Cerebrate

Community management and tool orchestration the open-source way

Andras Iklody & Sami Mokaddem

Cerebrate Project

FIRSTCON22
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 performing 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)**

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events</td>
<td>97,680 (+794)</td>
</tr>
<tr>
<td>Attributes</td>
<td>293,786,02 (+678,136)</td>
</tr>
<tr>
<td>Attributes / event</td>
<td>301</td>
</tr>
<tr>
<td>Correlations found</td>
<td>429,309,29</td>
</tr>
<tr>
<td>Proposals active</td>
<td>2,753</td>
</tr>
<tr>
<td>Users</td>
<td>4,171</td>
</tr>
<tr>
<td>Users with PGP keys</td>
<td>2,812 (67.4%)</td>
</tr>
<tr>
<td>Organisations</td>
<td>2,048</td>
</tr>
<tr>
<td>Local Organisations</td>
<td>1,499</td>
</tr>
<tr>
<td>Event creator orgs</td>
<td>600</td>
</tr>
<tr>
<td>Average Users / Org</td>
<td>2.8</td>
</tr>
</tbody>
</table>

**User and Organisation Statistics**

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>User (Total)</td>
<td>4171</td>
</tr>
<tr>
<td>User (Month)</td>
<td>44 ^</td>
</tr>
<tr>
<td>User (Year)</td>
<td>268 ^</td>
</tr>
<tr>
<td>Org Local (Total)</td>
<td>1,499</td>
</tr>
<tr>
<td>Org Local (Month)</td>
<td>15 ^</td>
</tr>
<tr>
<td>Org Local (Year)</td>
<td>70 ^</td>
</tr>
<tr>
<td>Org External (Total)</td>
<td>549</td>
</tr>
<tr>
<td>Org External (Month)</td>
<td>4 ^</td>
</tr>
<tr>
<td>Org External (Year)</td>
<td>102 ^</td>
</tr>
</tbody>
</table>
Some stats about one of our MISP instance: MISPPriv (2)
Rising number of communities is great!

- **Bridge the gap** 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)
    - #FIRSTCON22 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

<table>
<thead>
<tr>
<th>ID</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>UUID</td>
<td>55f6ea5e-2c60-40e5-964f-47a8950d210f</td>
</tr>
<tr>
<td>Local or remote</td>
<td>Local</td>
</tr>
<tr>
<td>Description</td>
<td>CIRCL is the CERT (Computer Emergency Response Team/Computer Security Incident Response Team) for the private sector, communes and non-governmental entities in Luxembourg.</td>
</tr>
</tbody>
</table>
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)
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!
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

- 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
Built with tool integration in mind, acting as a contact database

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, ...
### ContactDB Organisation Index

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Members</th>
<th>URL</th>
<th>Nationality</th>
<th>Sector</th>
<th>IPv4 address</th>
<th>IPv6 address</th>
<th>AS Number</th>
<th>Domain</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>CIRCL</td>
<td>21</td>
<td><a href="http://www.circl.lu/">http://www.circl.lu/</a></td>
<td>Luxembourg</td>
<td>private</td>
<td>185.194.92.0/22</td>
<td></td>
<td>AS197869</td>
<td>.lu</td>
<td></td>
</tr>
<tr>
<td>316</td>
<td>CYBER CIRCLE CSIRT</td>
<td>0</td>
<td>Public website not available</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th></th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>team</td>
<td>CIRCL</td>
</tr>
<tr>
<td>team-full</td>
<td>CIRCL - Computer Incident Response Center Luxembourg</td>
</tr>
<tr>
<td>host</td>
<td>security made in Lëtzeburig&quot; (SMILE) g.i.e.</td>
</tr>
<tr>
<td>establishment</td>
<td>2008-01-05</td>
</tr>
<tr>
<td>address</td>
<td>CIRCL - Computer Incident Response Center Luxembourg c/o smile - &quot;security made in Letzeburg&quot; GIIE 16, bd d’Avanches L-1160 Luxembourg</td>
</tr>
<tr>
<td>country</td>
<td>Luxembourg</td>
</tr>
<tr>
<td>website</td>
<td><a href="https://www.circl.lu/">https://www.circl.lu/</a></td>
</tr>
<tr>
<td>email</td>
<td><a href="mailto:info@circl.lu">info@circl.lu</a></td>
</tr>
<tr>
<td>timezone</td>
<td>GMT+1</td>
</tr>
<tr>
<td>operating-hours</td>
<td>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)</td>
</tr>
<tr>
<td>constituency</td>
<td>Government, Private and Public sectors</td>
</tr>
<tr>
<td>constituency-description</td>
<td>CIRCL is the CERT for the private sector, communes and non-governmental entities for the Grand Duchy of Luxembourg.</td>
</tr>
<tr>
<td>member-since</td>
<td>May 29, 2014</td>
</tr>
</tbody>
</table>

This meta-template contains 13 meta-fields
Cerebrate’s Contact Database: Meta-Fields

**MetaTemplate view**

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Multiple values</th>
<th>Validation regex</th>
<th>Field Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>first-id</td>
<td>text</td>
<td>x</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>team</td>
<td>text</td>
<td>x</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>team-full</td>
<td>text</td>
<td>x</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>host</td>
<td>text</td>
<td>x</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>establishment</td>
<td>date</td>
<td>x</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>address</td>
<td>text</td>
<td>x</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>
Cerebrate’s Contact Database: Meta-fields
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
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 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
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

### Broods Index

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Connection test</th>
<th>Description</th>
<th>Owner Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>cerebrate.misp-project.org</td>
<td>Run</td>
<td><a href="https://cerebrate.misp-project.org">https://cerebrate.misp-project.org</a></td>
<td>CIRCL</td>
</tr>
<tr>
<td>2</td>
<td>cerebrate.pilot.melicertes.eu</td>
<td>Run</td>
<td><a href="https://cerebrate.pilot.melicertes.eu">https://cerebrate.pilot.melicertes.eu</a></td>
<td>CSIRT.SK</td>
</tr>
<tr>
<td>3</td>
<td>Self</td>
<td>Run</td>
<td><a href="http://172.19.0.5:80">http://172.19.0.5:80</a></td>
<td>CIRCL</td>
</tr>
<tr>
<td>4</td>
<td>Pilot 2</td>
<td>Run</td>
<td><a href="https://cerebrate.pilot.melicertes.eu/">https://cerebrate.pilot.melicertes.eu/</a></td>
<td>CIRCL</td>
</tr>
<tr>
<td>5</td>
<td>localhost-test</td>
<td>Run</td>
<td><a href="http://localhost:8080/">http://localhost:8080/</a></td>
<td>CIRCL</td>
</tr>
</tbody>
</table>

Page 1 of 1, showing 5 broods out of 5 total, starting on record 1, ending on 5.
## Data Sharing

### Sheer Brood View

- **ID**: 1
- **Name**: cerebrate.misp-project.org
- **URL**: https://cerebrate.misp-project.org
- **Description**:
- **Owner**: CIRCL

### Organisation Index

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>UUID</th>
<th>URL</th>
<th>Nationality</th>
<th>Sector</th>
<th>Type</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CIRCL</td>
<td>80658fac879c-4a8b-8422-736a5f6fb2f6</td>
<td><a href="http://www.circl.lu/">http://www.circl.lu/</a></td>
<td>Luxembourg</td>
<td>Private</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>AKCESK/NAECCS</td>
<td>b9587990-016f-4a4f-82b1-bfe7e63a0d66</td>
<td><a href="https://cesk.gov.cz/">https://cesk.gov.cz/</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>ASNET-CERT</td>
<td>abd33501-36b2-d4b4-ae3c-d44045c130fc</td>
<td>Public website not available</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>CERT-AM</td>
<td>e56e2c47-d627-41e5-a493-d7913f1b7310</td>
<td>Public website not available</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>ACOnet-CERT</td>
<td>b055e352-0d05-4d04-a1c2-e7826f17214</td>
<td><a href="https://cert.aco.net/">https://cert.aco.net/</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>AEC</td>
<td>3176207b-4383-4f59-baa5-53295d2fe4f7</td>
<td><a href="https://www.energy-cert.at">https://www.energy-cert.at</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>CERT.at</td>
<td>3f1008d8-2307-46b1-84fd-94a7e3331f7</td>
<td><a href="https://www.cert.at">https://www.cert.at</a></td>
<td>Austria</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>FREQUENTIS SIRT</td>
<td>7c99b5d-bef6-4708-810d-257fd330e575</td>
<td><a href="https://www.frequentis.com">https://www.frequentis.com</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>GovCERT Austria</td>
<td>bbb09520-da04-4e13-8561-71f01bf2325</td>
<td><a href="https://www.gocert.eu.at">https://www.gocert.eu.at</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Two synchronisation strategies:

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

iglocska.eu control panel using MispConnector

**ID**: 2

**Name**: iglocska.eu

**Connector**: MispConnector

**Exposed**: 

**settings**

```
{  
  "url": "https://iglocska.eu",
  "authkey":
}
```

**Description**

ServerSettings

Organisations

<table>
<thead>
<tr>
<th>Name</th>
<th>uuid</th>
<th>nationality</th>
<th>sector</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-FUNKY-HUNGARIAN-BANK.hu</td>
<td>5d8a16d4-0bdc-4c24-bc0b-3c8aa5e38e14</td>
<td>Hungary</td>
<td>Financial</td>
<td></td>
</tr>
<tr>
<td>AFB</td>
<td>5d6e3320-6bd0-49dc-b0fe-5829a5e38e14</td>
<td>France</td>
<td>Financial</td>
<td></td>
</tr>
<tr>
<td>BICES</td>
<td>d5c12eb5-4a0e-41f3-b78f-99ee86a3b8da</td>
<td>International</td>
<td></td>
<td></td>
</tr>
<tr>
<td>camichel.com</td>
<td>59b3cea5-a9e8-414d-b6af-064cc0a80112</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CERN</td>
<td>56c4a555-3178-418e-b774-4e94bcb8b8ee</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CERT Polska</td>
<td>5db98ff5-1554-4d88-88d5-4c43950d2111</td>
<td>Poland</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CERT POLSKA</td>
<td>06c3bc02-9619-40a0-8a7a-bc31bddd60fa</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

### Local tool connector index

<table>
<thead>
<tr>
<th>Name</th>
<th>Connector</th>
<th>Version</th>
<th>Description</th>
<th>Connections</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>MISP</td>
<td>MispConnector</td>
<td>0.1</td>
<td>MISP connector, handling diagnostics, organisation and sharing group management of your instance. Synchronisation requests can also be managed through the connector.</td>
<td><img src="https://example.com" alt="Dev instance" /> Connection issue. <img src="https://example.com" alt="Iglocskaj.eu" /> OK</td>
<td><img src="https://example.com" alt="iGlocskaj.eu" /> OK</td>
</tr>
</tbody>
</table>

Page 1 of 1, showing 1 organisations out of 1 total, starting on record 1, ending on 1.
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.
Cerebrate can leverage its access to local tool to reach out to tools from other Cerebrate nodes
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

MY DEAR, COULD YOU PROVIDE ME WITH ACCESS TO YOUR MISP?

IT WOULD BE MY PLEASURE. HERE YOU GO.

MUCH APPRECIATED.
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.lkody@gmail.com @CIRCL.lu

Inter-connection data

{
   "email": "sync_ef11e9f6@cerebrate.pilot.melocytes.eu",
   "user_id": "1686",
   "authkey": "piBp**************m5Y",
   "url": "https://\ covid-19.iglocsa.eu",
   "connectorName": "MispConnector",
   "cerebrateURL": "https://\ cerebrate.misp-project.org",
   "local_tool_id": 1,
   "remote_tool_id": 1,
   "tool_name": "COVID-19 MISP"
}
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)
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!