

Collaborate on  
cybersecurity  
in an ecosystem of trust



**RambiCo**

## Article 29, Cybersecurity information-sharing arrangements

1. Member States shall ensure that entities falling within the scope of this Directive and, where relevant, other entities not falling within the scope of this Directive are able to exchange on a voluntary basis relevant cybersecurity information among themselves, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks, where such information sharing:

(a) aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;

(b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative cyber threat research between public and private entities.

2. Member States shall ensure that the exchange of information takes place within communities of essential and important entities, and where relevant, their suppliers or service providers. Such exchange shall be implemented through cybersecurity information-sharing arrangements in respect of the potentially sensitive nature of the information shared.

3. Member States shall facilitate the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 of this Article. Such arrangements may specify operational elements, including the use of dedicated ICT platforms and automation tools, content and conditions of the information-sharing arrangements. In laying down the details of the involvement of public authorities in such arrangements, Member States may impose conditions on the information made available by the competent authorities or the CSIRTs. Member States shall offer assistance for the application of such arrangements in accordance with their policies referred to in Article 7(2), point (h).

4. Member States shall ensure that essential and important entities notify the competent authorities of their participation in the cybersecurity information-sharing arrangements referred to in paragraph 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.

5. ENISA shall provide assistance for the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by exchanging best practices and providing guidance.

# What is an ISAC?

## 1. Information Sharing (IS)

- Sharing valuable knowledge and information about security topics that are operational, tactical and/or strategically important for the operations of the members.

## 2. Analysis Center (AC)

- Analyzing collected information and sharing the conclusions and recommendations with members.

3. An ISAC is a closed community where members know each other personally, have regular contact with each other and the above activities are carried out on the basis of TRUST and house rules.

# What is the benefit of an ISAC?

## BENEFITS OF INFORMATION SHARING AND ANALYSIS CENTRES



### TRUSTED COMMUNITY

ISAC is the community that brings together industry operators with the same goals and interests, creating a trusted environment.



### GOOD PRACTICES

ISACs are platforms for OES to exchange good practices and information about threats, incidents, risks and their mitigation.



### CYBERSECURITY AWARENESS

ISAC is enhancing the cybersecurity posture and awareness in the critical infrastructure sectors



### SUPPORT WITH EU LEGISLATIONS

ISACs can support the implementation of European legislation such as the NIS2 Directive, Network Code on cybersecurity (NCCS) and the Cyber Resilience Act (CRA)



### CRISIS MANAGEMENT

ISACs can be used as information exchange mechanisms in case of crisis

# Co-founder of multiple (EU Energy) ISACs





# EMPOWERING EU ISACS PROJECT

EU support for existing and to-be EU ISACs

[www.isacs.eu](http://www.isacs.eu)

# 2022 Sector overview: Involved in 19 EU ISAC initiatives

 Involved  
 Identified



Energy



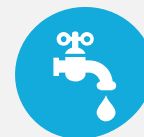
Transport



Health sector



Finance



Drinking water  
supply & distribution



Digital  
Infrastructure



Rail



Maritime



Aviation



Financial market/  
Banking



Financial  
infrastructures



TLD



IXP



Cloud  
Providers



Telecom



ICS-  
SCADA



Audio-visual &  
Media



Nuclear



Government and  
public  
authorities



Defence



Supply  
Chain



Public  
Safety



Cities



Tourism



Automotive



Space



Pharmaceuticals



Agri food



Empowering EU-ISACs

# Use a structured approach to set up an ISAC

## 1. Getting aligned = building trust

- Discuss about goals, mutual interest, benefits and mission of an ISAC
- **WHY** do we want an ISAC?

## 2. Create one Way of Working

- Focus on the type of activities and which information (not) to share
- **WHAT** do we want to share and analyse?

## 2. Set up governance and organization

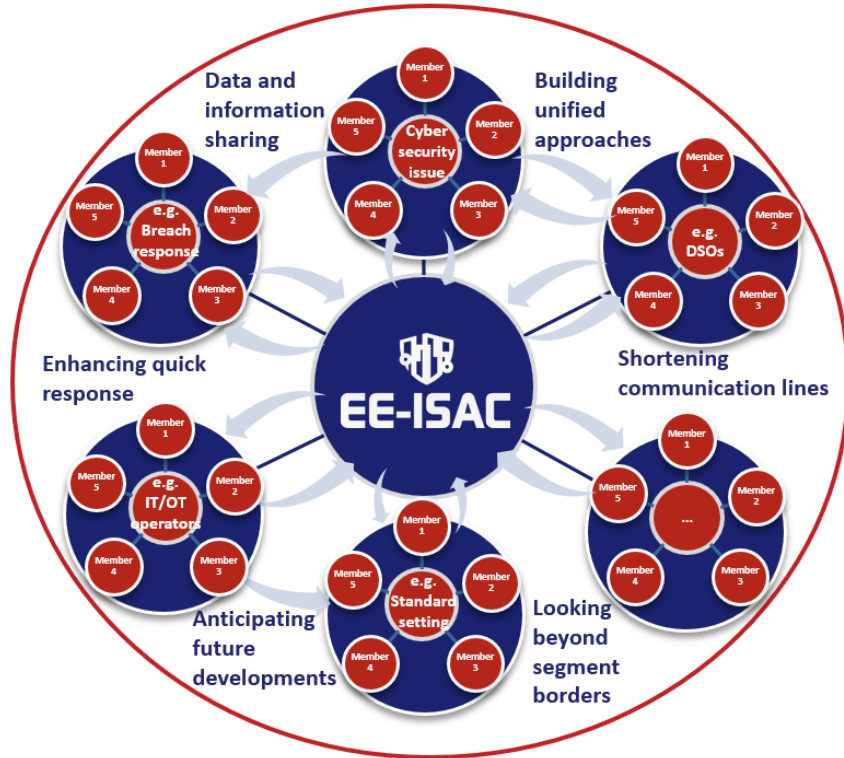
- Focus on the set-up of organization and governance structure
- **HOW** do we want to perform and collaborate?



# Example of a mission statement

*“to improve the **resilience** and **security** of the European energy infrastructure. We do so through **trust** based **information sharing** and by enabling a **joint effort** for the analysis of threats, vulnerabilities, incidents, solutions and opportunities. EE-ISAC offers a **community of communities** to facilitate this proactive information sharing and analysis, allowing its members to take their own effective measures.”*

# Example of a closed EE-ISAC community



A CLOSED COMMUNITY OF COMMUNITIES

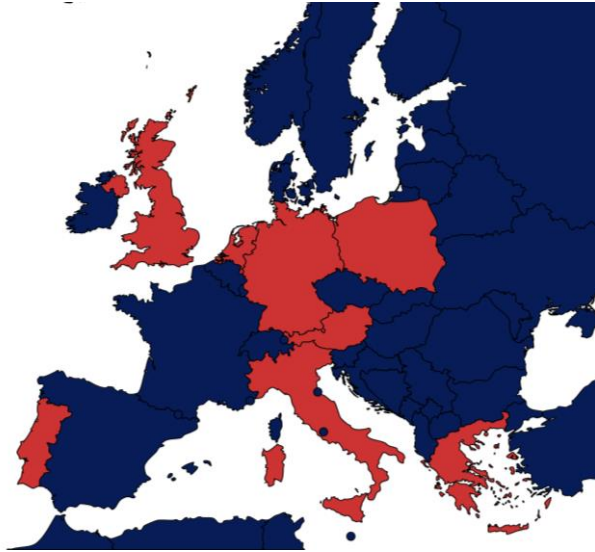
to **SHARE information, views, knowledge & initiatives**

- ✓ Cross-value chain
- ✓ Cross-functional levels
- ✓ Communities formed based on needs /peer groups
- ✓ Virtual as well as physical connection

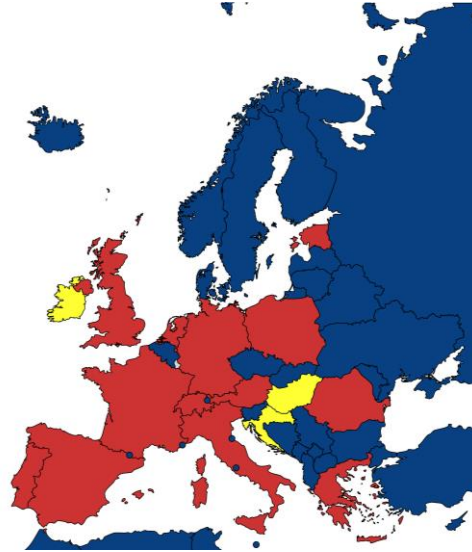
driving a **JOINT effort** for the **analysis** of

- ✓ Threats, Vulnerabilities, Incidents, Solutions, and improvement Opportunities

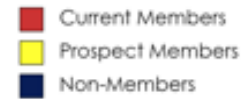
# Example of a closed EE-ISAC community



2016 (16)



2023 (37)



# Determine the role/function of the ISAC

1. Social gathering
2. Central information sharing center for the sector
3. Threat intel and information hub service
4. Information sharing AND **Analysis** center
5. “One stop shop” for collaborative activities
6. Lobby association
7. ....

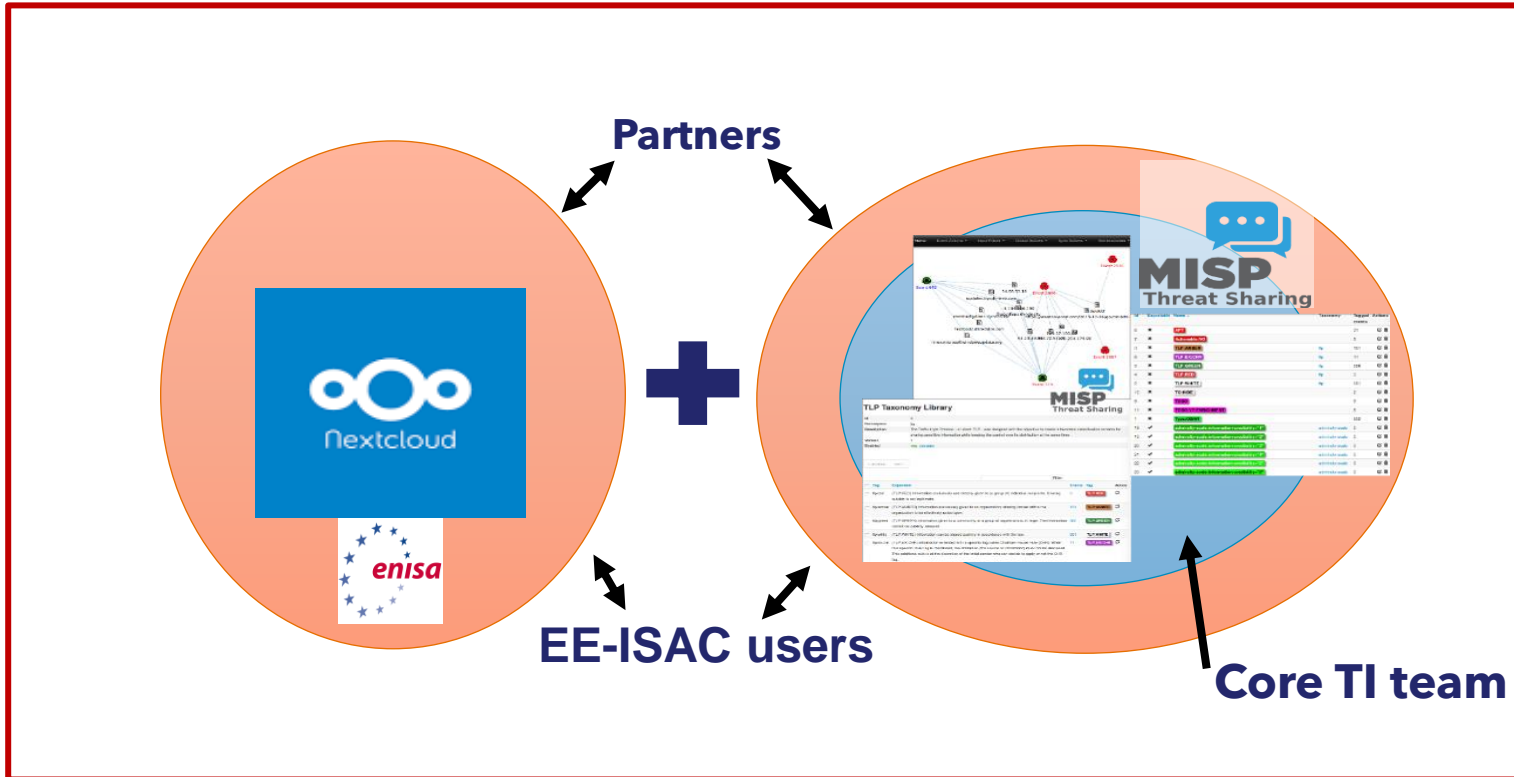
# Only share valuable information!

1. Threat intel data and threat landscape reports
2. Mitigation of critical vulnerabilities
3. Root Cause Analysis of incidents
4. Incident response & recover activities
5. Best practices of improvements/solutions
6. Lessons learned from cybersecurity projects
7. ....

# Social events are necessary to build up trust




# Use tools to collaborate and share more effectively



# Strive for global information sharing

**Trilateral  
MoU**

October 17  
2018  
Las Vegas



**EE-ISAC**  
EUROPEAN ENERGY INFORMATION SHARING AND ANALYSIS CENTER

**E-ISAC**  
ENERGY INFORMATION SHARING AND ANALYSIS CENTER

**JE-ISAC**  
JAPAN ENERGY INFORMATION SHARING AND ANALYSIS CENTER





# Key recommendations

1. Insert the ISAC model in national NIS2 regulation as example for Article 29 of NIS2 directive
2. Establish ISACs for other (smaller) domains/sectors
3. Develop and/or improve cross-sector information sharing with other ISACs
4. Use EU-ISACs' sharing platforms: MISIP and NextCloud
5. Position international collaboration as cornerstone for cybersecure Europe

International collaboration via an ISAC is crucial !!



**Please contact me if  
you want more info**

- **Name** : Johan Rambani
- **Role** : Cybersecurity consultant
- **Organization** : Rambico
- **Telephone** : +316 11879945
- **E-mail** : [info@rambico.com](mailto:info@rambico.com)

**Rambico**