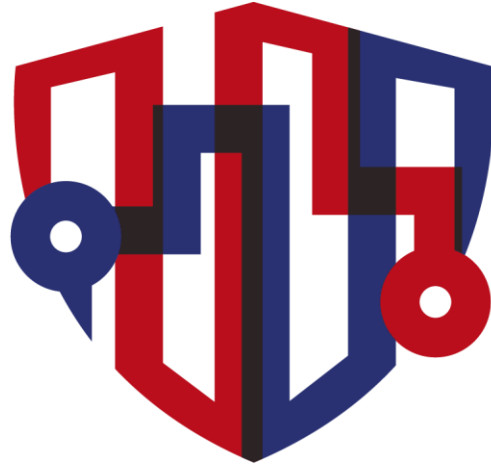


EE-ISAC





EE-ISAC

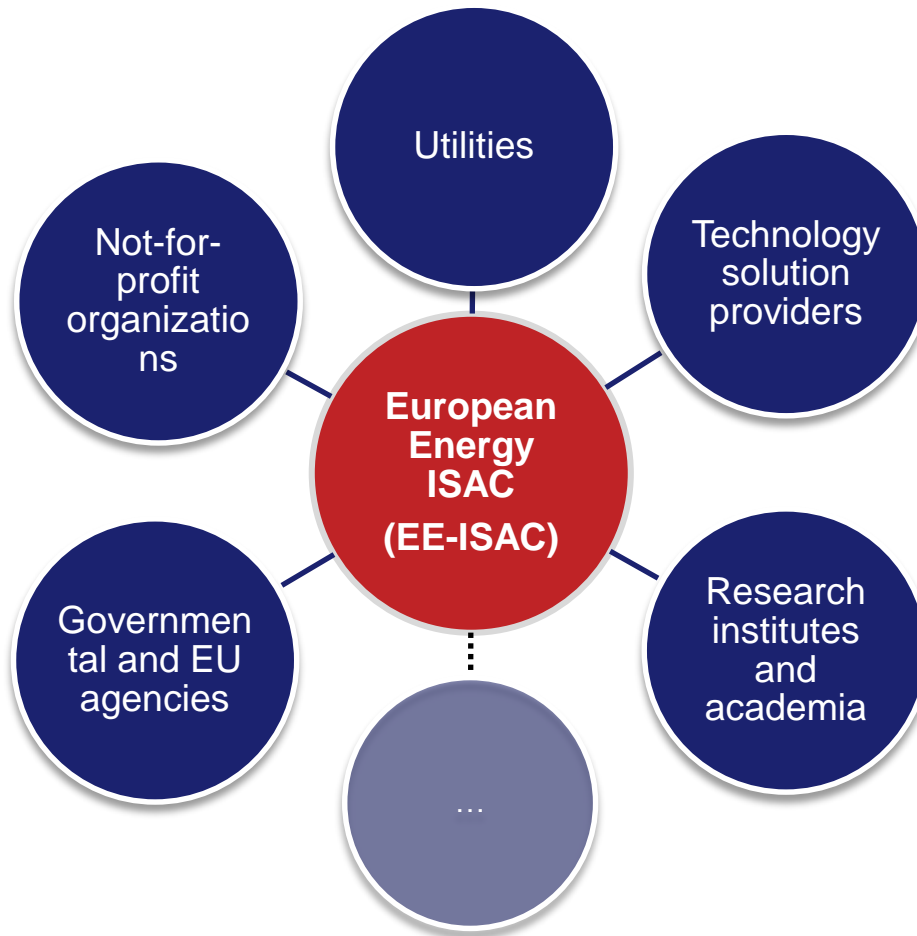
Information sharing in network of trust

EE-ISAC launched in December 2015

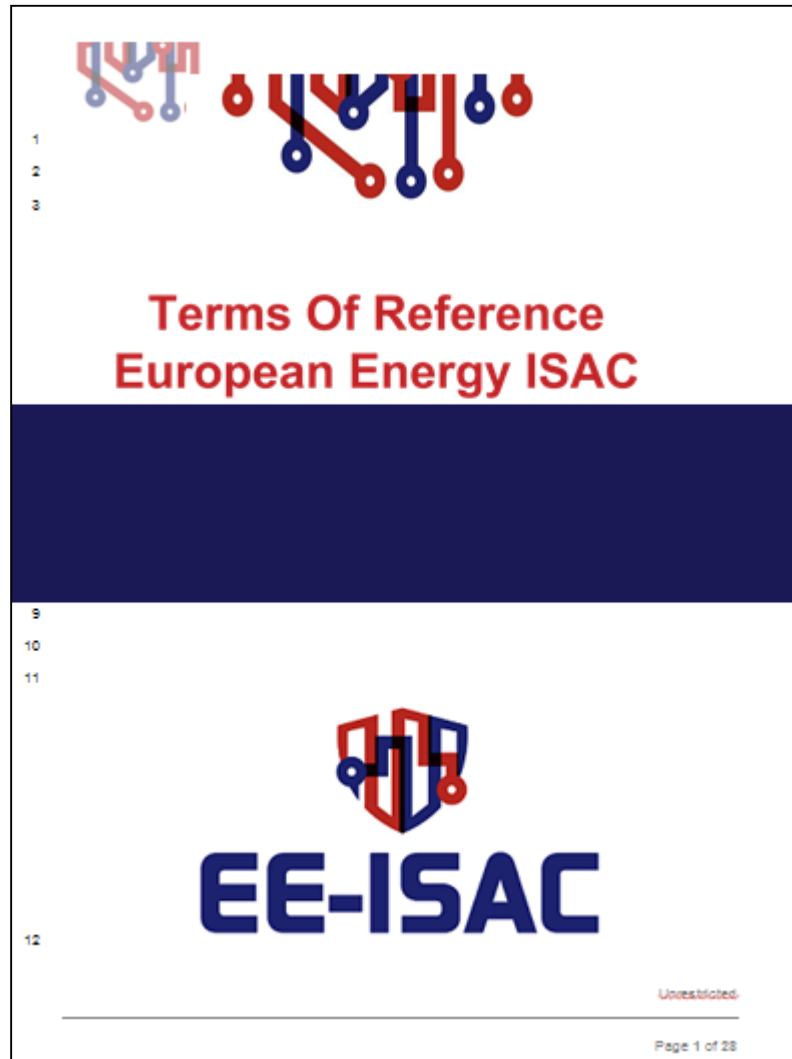
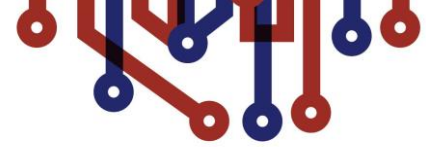


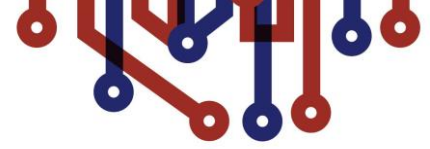
EE-ISAC

25 Believers of the EE-ISAC



EE-ISAC game rules for members



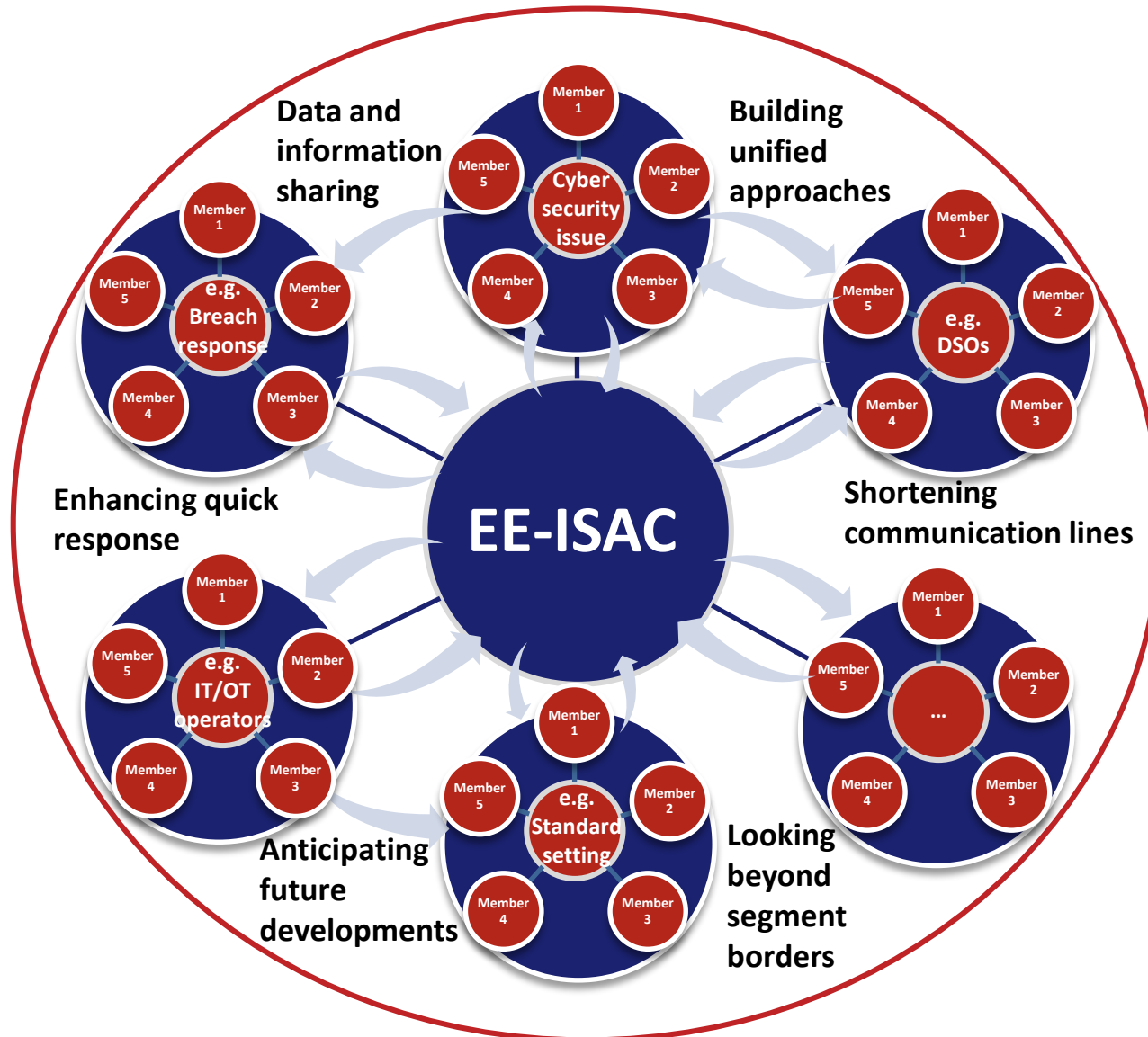


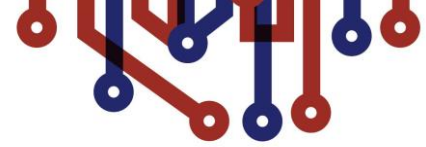
EE-ISAC Mission Statement

*“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.”*



Community of communities





Activities & channels

Physical Community

- In-person meetings to strengthen community sense and hold content based discussions
- Organised theme based meetings
- Aim is to build trust and share confidential knowledge and information

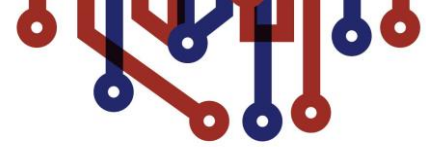
European Energy ISAC (EE-ISAC)



Digital Community

- Development of a platform or portal to connect the EE-ISAC members on a direct and continuous manner
- Facilitate information sharing through reports, newsletters, webinars and e-learning, etcetera





Activities & sharing topics

Current focus on activities :

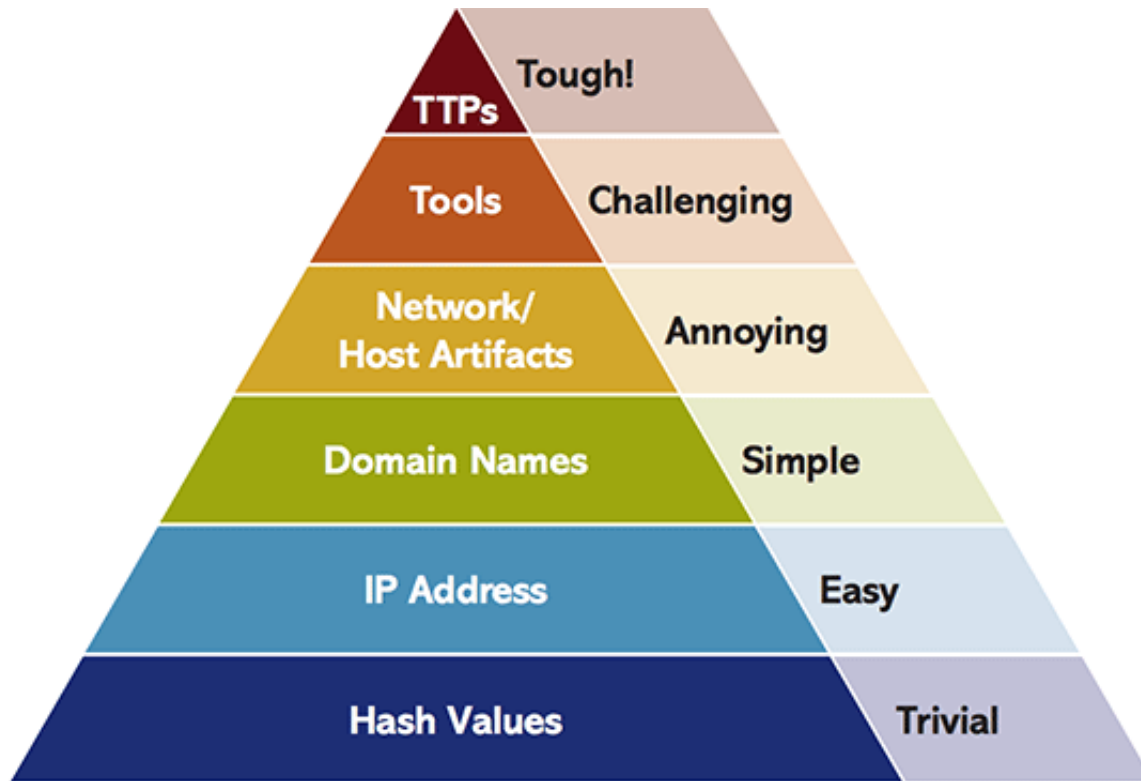
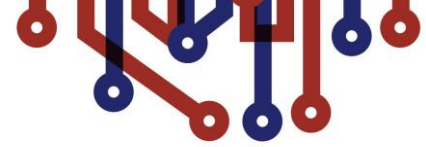
- **Physical info sharing community**
 - Plenary meetings
 - Community meetings
 - Theme based meetings
 - Open house meetings
- **Digital info sharing community**
 - Information requests/push
 - (Daily) chat contact
 - Circles of trust for webmeetings
 - Newsletters
 - Forum for Q&A
 - Webinars
 - E-learning modules
 - Marketplace for students

Topics of information sharing :

- Vulnerabilities in IT and OT systems
- Threat/Risk analysis information
- Incidents
- (Penetration) test results
- Lessons learned / best practices
- Alerts and (patch)notifications
- Near real-time threat data exchange
- Trends and improvement initiatives
- Share subject matter expertise
- (Technical) support requests
- Use of standards (ISO, IEC, NIST, NERC etc.)
- Research (H2020) topics
- Phd assignments



Digital information sharing

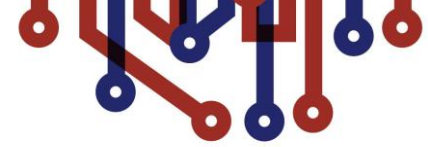


Vmoso sharing platform

Our sharing platform, powered by BroadVision, permits to share documents, posts and chat among members and external peers

The screenshot displays the Vmoso sharing platform interface. The top navigation bar includes the Vmoso logo, the user name 'Massimo Rocca', a search bar, and a '+ Create' button. Below the navigation bar, there are two main panels. The left panel, titled 'Posts Stream', shows a list of posts with user avatars and dates. The right panel, titled 'Files Stream', shows a list of files with PDF icons and dates. A document viewer is open in the foreground, displaying a document titled 'Cyber Security Risk Management - EE-ISAC ...'. The document content includes the text 'CYBER SECURITY RISK MANAGEMENT FOR DIGITALIZED ENERGY SYSTEMS: CHALLENGES AND SOLUTIONS' and a logo of EE-ISAC. The interface also features a bottom navigation bar with icons for Chats, Content, and Posts.

MISP



MISP is a de-facto standard:

- An efficient IoC and database about malware samples, incidents and attackers
- Automatic correlation finding relationships between attributes and indicators



MISP

Threat Sharing

The screenshot displays the MISP web interface. At the top, there's a navigation bar with 'Home', 'Event Actions', 'Input Filters', 'Global Actions', 'Sign Actions', and 'Administration'. Below this is a network graph showing relationships between various events (e.g., Event 612, Event 2686, Event 2687, Event 275) and indicators like IP addresses and domains. A 'MISP Threat Sharing' logo is visible in the bottom right of the graph area.

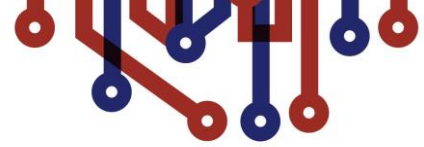
Below the graph is the 'TLP Taxonomy Library' section, which includes a table of TLP tags and their descriptions:

Tag	Expanded	Events	Tag	Action
<input type="checkbox"/> TLP:RED	(TLP:RED) Information exclusively and directly given to (a group of) individual recipients. Sharing outside is not legitimate.	5	TLP:RED	
<input type="checkbox"/> TLP:AMBER	(TLP:AMBER) Information exclusively given to an organization; sharing limited within the organization to be effectively acted upon.	131	TLP:AMBER	
<input type="checkbox"/> TLP:GREEN	(TLP:GREEN) Information given to a community or a group of organizations at large. The information cannot be publicly released.	500	TLP:GREEN	
<input type="checkbox"/> TLP:WHITE	(TLP:WHITE) Information can be shared publicly in accordance with the law.	621	TLP:WHITE	
<input type="checkbox"/> TLP:EX-CHRI	(TLP:EX-CHRI) Information extended with a specific tag called Chairman House Rule (CHR). When this specific CHR tag is mentioned, the attribution (the source of information) must not be disclosed. The additional rule is at the discretion of the initial sender who can decide to apply or not the CHR tag.	11	TLP:EX-CHRI	

Below the taxonomy library is a table of events with their taxonomies:

Event	Exportable	Name	Taxonomy	Tagged	Actions
6	<input checked="" type="checkbox"/>	APT		31	
7	<input checked="" type="checkbox"/>	Actionable:IO		5	
3	<input checked="" type="checkbox"/>	TLP:AMBER	tlp	131	
8	<input checked="" type="checkbox"/>	TLP:EX-CHRI	tlp	11	
5	<input checked="" type="checkbox"/>	TLP:GREEN	tlp	500	
4	<input checked="" type="checkbox"/>	TLP:RED	tlp	3	
2	<input checked="" type="checkbox"/>	TLP:WHITE	tlp	531	
10	<input checked="" type="checkbox"/>	TO:MODE		2	
9	<input checked="" type="checkbox"/>	TO:DO		9	
11	<input checked="" type="checkbox"/>	TO:CVT-EMPLOYEE INT		8	
1	<input checked="" type="checkbox"/>	Type:OSINT		832	
18	<input checked="" type="checkbox"/>	admiralty-scale:information-credibility="1"	admiralty-scale	0	
19	<input checked="" type="checkbox"/>	admiralty-scale:information-credibility="2"	admiralty-scale	0	
20	<input checked="" type="checkbox"/>	admiralty-scale:information-credibility="3"	admiralty-scale	0	
21	<input checked="" type="checkbox"/>	admiralty-scale:information-credibility="4"	admiralty-scale	0	
22	<input checked="" type="checkbox"/>	admiralty-scale:information-credibility="5"	admiralty-scale	0	
23	<input checked="" type="checkbox"/>	admiralty-scale:information-credibility="6"	admiralty-scale	0	



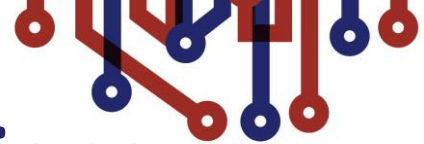


Sharing topics

During the first 2018 plenary held in Madrid, the members shared reports and analysis on the following incidents:

- WannaCry/NotPetya
- CrashOverride/Industroyer
- RSA/Infineon
- Triton
- Meltdown/Spectre
- Intel AMT

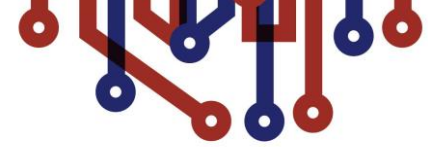


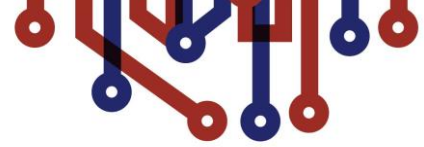


EE-ISAC (global) partners and relations

- **Energy-ISAC, the Netherlands**
- **European Commission DG ENER EECSP**
- **European Commission DG ENER TNCEIP**
- **EU ENISA**
- **EU EC SO**
- **US E-ISAC, USA**
- **ICS-ISAC, USA**
- **METI, Japan**
- **FEPC, Japan**

Formal partnership with JE-ISAC





EE-ISAC Key Strengths

- Sector specific information across the energy value chain
- Engagement of a variety of sector Stakeholders
- Access to a broad network of organizations
- Proactive and trust-based sharing community



Enhance organizational resilience and preparedness

Have a look online! www.ee-isac.eu



Home

About EE-ISAC

Members & Board

Insights

Contact

Bridging the gaps between disciplines



Members

The *European Energy - Information Sharing & Analysis Centre* (EE-ISAC) brings together key industry players representing the following categories:

1. European utilities
2. Technology & Service providers
3. Academic institutes
4. Governmental & not-for-profit organizations.

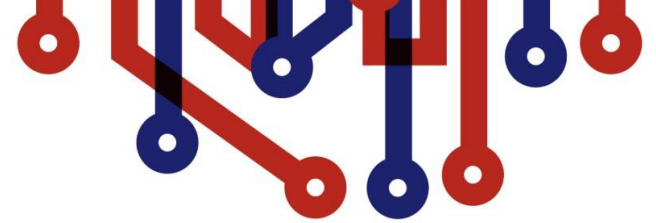
Scroll down for more information about the individual members.

Join us?

If you think your company adds up to our geographical scope (European utilities), coverage of the smart energy supply chain or cyber security expertise, please [contact us](#).



Let's discuss further



Jaroslav Sordyl

contact@ee-isac.eu

www.ee-isac.eu