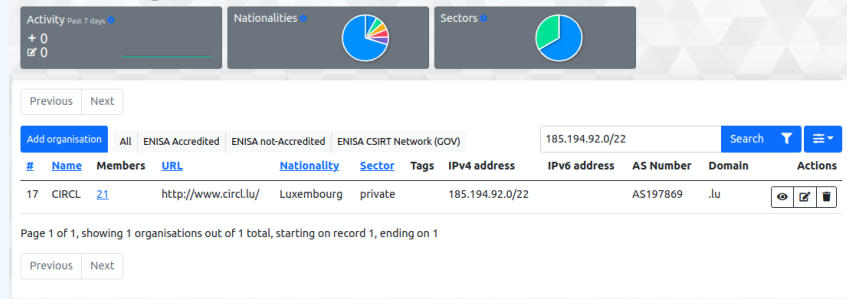
2022-03-21

- Managing information sharing communities
 - Community management and orchestration tool
 - Cerebrate: Contact database

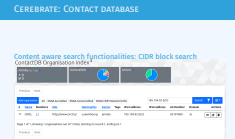


Content aware search functionalities: CIDR block search

ContactDB Organisation Index ⁱ



- Managing information sharing communities
 - Community management and orchestration tool
 - Cerebrate: Contact database



Global searches on a large variety of data point

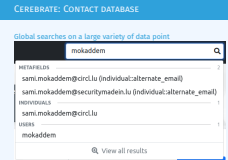
The screenshot shows a search bar with the text 'mokaddem' and a magnifying glass icon. Below the search bar, the results are categorized into three sections: METAFIELDS (2 results), INDIVIDUALS (1 result), and USERS (1 result). The METAFIELDS section lists two email addresses: 'sami.mokaddem@circl.lu (individual::alternate_email)' and 'sami.mokaddem@securitymadein.lu (individual::alternate_email)'. The INDIVIDUALS section lists 'sami.mokaddem@circl.lu'. The USERS section lists 'mokaddem'. At the bottom of the results, there is a link with a magnifying glass icon and the text 'View all results'.

Category	Count	Results
METAFIELDS	2	sami.mokaddem@circl.lu (individual::alternate_email) sami.mokaddem@securitymadein.lu (individual::alternate_email)
INDIVIDUALS	1	sami.mokaddem@circl.lu
USERS	1	mokaddem

[View all results](#)

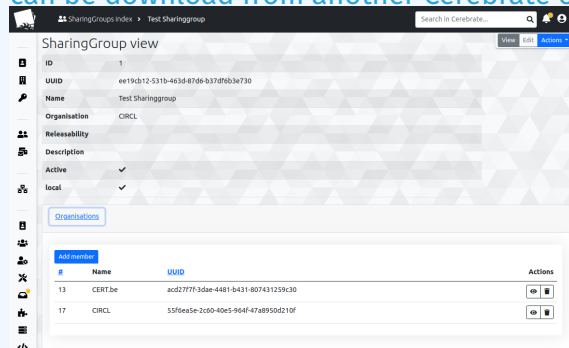
Managing information sharing communities

- Community management and orchestration tool
- Cerebrate: Contact database



CEREBRATE: SHARING GROUP MANAGEMENT

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

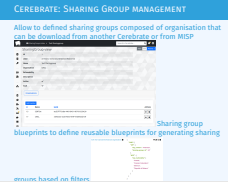


Sharing group blueprints to define reusable blueprints for generating sharing

```
#10: Non-sanctioned financial organisations {
  "AND": {
    "OR": {
      "org_sector": "Financial",
      "sharing_group_id": 127
    },
    "NOT": {
      "org_nationality": [
        "Russia",
        "Russian Federation",
        "Belarus",
        "Republic of Belarus"
      ]
    }
  }
}
```

2022-03-21

Managing information sharing communities
└ Community management and orchestration tool
└ Cerebrate: Sharing Group management



CEREBRATE: SYNCHRONISATION

CEREBRATE-CEREBRATE

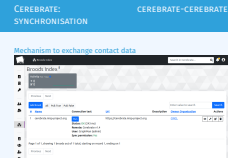
Mechanism to exchange contact data

The screenshot shows the 'Broods Index' interface. At the top, there's a search bar labeled 'Search in Cerebrate...'. Below it, a summary box shows 'Activity Past 7 days' with '+ 0' and '0'. The main table lists broods with columns: #, Name, Connection test, Url, Description, Owner Organisation, and Actions. One brood is listed: 'cerebrate.misp-project.org' with a 'Run' button and status 'OK (243 ms)'. The footer indicates 'Page 1 of 1, showing 1 broods out of 1 total, starting on record 1, ending on 1'.

#	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

2022-03-21

- Managing information sharing communities
 - Community management and orchestration tool
 - Cerebrate: cerebrate-cerebrate synchronisation



CEREBRATE: LOCAL TOOL ORCHESTRATION

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

The screenshot shows the 'LocalTools Index' interface. At the top, there's a search bar labeled 'Search in Cerebrate...'. Below it, the 'Local tool connector index' is displayed. A table lists connectors with columns: Name, Connector, Version, Description, Connections, and Actions. The table shows one entry for 'MISP' with connector 'MispConnector' and version '0.1'. The description states it handles diagnostics, organization, and sharing 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, a table shows the request details: Date (2021-08-11 12:05:11), Tool Name (MISP (v0.1)), Brood (CIRCL cerebrate), Individual (andras.iklody@gmail.com), and Alignment (@ CIRCL.lu). At the bottom, 'Inter-connection data' is shown as a JSON object: { "email": "sync_ef11e9f6@ccerebrate.pilot.melicertes.eu", ... }.

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	

Interconnection Request for MispConnector

Request Sent | Request Accepted | Connection Done

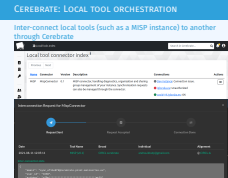
Date	Tool Name	Brood	Individual	Alignment
2021-08-11 12:05:11	MISP (v0.1)	CIRCL cerebrate	andras.iklody@gmail.com	@ CIRCL.lu

Inter-connection data

```
{  "email": "sync_ef11e9f6@ccerebrate.pilot.melicertes.eu",  ...}
```

2022-03-21

Managing information sharing communities
└ Community management and orchestration tool
└ Cerebrate: Local tool orchestration



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

CEREBRATE
PROJECT

2022-03-21

Managing information sharing communities

└ Community management and orchestration tool

└ Use case specific to LE

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

CEREBRATE
PROJECT