## MANAGING INFORMATION SHARING COMMUNITIES

E.103

CIRCL COMPUTER INCIDENT RESPONSE CENTER LUXEMBOURG



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

MARCH 29, 2022 - VO.7

### Managing information sharing communities

ANAGING INFORMATION SHARING MMUNITIES

----

COMPUTER INCIDENT RESPONSE CENTER LUXEMBOUR



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

#### **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

Managing information sharing communities

-Objectives of this module

Tool for managing a sharing community

Tips for joining information sharing communities

2022-

# BEING PART OF AN INFORMATION SHARING COMMUNITY

Managing information sharing communities

Being part of an information sharing community

ART OF AN INFORMATIO 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

Managing information sharing communities

Being part of an information sharing community

-Joining an information sharing communities

OINING AN INFORMATION SHARING COMMUNITIES

is a wide range of MISP communities type: ivate sector communities

- ➤ Private organisations, researchers, central hub
- Central hub for sectorial or geographical Communities
   Examples: GSMA, FIRST.org, CSIRT Network, Banking, etc.
- ➤ Often use for exercises such as ENISA

#### 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

Managing information sharing communities

Being part of an information sharing community

-Joining an information sharing communities

 Defense, prevention, collaboration, research, specific reporting duties
 Make sure the use-cases are not conflicting

False-positive appetite, maturity levels, topical interest
 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

Managing information sharing communities Being part of an information sharing community

> Tips for being a good member of a sharing community

- Validating data (sightings) or flagging false positives Asking for support from the communit

- 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

Managing information sharing communities

Being part of an information sharing community

Tips for building your own sharing community

IPS 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
- Planning ahead for future growth
- Estimating requirements (workfo
- Estimating requirements (worknorce, naroware requirement)
   Deciding early on common vocabularies (i.e. taxonomies)
   Offering conince through MISP to nonmote adhesion

- **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 **vour constituents**

Managing information sharing communities Being part of an information sharing community

Tips for building your own sharing community

- - Side effect is that you will end up raising the capabilities

- 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

Managing information sharing communities

Being part of an information sharing community

Tips for building your own sharing community

Lead by example
 Give credit where credit is due
 Meve state the contribution of your community
 Offices the possibility to take over their data via delegation
 Anonymity of organizations might help then building confidence at the beginning

- 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

Managing information sharing communities

Being part of an information sharing community

Lips for building your own sharing community

FOR BUILDING YOUR OWN SHARING COMMUNITY

Encourage sharing of supporting materials, scripts or
 suidance for protection

 Raise awareness about the benefits of a well modelled, graph-based information

Again, context is king! If possible, make contextualisati requirement

Users can then niter based on their needs
 Classification help your peers to understand why the important

And also, why this data can be useful to them

R

### 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 information sharing communities

Being part of an information sharing community

-Dispelling the myths around blockers when it comes to information sharing

ING THE MYTHS AROUND BLOCKERS WHEN IT O INFORMATION SHARING

- naring diministrates are not really technical issues but o '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

   "Burk of information look is too bight and iffs too sinks for o
- "Risk of information leak is too high and it's too risky for organization or partners."
   Practical restrictions
- "We don't have information to share."

  "We don't have time to process or contribution."
- "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 form.

q

#### 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 information sharing communities

—Being part of an information sharing community

-Managing sub-sharing communities

AGING SUB-SHARING COMMUNITIES

sharing will form

• e.g. Within a national private sector community, a dedicar community for financial institutions

► If an incident involves multiple organisations

f you are building your own community, consider cootstraping these specific sharing community

ing these specific sharing community isations can self-organise, but you are probably th with the know-how to get them started

# **COMMUNITY MANAGEMENT AND OR- CHESTRATION TOOL**

Managing information sharing communities

—Community management and orchestration tool

TY MANAGEMENT AND OF

**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

Managing information sharing communities Community management and orchestration tool -Additional challenges of community management

#### 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

Managing information sharing communities —Community management and orchestration tool

-What is Cerebrate?

WHAT IS CEREBRATE?

CESSERATE

- Open source community management and orchestration
  col
- Project for the CSIRT network building a common set of too and services for the national CSIRTs
- and services for the national CSIRTs

  Flexible to support a wide range of communities
- Tight integration with various open-source tool
   Planned as the primary MISP management tool

## WHY DO WE NEED CEREBRATE FROM A MISF 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?

Managing information sharing communities

—Community management and orchestration tool

-Why do we need Cerebrate from a MISP perspective

DO WE NEED CEREBRATE FROM A MISP CTIVE

- # Deficiencies in our current tool chain
  - chains to onboard new members?

    How do I find trusted information on who an organisation
- How can I manage a large cluster of MISPs without tedior manual labour?
- member information for other community tasks such a
- mailing lists?

  Information signing has been on the MISP roadmap for a long

#### 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

Managing information sharing communities

Community management and orchestration tool

► Cryptographic key tookup for information signing.
 Local tool management.
 ► Instrumentation of local tool interconnections.
 ► Local tool fleet management.

-What issues is Cerebrate trying to tackle? • Introduction of local table intercent. • In the control of the co

#### **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

Managing information sharing communities Community management and orchestration tool

2022

-Cerebrate: What is available currently?

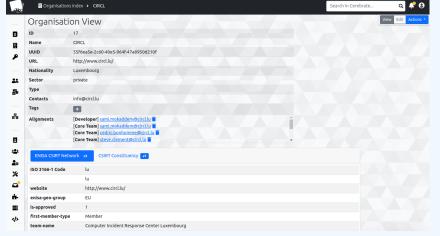
- Index of Organisations and Individuals
- Flexible meta-data model (community specific, constituency, etc)
- Content aware search functionalities

Managing information sharing communities

Community management and orchestration tool

Cerebrate: Contact database

Flexible meta-data model to include community specific data point



Managing information sharing communities —Community management and orchestration tool

Testable meta-data model to include community specific data.

-Cerebrate: Contact database

- 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

### Content aware search functionalities: CIDR block search ContactDB Organisation Index i



 $\begin{tabular}{ll} \textbf{Managing information sharing communities} \\ \begin{tabular}{ll} \textbf{L} \\ \begin{tabular}{ll} \textbf{Community management and orchestration tool} \\ \end{tabular}$ 

CONTROL CONTRO

—Cerebrate: Contact database

- 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

Global searches on a large variety of data point

	mokaddem	Q
i	m@circl.lu (individual::alternate_email) m@securitymadein.lu (individual::alternate_ema m@circl.lu	- 2 ail) - 1
	ℚ View all results	

Managing information sharing communities —Community management and orchestration tool

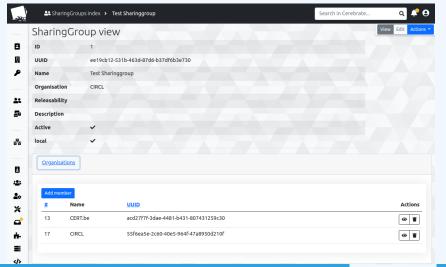
-Cerebrate: Contact database



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



Managing information sharing communities —Community management and orchestration tool

All the second of the second o

—Cerebrate: Sharing Group management

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
                                                                                   ④ぼ讼盲
                                                  "AND": {
                                                    "OR":
                                                       "org sector": "Financial",
                                                       "sharing group id": 127
                                                    "NOT": {
                                                       "org nationality": [
                                                         "Russia".
                                                         "Russian Federation",
                                                         "Belarus",
                                                         "Republic of Belarus"
```

Managing information sharing communities

—Community management and orchestration tool

Sharing groups can also be generated based on filters via the restable biosprints

as to be accessed that or parameter and the state of the state of

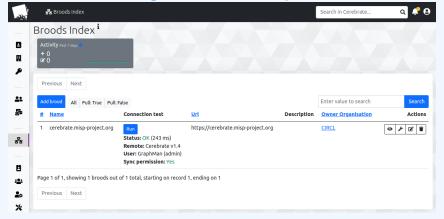
—Cerebrate: Sharing Group management

- 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

## CEREBRATE: SYNCHRONISATION

#### CEREBRATE-CEREBRATE

#### Mechanism to exchange contact data via synchronisation



Managing information sharing communities

—Community management and orchestration tool

I fam (menterint at franche (manipulation Ad-					WITTENAM.	,
The state of the s	Broods Index.*					
The control of the co	Reference to the State of Stat					
In the Contract of the Contr	Wi					
In the Contract of the Contr						
Insection Sequence						
andrea representar     andrea representa	MARKET OF REPORT AND	No				100
International In		(menuter less	w	Drawlyden	Description in	Alle
Associa (indistrict) (and (ingline)) (by promobile (in Associal Conting 1 produced of 1645) deling commet (continger)	1 and compared by		Mys/sedent representati		010.	
Spa permitter in Space of Celebra Space and Falsi, delay arrange Celebrary						
Aspert of Culturing 1 breaks and 4 total during arrespect Conditions 1		THE STATE OF STREET				
	Aspell of Caloning 1 broads and	of Table during remon	Contingent			

synchronisation

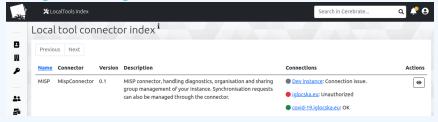
-Cerebrate: cerebrate-cerebrate

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

03-29

#### **CEREBRATE: LOCAL TOOL ORCHESTRATION**

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



 $\begin{tabular}{ll} \textbf{Managing information sharing communities} \\ \begin{tabular}{ll} \textbf{L} \\ \begin{tabular}{ll} \textbf{Community management and orchestration tool} \\ \end{tabular}$ 

Manage and configure local tools (such as MISS) via Constrain

Manage and configure local tools (such as MISS) via Constrain

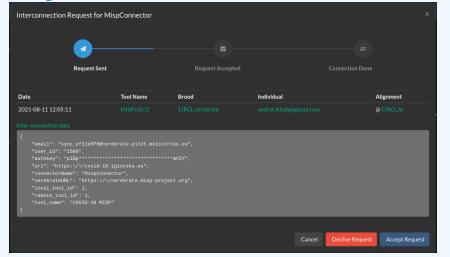
Team of the Constraint Constraint Constraint Constraint Constraint Constraint Constraint Cons

Cerebrate: Local tool orchestration

- 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



Managing information sharing communities —Community management and orchestration tool

There connect focat does focus as a MSP instance) to another storage of the second sec

—Cerebrate: Local tool orchestration

- The screenshot shows a message received from another Cerebrate instance
- 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

Managing information sharing communities Community management and orchestration tool

-Use case specific to law enforcement