



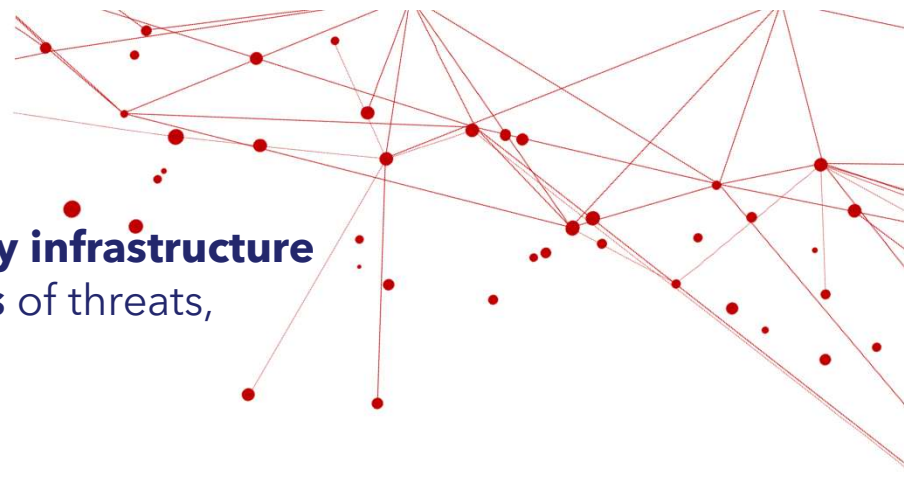
Information Sharing in Network of Trust

6th Joint Data Exchange and Cybersecurity WS 2026

Cybersecurity Information Sharing
as a Pillar of a Resilient Utility

MISSION STATEMENT

Improve the **resilience** and **security** of the European **energy infrastructure** through trust-based **information sharing** and **joint analysis** of threats, vulnerabilities, incidents, solutions and opportunities



WHEN | launched in December 2015



WHO | EE-ISAC is a **community of communities** involving Utilities/Energy Operators, Solution Providers, Academia and EC Entities



HOW | building a collective Intelligence leveraged by **information sharing** and **joint analysis** of threats, vulnerabilities and incidents

- Empowering each member to take more effective decisions



Defensive capabilities

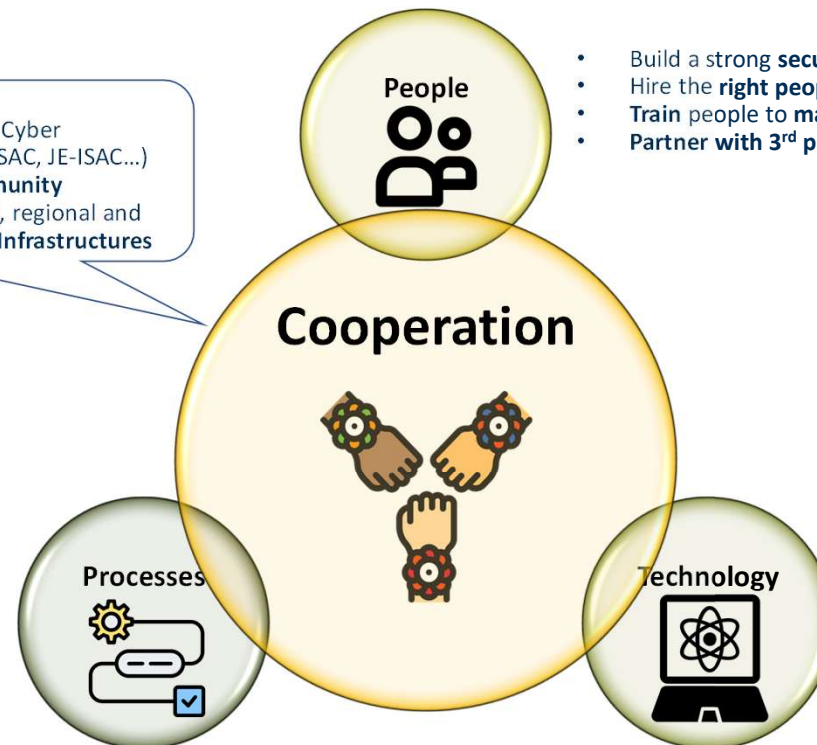


Collaborative Cybersecurity is the key

. Together we are stronger

- **SHARE incidents**, help and ask for help
- **SHARE knowledge & GIVE BACK** to the Cyber Community, (Cynergy ISAC, EE-ISAC, E-ISAC, JE-ISAC...)
- **Strengthen TRUST** and **Grow the Community**
- **Establish partnerships** focused on local, regional and global **Cybersecurity of Energy Critical Infrastructures**

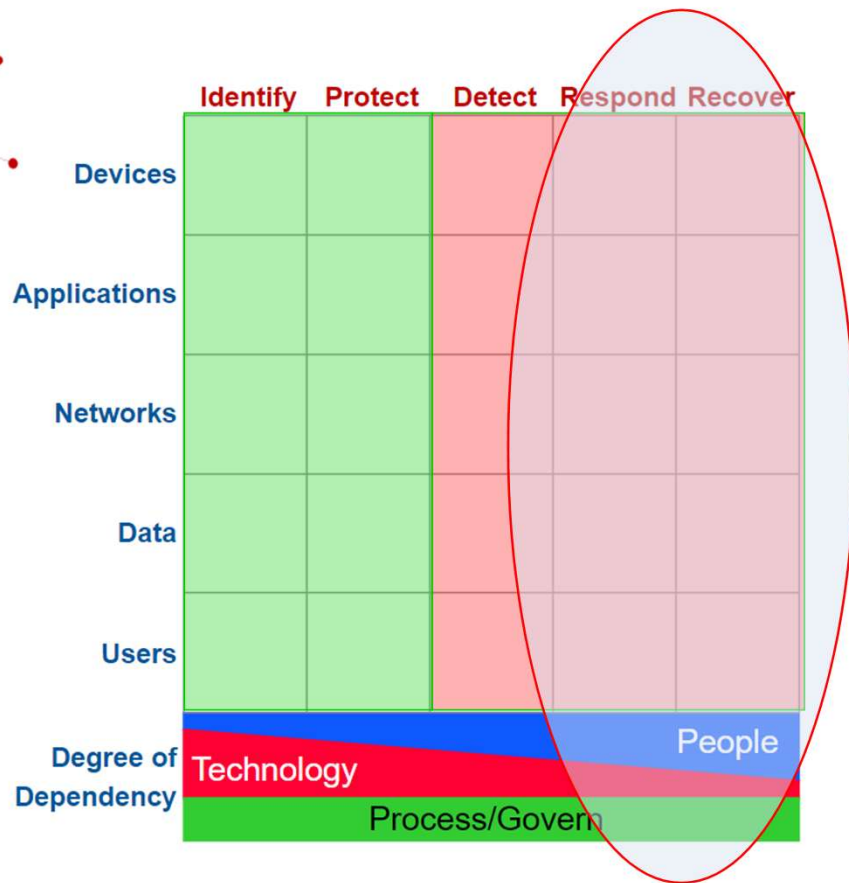
- Adopt **industry standards & frameworks** (NIS2, ISO,...)
- Develop and maintain **policies, procedures, plans, playbooks** according to industry standards and best practices
- **Audit** your existing processes



- Build a strong **security culture**
- Hire the **right people** with the **right skillset**
- **Train people** to **maintain & develop skills**
- **Partner with 3rd parties** to assure the expertise and/or capacity

- **Design & Build** a defensible architecture
- Acquire the **right tools**
- Maintain your tools **up-to-date**
- **Build business-specific use-cases**
- **Implement principles** as defense-in-depth, ringed-fence, zero-trust

Collaborative Cybersecurity is the key

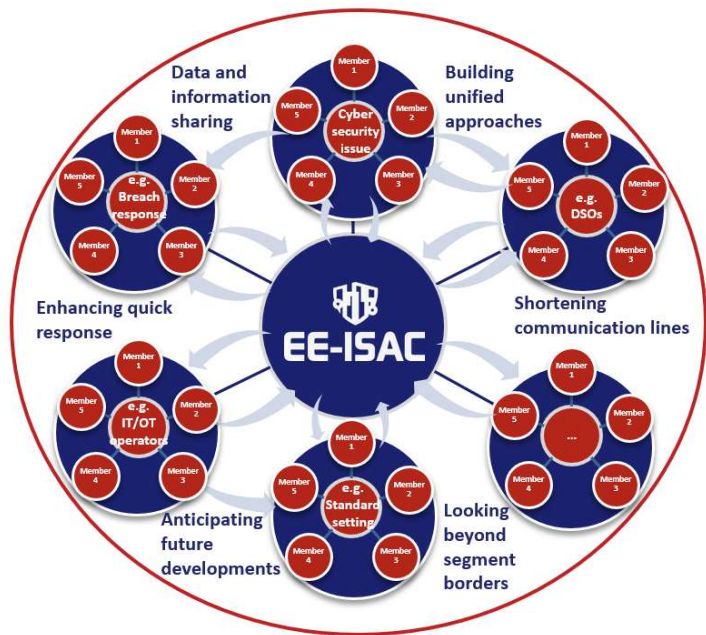


- **Attackers cooperate** when executing cyber attacks - we must cooperate to detect them as early as possible
- **Collaborative Cybersecurity** exponentiates individual capabilities
- **Communication & real-time threat intelligence** are decisive

Reasons behind the EE-ISAC

Source: <https://cyberdefensematrix.com/>

COMMUNITY OF COMMUNITIES



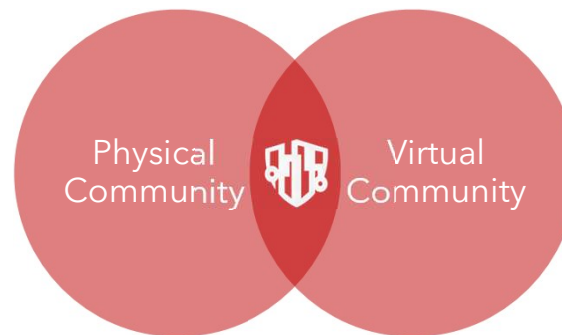
A CLOSED COMMUNITY OF COMMUNITIES

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



Network Footprint of Member DSOs:

+102M electricity customers

(51% of EU Electricity Customers)

Network Footprint of Member DSOs+TSOs:

+146M electricity customers

(72% of EU Electricity Customers)

Base: ~202M EU households (Eurostat 2024). Internal simulation, not official.

Operators	26
Solution Providers	15
Academia	6
Governmental - NFP	7
Research	1



UNIVERSITÉ DE FRIBOURG
UNIVERSITÄT FREIBURG



University of
Strathclyde
Glasgow



VATTENFALL



Vestas

Collaboration: #14 Partners + EU Institutions

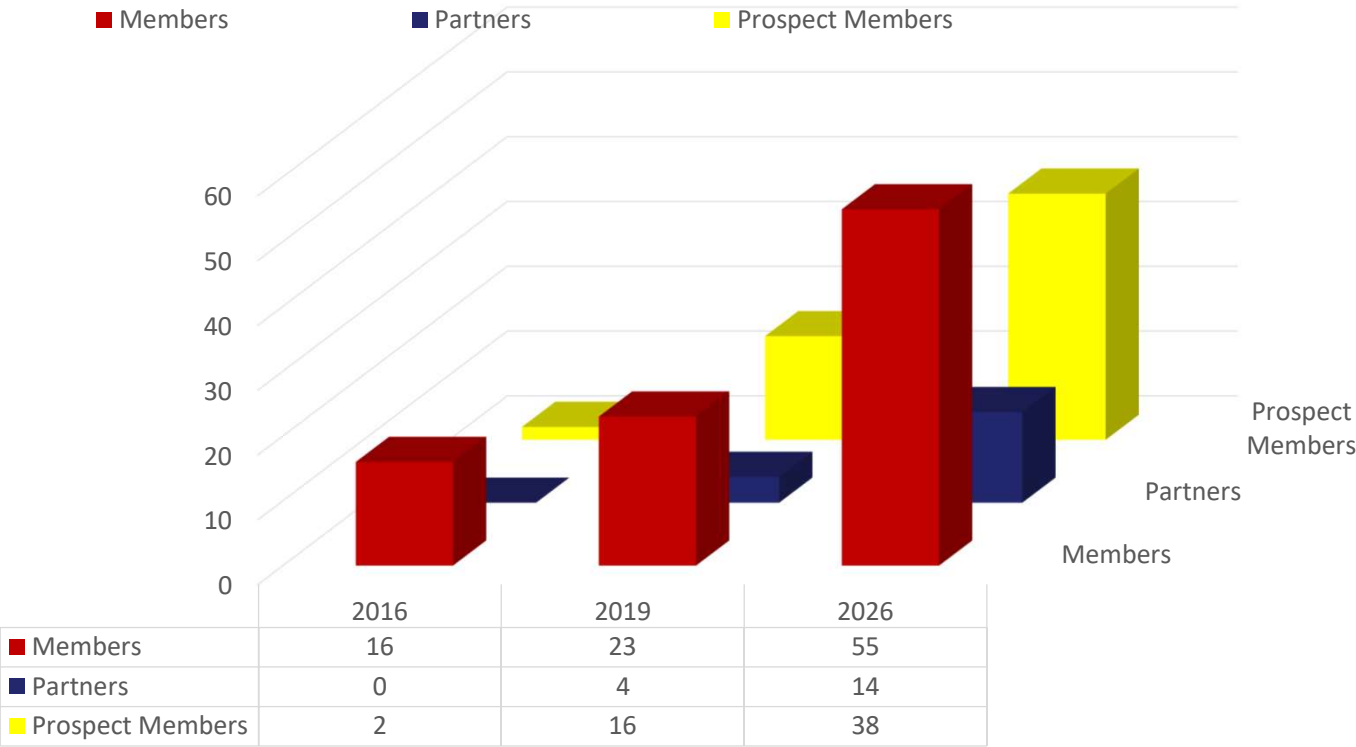
MoU Partners (14)



Institutions & Agencies (3)



MEMBERSHIP STATUS BY JUNE 2026



MEMBERSHIP MAP

- Current members
- Members operating
- Non-members

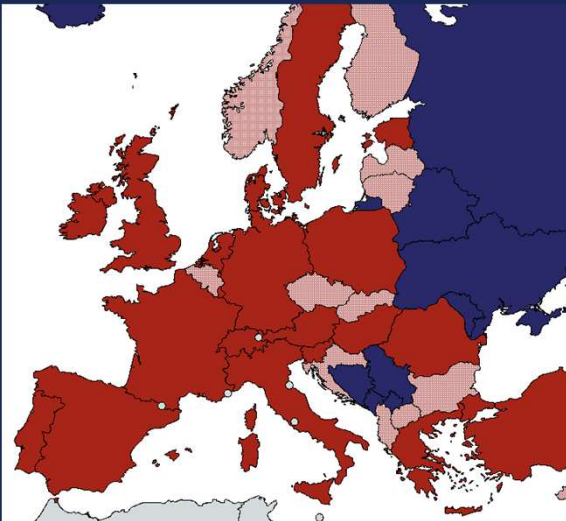
2016 (16)



2019 (27)



2026 (55)



6 TASK FORCES

- **Membership & Partnerships**
 - Grow Energy Operators' community
 - Exchange of information between member experts and ISACs
- **Info sharing platforms, Threat Intelligence & TF Threat Landscape**
 - Daily Tracker and Monthly Threat Report with detected vulnerabilities and malware
 - Best practices
 - Energy Threat Landscape Report with ENISA (2023)
- **Advocacy**
 - Position Papers
 - Participation in EC calls and expert groups (e.g. SEEG)
- **Communication**
 - Organisation and coordination of international events
 - Presence in European and International conferences on cybersecurity
- **Physical Security**
 - Best practices and use cases
 - Report on national standards for the physical security of the energy network.
- **Offshore Wind Sector**
 - Cybersecurity baseline across the offshore wind value chain

Digital Information Sharing



NEW

EE-ISAC
Nextcloud

Physical Information Sharing

Physical Information Sharing Community

- Community meetings
- Theme based meetings
- Open house Plenary meetings

Topics

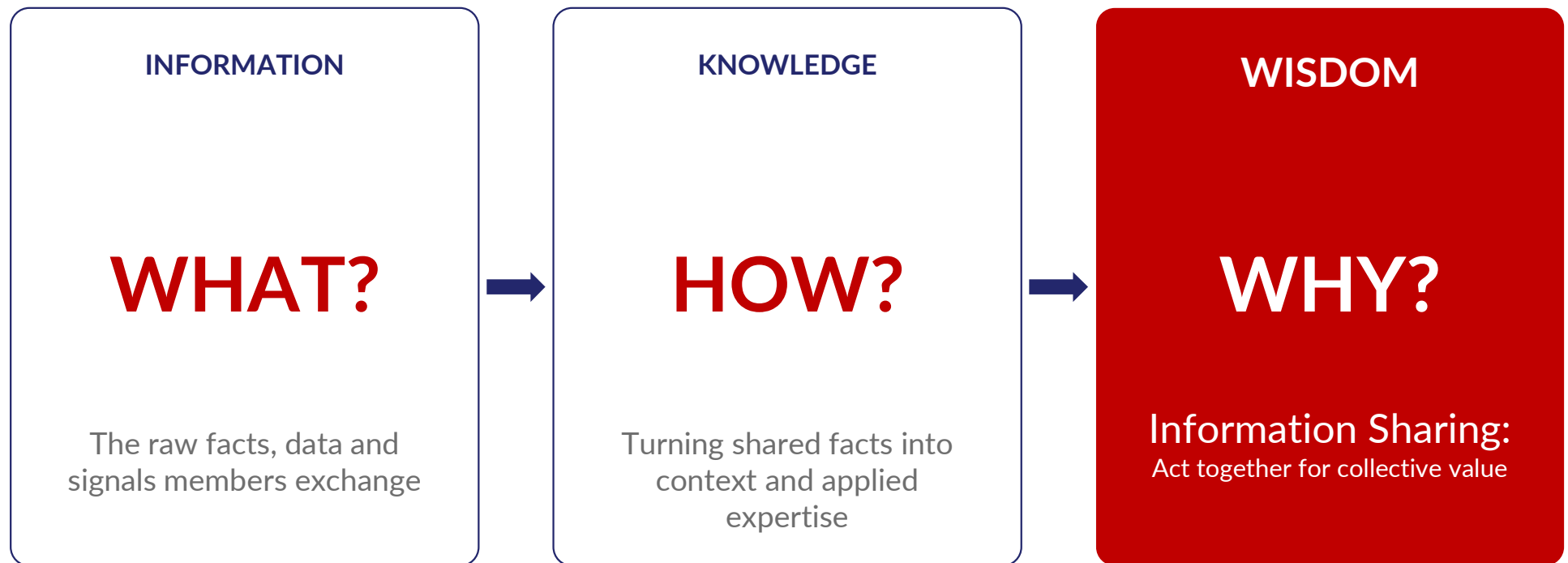
- **Vulnerabilities** and **Threat/Risk** analysis information
- **Lessons learned**/best practices
- **Alerts** and notifications
- Use of standards
- **Ex-post** analysis of incidents



EE-ISAC Plenary Meetings

- Confidentiality (TLP Protocol)
- Task Forces Progress
- Hosted by the Utilities

EE-ISAC: Sharing Information for a Collective Action



Key Takeaway

Attackers Share with each other
Energy Defenders must Share through the EE-ISAC



For further information, please refer to the below:

communications@ee-isac.eu

www.ee-isac.eu

powered by

ianusGroup
STRATEGIC CONSULTING