



Documentation formalizing information sharing and cooperation activities

Version: 1.0

Date: 30/08/2021

Information

Title	Documentation formalizing information sharing and cooperation activities
Classification	LX-Internal
Type	Policy
Distribution List	LU-CIX Internal
Owner	ndebeffe

History

Version	Who	Date	Reasons of modifications
0.1	ndebeffe	02/07/2021	Documentation formalizing information sharing and cooperation activities - Initial draft version
0.2	gwagener, adulaunoy, adeoliveira, vmammadzada, nsalash.	26/08/2021	Documentation formalizing information sharing and cooperation activities - Reviewed version
1.0	ndebeffe	30/08/2021	Initial version

Table of content

INFORMATION	2
HISTORY.....	2
TABLE OF CONTENT	3
1. INTRODUCTION	4
1.1 GENERAL INFORMATION ABOUT PISAX	4
1.2 WHY DO WE NEED INFORMATION SHARING?.....	4
1.3 DOCUMENT OBJECTIVE	4
1.4 TERMS USED IN THE POLICY PARTS OF THE DOCUMENTATION	4
2. STEPS TO SETUP AN INFORMATION SHARING COMMUNITY	5
2.1 THE SIX SUGGESTED STEPS	5
3. GOALS AND FOUNDATION	6
3.1 GOVERNANCE	6
3.2 MEMBER ONBOARDING PROCEDURE.....	8
4. ORGANIZATION	10
4.1 SERVICE OFFERING.....	10
4.2 OPERATING MODEL	10
4.3 BUSINESS MODEL.....	10
5. SHARING RULES	11
5.4 INFORMATION EXCHANGE POLICY	11
5.5 PARTNERSHIPS AND SUPPORT	13
6. MECHANISMS AND TOOLS.....	15
6.1 INFORMATION COLLECTION AND DISSEMINATION STANDARDS AND BEST PRACTICES	15
6.2 SHARING MODEL AND MECHANISM.....	16
7. SECURITY AND COMPLIANCE	17
7.1 SECURITY REQUIREMENTS.....	17
7.2 COMPLIANCE REQUIREMENTS	17
8. FOLLOW-UP AND IMPROVEMENT	18
8.1 MEASURE EFFECTIVENESS OF SHARING	18
8.2 EVALUATE MEMBERS NEEDS	18

1. INTRODUCTION

1.1 General information about PISAX

The Action's overall objective is to create a common pan-European Information Sharing and Analysis Center (ISAC) to support Internet Exchange Points (IXPs) and General Packet Radio Service Roaming eXchange (GRXs) at the national, European and international level.

IXPs are the infrastructures connecting Internet Service Providers in a country or across countries. GRXs are also connecting network systems but focus on connecting Roaming networks. The ISAC (hereby referred to as "PISAX") aims at gathering the maximum IXPs and GRXs organisations.

The Action will provide an automated and secure threat intelligence sharing system for these entities building on the existing Malware Information Sharing Platform (MISP) hence improving their current security posture.

The development of the scripts and MISP enhancements in order to guarantee maximum automation are released in open source.

1.2 Why do we need Information sharing?

Malicious cyber actors are becoming more organized, smarter, and more sophisticated, which is rendering traditional defense methods and tools less effective in dealing with new threats appearing. One solution to this problem is the sharing of information about cyber threats and incidents. This helps to prevent major security incidents from recurring and emerging threats from claim.

1.3 Document objective

The objective of the document is to formalize information sharing and cooperation's activities around the pan-European Information Sharing and Analysis Center dedicated to Internet exchange points (IXPs) and General Packet Radio Service Roaming eXchange (GRXs) called PISAX. The current document is based on the guideline for setting up an information sharing community that can be found at the following link:

https://www.x-isac.org/assets/images/guidelines_to_set-up_an_ISAC.pdf

1.4 Terms used in the policy parts of the documentation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Note that the force of these words is modified by the requirement level of the document in which they are used.

MUST This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

MUST NOT This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

SHOULD This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood, and the case carefully weighed before implementing any behavior described with this label.

2. Steps to setup an information sharing community

2.1 The six suggested steps

The following infographic describes six suggested steps to set up an information sharing community, including the recommended documentation to be drafted. These steps will serve as a framework of the present document. Each step will be further described and expanded in the following chapter:



3. Goals and foundation

3.1 Governance

3.1.1 Vision, mission, and objectives

The vision of the pan-European Information Sharing and Analysis Center (PISAX) is to become a key platform for cooperation on cybersecurity matters between Internet Exchange Points (IXPs), General Packet Radio Service Roaming exchanges (GRXs) and professionals or organizations involved in Information security.

PISAX's mission is to promote cybersecurity defense and response within IXPs and GRXs at the national, European and international level. The mission is conducted through private information sharing within a community of trusted representatives at member organizations, and active role on improving the security of IXPs and GRXs.

The objectives of the pan-European Information Sharing and Analysis Center (PISAX) are to:

- Improve internal capabilities of IXP/GRX to meet security and reporting requirements under national laws implementing the NIS Directive.
- Facilitate the collaboration on threat intelligence and analysis of technical and non-technical information about malware and attacks on PISAX members.
- Enable the automatic sharing of indicators of compromise (IoC) by developing interfaces between PISAX members utilizing the MISP threat sharing platform to improve the security posture.
- Join a European Level Sectoral ISAC to enhance the cross-sectoral sharing.

3.1.2 Legal structure

PISAX is a cooperation between POST, a private company, and two Economic Interests groups: LU-CIX GIE and SECURITYMADEIN.LU. All entities are members of LU-CIX GIE. The sharing platform is hosted at SECURITYMADEIN.LU G.I.E.. There is no need to create a dedicated legal structure for PISAX.

3.1.3 Type of agreements on information sharing

Information sharing is intrinsically about communication between parties, and communication usually involves some kind of agreement(s) to enable the involved parties to understand each other. In existing information sharing communities and specifically ISACs, different options may be considered to formalise those information sharing agreements. The chosen type of agreement in the context of the pan-European Information Sharing and Analysis Center (PISAX) is based on a **“Gentlemen’s agreement”** as described below:

A “Gentlemen’s agreement” is an informal agreement that is based on trust of the members of the organisation. It does not require any formalisation and is usually communicated orally. It is important to highlight the difference of the gentlemen’s agreement and a common verbal agreement (contract) that is legally binding.

3.1.4 Consequences for non-compliance with the information sharing community rules

Currently not applicable, apart from:

- the consequences of not respecting the TLP rules, in which case the access to the platform will be blocked.
- the consequences of not respecting the Licensing rules, in which case the organization not respecting the rules will be cancelled after a first warning.

3.1.5 Termination clause

Currently not applicable

3.1.6 Organization

PISAX is composed of volunteer members that share the workload of the community to improve the capabilities of each individual group member. Every member of the PISAX community can volunteer to lead the organisation’s meetings (e.g. by hosting a meeting themselves), while ensuring that the host role is rotated to the other members of the community.

3.1.7 Acceptance criteria of new members and plan for future growth

The criteria for joining the sharing community are the following:

- Being an Internet eXchange Point at the national, European or international level.
- Being a General Packet Radio Service Roaming eXchange at the national, European or international level.

During the requirements gathering and the feedback from the initial proof-of-concept using MISP, there was significant interest from the LIRs¹ that often share common network infrastructure via interconnection services on IXPs/GRXs. The objective of sharing threat intelligence helped not only the IXPs/GRXs but also the interconnecting members having interconnected/shared infrastructure.

In this scope, PISAX.org has extended the vetting process of on-boarding new members to include LIR, which can benefit from the same information in order to improve the security of their interconnecting infrastructure.

3.1.8 Marketing and communications strategy

Information about PISAX will be disseminated through the participation in events targeting:

- IXP representative of European countries:
 - Euro-IX; Peering Forum.
 - Réseaux IP Européens.
 - RIPE meetings.
- GRX representatives of several European countries:
 - Global System for Mobile Communications – GSMA.
 - International Telecommunication Union - ITU.

Information about PISAX will also be disseminated through:

- social media (LinkedIn, twitter, etc.).
- direct mailing to IXPs and GRXs.
- the PISAX website (<https://www.pisax.org>) or other dissemination means (e.g. F.A.Q, technical documentation, presentations, github code link).

PISAX is now an official MISP community in the MISP core software and any user of MISP can see PISAX in the community list and can request access to PISAX.

In addition, PISAX is in the process of joining a relevant European Level Sectoral ISAC and participates in events organised by the ISAC's facilities manager (set-up by the European Commission). PISAX participates in relevant stakeholder forums set-up by the European Commission.

¹ LIR: A member of a Regional Internet Registry (RIR). The RIPE NCC refers to most of its members as LIRs. An LIR distributes IP addresses to End Users and/or uses them in its own infrastructure.

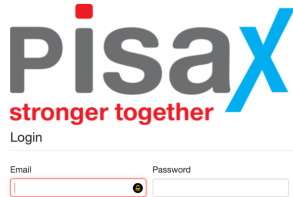
3.2 Member onboarding procedure

3.2.1 Self-registration step

The onboarding procedure is simple; the new member (which must belong to an Internet exchange point, a GPRS Roaming exchange or Local Internet registry community) must connect to the PISAX platform:

<https://misp.pisax.org>

- At the login prompt – <https://misp.pisax.org>



- There is an Hyperlink : **Register Now!**

[No account yet? Register now!](#)

The new member then fills in the requested information and clicks on the **submit** button

Register for a new user account

If you would like to send us a registration request, please fill out the form below. Make sure you fill out as much information as possible in order to ease the task of the administrators. Please add the IXP or GRX you are working for in the free-text comment

Your email address

Your organisation's name (optional)

Your MISP org uuid (optional)

Request custom role

PGP key (optional)

Message to the admins

https://www.lu-cix.lu/"/>

In the “message to the admin” field, it is recommended that the new member enters information about the community to which they belong and:

- Internet exchange point information
- GPRS Roaming exchange information
- Local Internet Registry information

This information will help the administrator in the validation process.

3.2.2 Validation step

After the new member has finalized the self-registration process, a MISP platform administrator must validate the request.

4. Organization

4.1 Service Offering

PISAX provides an automated and secure threat intelligence sharing system built on the open-source MISP threat sharing platform. Given that MISP threat sharing platform is a mature and popular tool already used by various organisations across the world, the security and privacy aspects of the PISAX platform is battle tested and continues to improve due to an active community around it.

4.1.1 Service offered additionally to sharing

Currently, there are no additional services offered by the pan-European Information Sharing and Analysis Center (PISAX).

4.2 Operating model

4.2.1 Type of ISAC / Information sharing community

Information sharing communities can be categorized according to two main axes: (1) whether the information sharing community is limited to one sector or it is crossing sectors, and (2) its geographical scope (e.g. country focused, EU, international scope).

The pan-European Information Sharing and Analysis Center (PISAX) is a **cross sector ISAC** dedicated to Internet eXchange points (IXPs), GPRS Roaming exchanges (GRXs) and Local Internet Registries (LIR) across Europe.

4.3 Business model

4.3.1 Funding model

The setup of the pan-European Information Sharing and Analysis Center (PISAX) was based on a Connecting Europe Facility funding program:

AGREEMENT No INEA/CEF/ICT/A2018/1818230

The Connecting Europe Facility (CEF) is a key EU funding instrument to promote growth, jobs and competitiveness through targeted infrastructure investment at European level. It supports the development of high performing, sustainable and efficiently interconnected trans-European networks in the fields of transport, energy and digital services. The CEF investments fill the missing links in Europe's energy, transport and digital backbone.

The CEF funding was received in order to support the PISAX initiative. The grant stopped on August the 31st 2021.

After the CEF grant, CIRCL (hosted by SECURITYMADEIN.LU) will ensure the sustainability of the PISAX sharing community along with partners such as LU-CIX GIE and POST Luxembourg.

SECURITYMADEIN.LU is financed by the Grand Duchy of Luxembourg. The financing details and mission statement of SECURITYMADEIN.LU is established by a 5-year agreement² signed between the G.I.E. and its supervisory ministry, the Ministry of the Economy.

The funding is in line with the Luxembourg security strategy.³

4.3.2 Funding mechanisms

The pan-European Information Sharing and Analysis Center (PISAX) is a joint initiative open to international contribution.

² https://securitymadein.lu/images/convention-pluriannuelle_2020-2025_meco-smile_web.pdf

³ <https://defense.gouvernement.lu/dam-assets/la-defense/Luxembourg-Cyber-Defence-Strategy.pdf>

5. Sharing rules

5.4 Information exchange policy

According to the FIRST Information Exchanged Policy framework⁴, an information exchange policy can include four parts:

- **Handling policy** statements define any obligations or controls on information received to ensure the confidentiality of information that is shared.
- **Action policy** statements define the permitted actions or uses of the information received that can be carried out by a recipient.
- **Sharing policy** statements define any permitted redistribution of information that is received. For example, enforcing dissemination marking such as TLP. Also, the sharing policy can define in which case information sharing is mandatory or voluntary.
- **Licensing policy** statements define any applicable agreements, licenses, or terms-of-use that govern the information being shared.

5.4.1 Handling Policy - Obligations or controls on information received

5.4.1.1 Encryption in transit

Policy Statement	Encryption in transit
Policy Description	States whether the received information must be encrypted when it is retransmitted by the recipient.
Policy Enumerations	Recipients MUST encrypt the information received when it is retransmitted or redistributed.

5.4.1.2 Encryption at rest

Policy Statement	Encryption at rest
Policy Description	States whether the received information must be encrypted by the recipient when it is stored at rest.
Policy Enumerations	Recipients MAY encrypt the information received when it is retransmitted or redistributed.

⁴ https://www.first.org/iep/FIRST_IEP_framework_1_0.pdf

5.4.2 Action Policy - What the information shared can be used for

5.4.2.1 Permitted actions

Policy Statement	Permitted actions
Policy Description	States the permitted actions that Recipients can take with the information received.
Policy Enumerations	<p>INTERNALLY VISIBLE ACTIONS</p> <p>There is no restriction on actions that recipients can take on PISAX information, except if the creator sets a PAP (Permissible Actions Protocol) Tag label⁵.</p>

5.4.2.2 Affected party notification

Policy Statement	Affected party notification
Policy Description	Recipients are permitted to notify affected third parties of a potential compromise or threat.
Policy Enumerations	Recipients MAY notify affected parties of a potential compromise or threat.

5.4.3 Sharing Policy - Dissemination marking and disclosure

Policy Statement	Traffic light protocol
Policy Description	Recipients are permitted to redistribute the information received within the redistribution scope as defined by the enumerations. The enumerations "RED", "AMBER", "GREEN", "WHITE" in this document are to be interpreted as described in the FIRST Traffic Light Protocol Policy.
Policy Enumerations ⁶	<p>RED Information exclusively and directly given to (a group of) individual recipients. Sharing outside is not permitted.</p> <p>AMBER Information exclusively given to an organization; sharing limited within the organization.</p> <p>GREEN Information given to a community or a group of organizations at large. The information cannot be publicly released.</p> <p>WHITE Information can be shared publicly in accordance with applicable law.</p>

⁵ https://www.misp-project.org/taxonomies.html#_pap

⁶ https://www.misp-project.org/taxonomies.html#_t1p_2

5.4.4 Licensing Policy - Applicable agreements, licenses, or terms-of-use

Policy Statement	Licensing
Policy Description	States whether the recipient MAY or MUST NOT resell the information
Policy Enumerations	<p>“unmodified_resale” received unmodified or in a semantically equivalent format.</p> <p>Recipients MAY resell the information received.</p>

5.4.5 Non-Attribution - Decide whether anonymity of member sharing is acceptable

Under certain circumstances, a member or other information sharing partner may possess useful information, but not wish to be attributed when sharing the information. In that case, the member or partner can pass the information directly to CIRCL (Computer Incident Response Center Luxembourg) or any member of the platform (using the “delegate” button), and by that way request non-attribution, also known the Chatham House Rule. If CIRCL or the delegated PISAX member determines the information is adequate, the delegated organization will publish it, without the original attribution.

5.5 Partnerships and support

5.5.1 Inter ISAC Collaboration

- GSAM T-ISAC

From the very beginning of the platform setup, partnership was developed with GSMA (T-ISAC) specifically to avoid duplication of sharing among communities. The goal was to use the influence of GSMA to foster faster growth of the community.

- ISAC Facilities Manager — SMART 2018/1022⁷

Information Sharing and Analysis Centres (ISACs) are non-profit groupings facilitating voluntary information gathering on cyber incidents, threats and vulnerabilities, along with sharing experience, knowledge and analysis. The establishment and further development of EU level sectoral ISACs is a policy priority for the European Commission, and aligns with the NIS Directive, which determines the Operators of Essential Services (OES) in specific sectors as well as the security and reporting requirements. The Facilities Manager provides logistical support, specialist advice, IT platform support, thematic analysis and subscription-based services to the ISACs.

- EU ISACA Conferences

PISAX participated in the Empowering EU ISACs Conference on June 29th 2020⁸.

⁷ <https://etendering.ted.europa.eu/cft/cft-display.html?cftId=4394>

⁸ Recording of the conference can be accessed here <https://www.youtube.com/watch?v=AtVAAtW7fg30&t=2609s>

5.5.2 Existing Partnerships

Core service platform cooperation mechanisms for ISACs include:

- Interconnect the PISAX MISP with JTAN

“Joint Threat Analysis Network”(JTAN)⁹ is a CEF-funded project (CEF-TC-2020-2 - Cybersecurity – Objective 2 - 2020-EU-IA-0260 Joint Threat Analysis Network) to improve analysis and information sharing. PISAX MISP community will connect to the future JTAN network and especially, to allow the interconnections with other information sharing and analysis community relying on the MISP open-source project

- Euro-IX

Euro-IX helps disseminate information regarding the PISAX platform. In multiple Euro-IX virtual forums, the PISAX team has had the opportunity to present the PISAX initiative¹⁰.

Euro-IX has also supported the PISAX mailing list that was used to disseminate information about the ISAC within the Internet exchange point community.

The PISAX initiative has also leveraged IXPdb¹¹ which serves as a source of IXP assets. PISAX then uses this asset list to feed the related vulnerabilities within the sharing platform.

⁹ https://ec.europa.eu/inea/sites/default/files/cefpub/1_en_annexe_acte_autonome_part1_v2_0.pdf

¹⁰ Recording of Euro-IX presentations <https://www.youtube.com/watch?v=vFVtxduoKMo>

¹¹ <https://ixpdb.euro-ix.net/en/>

6. Mechanisms and tools

6.1 Information collection and dissemination standards and best practices

6.1.1 Sources of data sharing inside PISAX information sharing community

The following sources of information are used to populate events in the PISAX information sharing platform:

- Open-Source INTelligence (OSINT),
- Github Git-vuln-finder¹²,
- Information collected during incidents,
- Data feeds shared by partners, such as honeypots.

6.1.2 Mechanisms used to provide context for events

- Github CVE-search¹³.

6.1.3 Data model, vocabulary and taxonomies

At initiation, successful information sharing communities establish common vocabularies. This critical step allows members to filter information depending on their capabilities, willingness to process contextual information or to ingest indicators for detection or defensive matters. Establishing common vocabularies helps members to clarify the scope of the information shared and limit information miscommunication.

6.1.3.1 Taxonomy

PISAX has adopted established taxonomies from the gsma-network-technology¹⁴.

6.1.3.2 Galaxy

PISAX has adopted established galaxies in order to stay consistent and to be comparable among different communities, such as:

- the Bhadra galaxy¹⁵:
- Cornell University Framework¹⁶:
- the ATT&CK framework¹⁷:

¹² <https://github.com/cve-search/git-vuln-finder>

¹³ <https://github.com/cve-search/cve-search>

¹⁴ https://www.misp-project.org/taxonomies.html#_gsma_network_technology

¹⁵ https://www.misp-project.org/galaxy.html#_bhadra_framework

¹⁶ <https://arxiv.org/abs/2005.05110>

¹⁷ <https://attack.mitre.org/>

6.2 Sharing model and mechanism

6.2.1 Collaboration mechanisms

Collaboration mechanisms include, but are not limited to:

- MISP sharing platform dedicated to PISAX community¹⁸.
- MISP encrypted emails generated by the PISAX platform.
- Teleconference and training platform¹⁹.
- Regular meetings and working groups (RIPE, Euro-IX, GSMA T-ISAC, ...).
- Euro-IX PISAX mailing list²⁰.

¹⁸ <https://misp.pisax.org>

¹⁹ <https://bbb.lu-cix.lu/>

²⁰ <https://lists.euro-ix.net/mailman/listinfo/pisax>

7. Security and compliance

7.1 Security requirements

PISAX security requirements are based on LU-CIX's Information Security Policy

7.2 Compliance requirements

7.2.1 Data protection – General Data Protection Regulation (GDPR)

7.2.1.1 Introduction

PISAX enables automated and secure threat intelligence sharing. PISAX is running on the MISP²¹ threat sharing platform, which data model is composed of “events”, that usually represent threats or incidents. Often information exchange could involve personal data, meaning that the requirements of the General Data Protection Regulation (GDPR) or any other relevant privacy regulation may apply.

7.2.1.2 What personal data is shared through PISAX?

Not all cyber security information constitutes personal data. Personal data is defined as “any information relating to an identified or identifiable natural person” (Art. 4(1) of the GDPR). Incidents shared through the PISAX platform are composed of “attributes”. In some cases, attributes can consist of IP addresses, domain names or other online personal identifiers. Such information can be considered as personal data when it can be linked to a specific individual. There can be cases when attributes within shared cyber security information would no longer include personal data if an individual cannot be identified from such information.

7.2.1.3 How is information exchange impacted by the GDPR?

Recital 49 of the GDPR states that the processing of personal data is allowed “to the extent strictly necessary and proportionate for the purposes of ensuring network and information security”. In other words, the GDPR may enable information exchange of personal data between any PISAX member to ensure the security of its network and information. According to the GDPR, this could for example include preventing unauthorized access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.

Information sharing is voluntary within PISAX. Any member having access to personal information is determining the purposes of processing information, which can include whether to share this information, or not. Nevertheless, collecting personal data in the first place - before sharing through PISAX - means that there are certain data protection responsibilities. For instance, it should be transparent to an individual how the personal data concerning him or her is collected, used and to what extent the personal data are or will be processed (transparency principle). In addition, data collected and processed should not be kept more than it is needed for the purpose (data minimization principle).

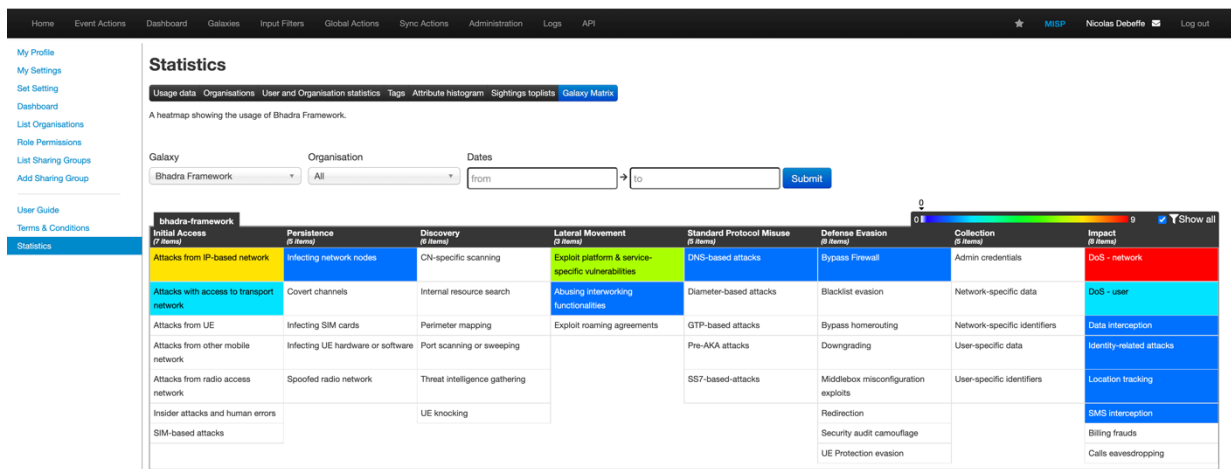
²¹ More information about MSIP threat sharing platform and how information sharing and cooperation is enabled by GDPR can be found here: https://www.misp-project.org/compliance/gdpr/information_sharing_and_cooperation_gdpr.html

8. Follow-up and improvement

8.1 Measure effectiveness of sharing

The PISAX MISP platform provides matrix and measurements capabilities, which can be used to enhance the platform usage, sharing practices, detection techniques and information gathering.

Example of matrix statistics:



8.2 Evaluate members needs

User feedback is to be collected during interactions with the users (e.g. mailing lists, training sessions, events) for future evolution of the platform.