Managing information sharing communities

E.103

CIRCL Computer Incident Response Center Luxembourg

MISP Project
https://www.misp-project.org/

March 29, 2022 - v0.7

Managing information sharing communities
E.103
CIRCL Computer Incident Response Center Luxembourg
MISP Project
https://www.misp-project.org/
March 29, 2022 - v0.7

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

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

Joining an information sharing communities

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

Joining an information sharing communities

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

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

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:
  - 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

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

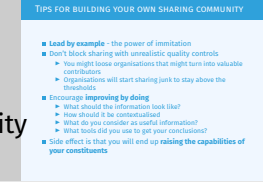
Tips for building your own sharing community

- 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
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 immitation
- Don't block sharing with unrealistic quality controls
  - You might loose 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**



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 possiblity 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

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."

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."

Managing sub-sharing communities

- 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 bootstraping these specific sharing community
  - Organisations can self-organise, but you are probably the ones with the know-how to get them started

Managing sub-sharing communities
- 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 bootstraping 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

Additional challenges of community management

- 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

Additional challenges of community management
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

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?

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

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

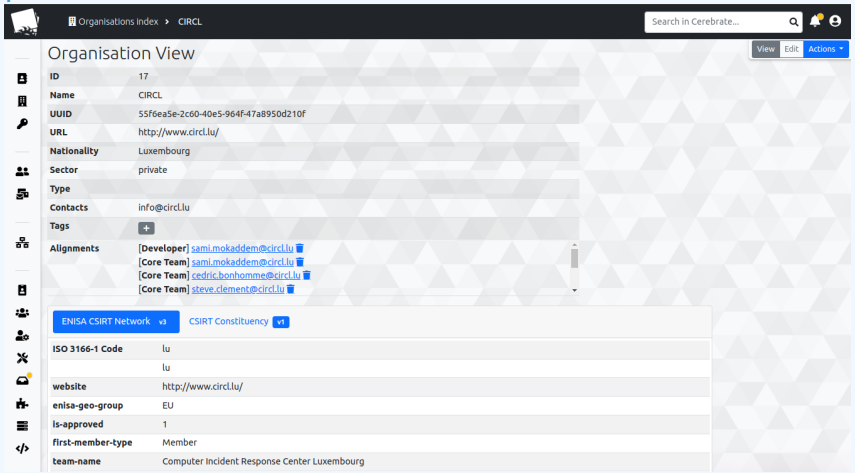
Cerebrate: Contact database

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

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

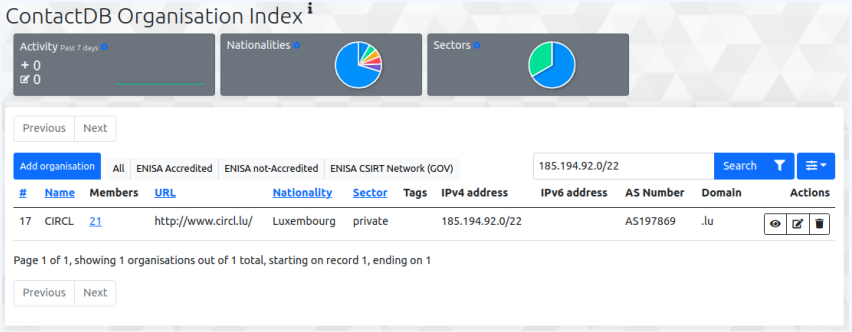


Cerebrate: Contact database
Flexible meta-data model to include community specific data point

1. Cerebrate includes a system to support meta-data that can be attached to existing enties
2. This system is composed of meta-template which defines additional data-point
3. It can be used to create new structure unknown to a default Cerebrate installation

Cerebrate: Contact database

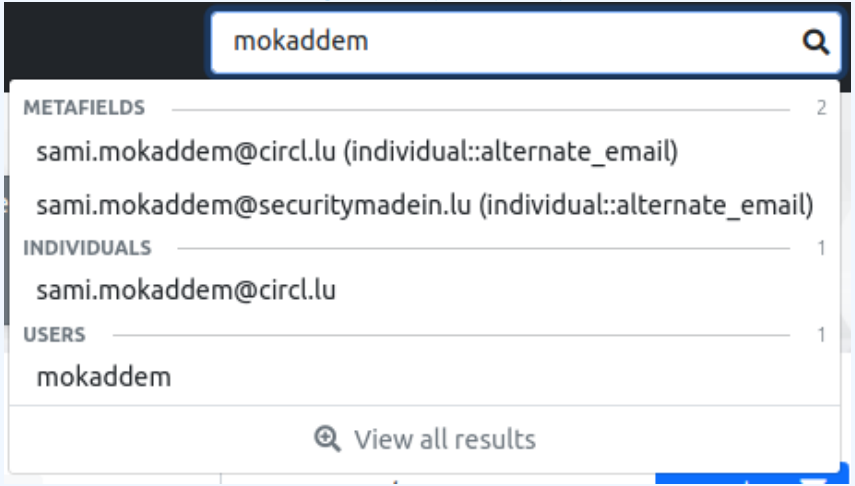
Content aware search functionalities: CIDR block search

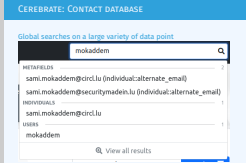


1. The meta-template system also support different data type
2. In this screenshot, we can a search for an IP address and the matching CIDR block is returned

Cerebrate: Contact database

Global searches on a large variety of data point

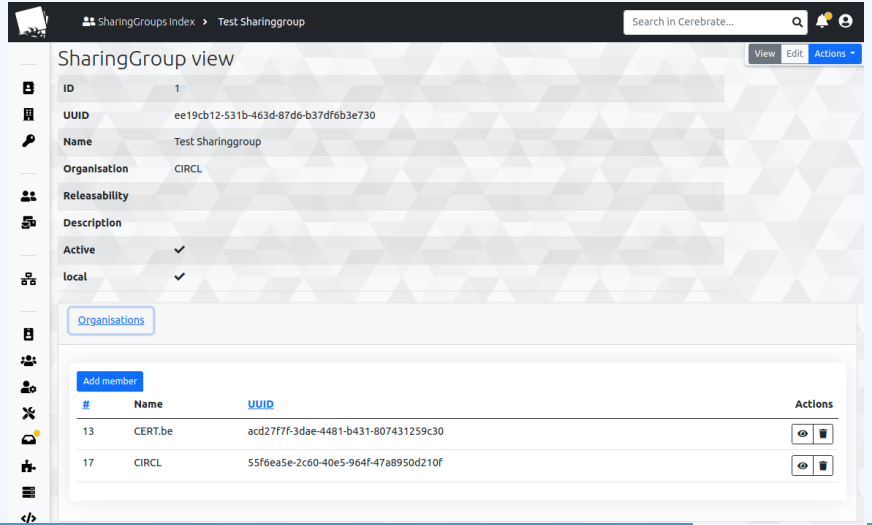


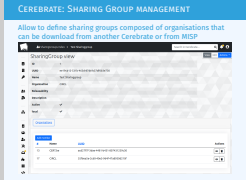


1. The tool allows users to search in a multiple of scope at the same time

Cerebrate: Sharing Group management

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





1. In this screenshot, we can see a sharing group composed of two organisations: CIRCL and cert.be

Cerebrate: Sharing Group management

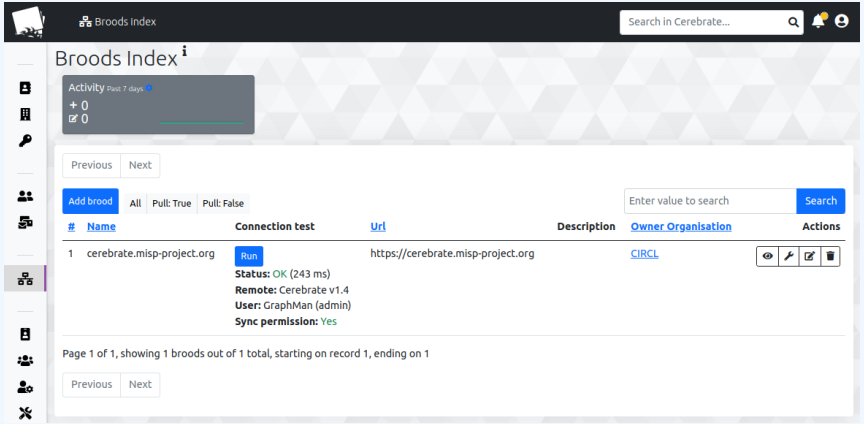
Sharing groups can also be generated based on filters via the reusable blueprints

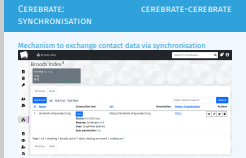
#19: Non-sanctioned financial organisations

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


1. In this screenshot, we can see a sharing group blueprint definition where
2. Organisation of the RU nationality are exluded
3. Organisation from the "Financial" sector are included
4. All organisation contained in the sharing group 127 are included

Mechanism to exchange contact data via synchronisation

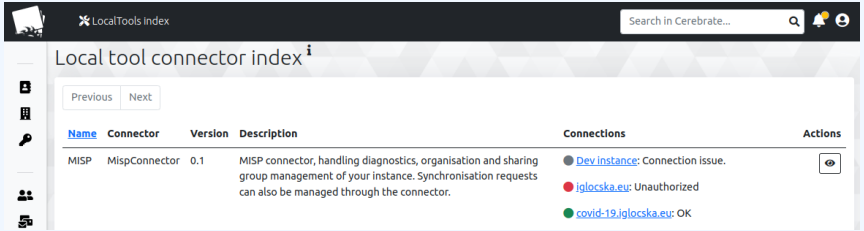


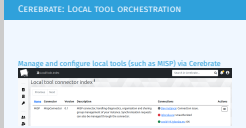


1. Similar to MISP, cerebrate suport data exchange to and from other Cerebrate instances

Cerebrate: Local tool orchestration

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

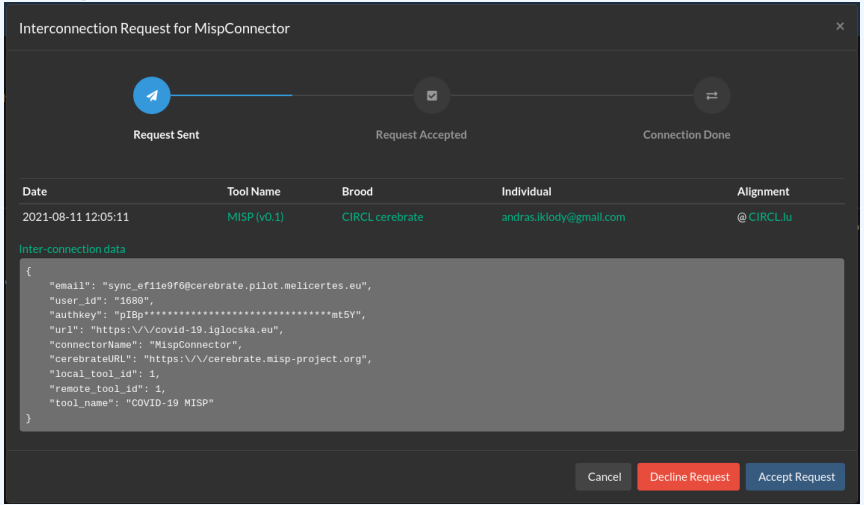


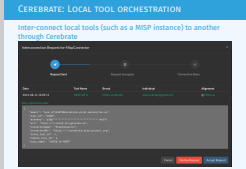


1. The screenshot shows that Cerebrate has a MISP connector
2. This connector is used to control 3 MISP instances where we can see their connection status

Cerebrate: Local tool orchestration

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





1. The screenshot shows a message received from another Cerebrate instance
2. This message request the inter-connection of the local MISP instance with the MISP instance of the remote Cerebrate
3. To have the connection between the two MISP finalized, the user must accept the request, then the initiator must finalize it

Use case specific to law enforcement

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

TODO: Include picture of data stored in Cerebrate

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

TODO: Include picture of data stored in Cerebrate