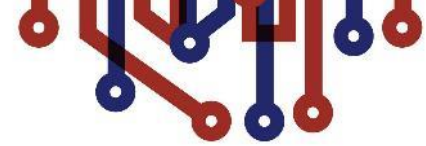


# EE-ISAC

Information sharing in network of trust



# EE-ISAC started from an EU project in 2013

European Energy ISAC (EE-ISAC) is the outcome of the EU funded Distributed Energy Security Knowledge (DENSEK) project from DG HOME, which had the objective of **improving the cyber resilience of the energy infrastructure (i.e. improving the cyber security of the Smart Grid Energy Grid).**

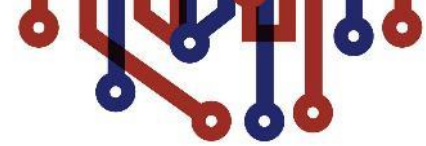
## How:

- Join forces at **EU** level;
- Involving **entire energy supply chain**;
- Improving know-how and awareness of **all stakeholders**.

## Three deliverables:

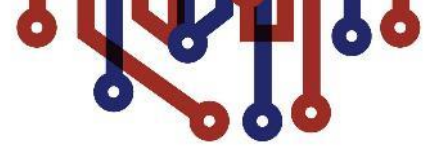
- European Energy Information Sharing and Analysis Center (EE-ISAC);
- Digital Information Sharing Platform;
- Situational Awareness Network model.





# EE-ISAC launched in December 2015



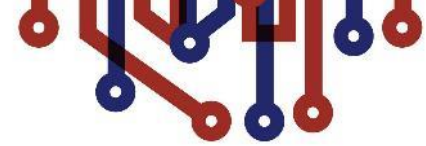


# EE-ISAC Mission Statement

---

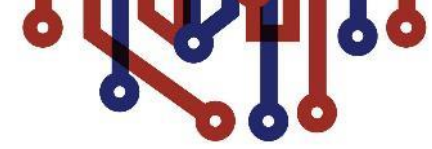
*“to improve the **resilience** and **security** of the European energy infrastructure. We do so through trust-based **information sharing** and by enabling a **joint effort** for the analysis of threats, vulnerabilities, incidents, solutions and opportunities. EE-ISAC offers a **community of communities**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

---



# Community of communities





# Community of communities



## A CLOSED COMMUNITY WITH CIRCLES OF TRUST

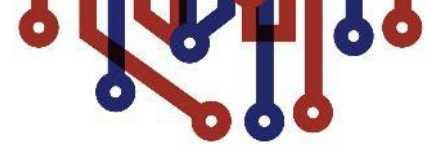
Brought together to share information, views, knowledge and initiatives

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

Physical  
Community



Virtual  
Community



# EE-ISAC in 2019

# 24

MEMBERS

-  Utilities
-  Vendors
-  EU/Public Bodies
-  Academia
-  Research Labs

# 23

EVENTS



 3 Open EE-ISAC Plenaries  
 Event @ EU Parliament +  
 Signed MoUs with Japan &  
 US E-ISACs; EASE; KraftCERT

# 10

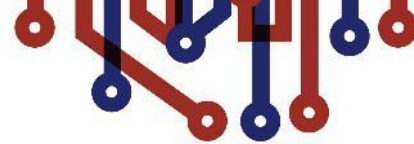
TASK FORCES

- 
- 
- 
- 

 1 White Paper / 3 Webinars  
 Secure sharing on Vmoso  
 Use of MISP







# EE-ISAC Partners & Relations

## International Information Sharing Communities



## International Research Organisations



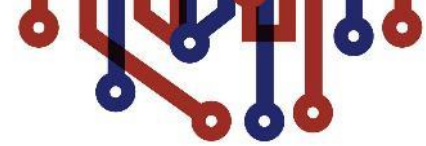
## EU Institutions



## EU Associations







# Activities & Sharing Topics

## Physical Info Sharing Community

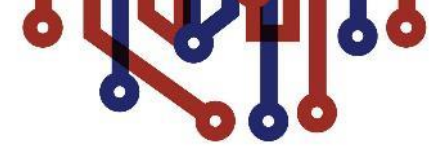
- Plenary meetings
- Community meetings
- Theme based meetings
- Open house meetings

## Digital Info Sharing Community

- Information requests / push
- Webinars
- Whitepaper

## Topics of Information Sharing

- Vulnerabilities in OT systems and critical assets
- Threat/Risk analysis information
- Incidents
- Lessons learned / best practices
- Alerts and (patch)notifications
- Use of standards (ISO, IEC, NIST, NERC etc.)
- Research (H2020) topics



# Three plenary EE-ISAC meetings per year

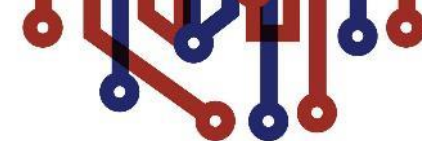


- ➔ Confidentiality (TLP Protocol)
- ➔ Transparency
- ➔ Task Forces reporting
- ➔ Led by the utilities

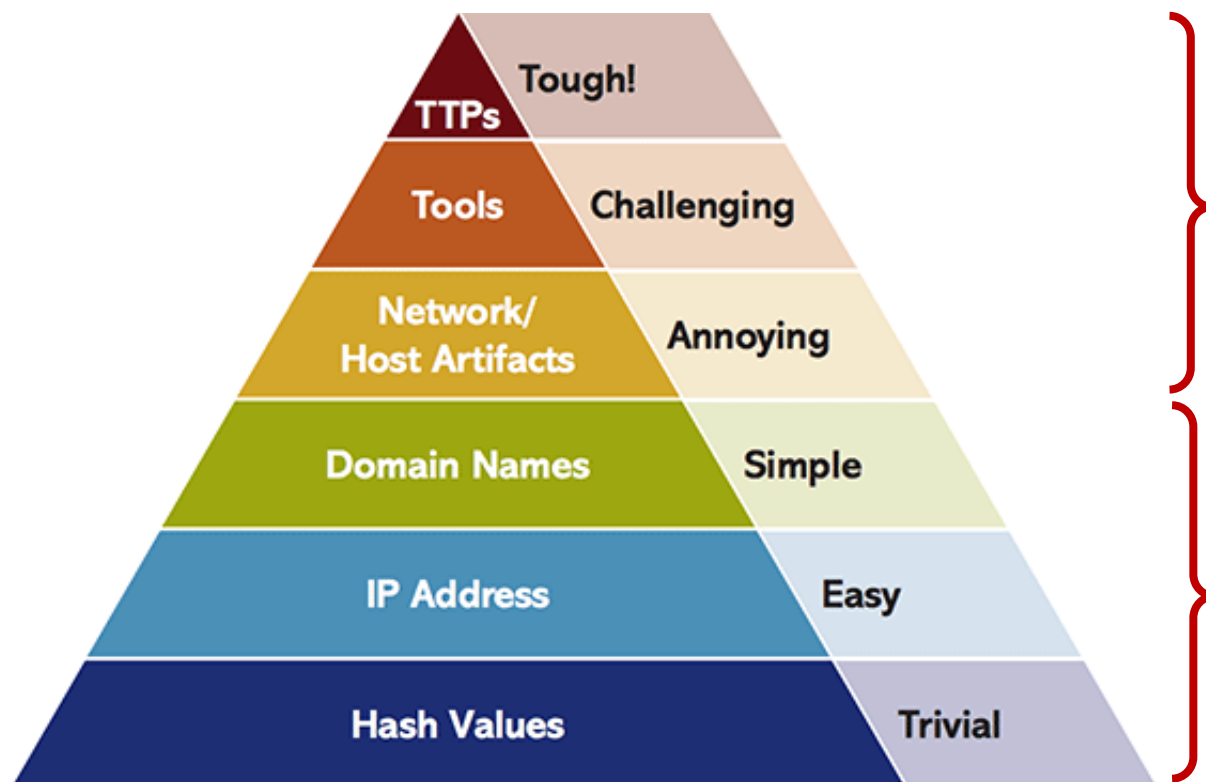
Physical

Digital

Topics



# Digital Information Sharing Platforms

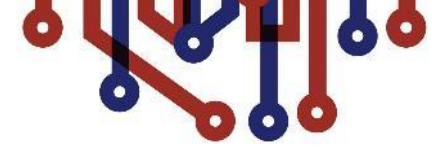


Physical

Digital

Topics

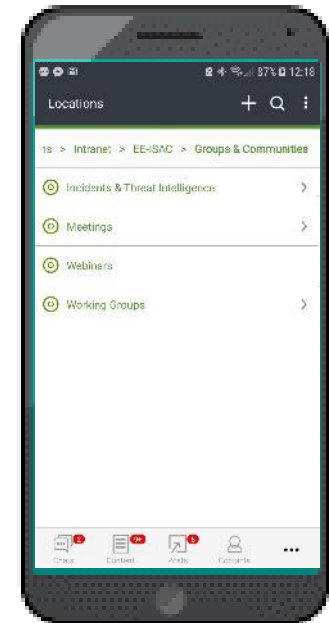




# Vmoso

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

The screenshot displays the Vmoso web interface. The top navigation bar includes a home icon, the Vmoso logo, the user name 'Massimo Rocca', a search bar, and a '+ Create' button. Below the navigation bar, there are tabs for 'Posts Stream', 'Local Search', and a document viewer. The main content area shows a feed of posts and documents. One post is titled 'Weekly CERT PSE bulletin. Jaroslaw Sordyl: Created a Post'. Another post is titled 'NESCOR Guide to Penetration Test Marcel Kulicke: Created a Post'. A document viewer is open, showing a PDF 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 decorative graphic of red and blue circuit lines.



Vmoso



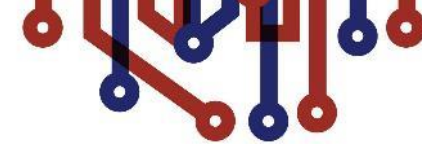
EE-ISAC

Physical

Digital

Topics





# Malware Information Sharing Platform

MISP is a de-facto standard:

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



**TLP Taxonomy Library**

ID: 5  
 Name: TLP  
 Description: The TLP (Trusted Language Protocol) or "secret" TLP, was designed with the goal to be a flexible classification scheme for sharing sensitive information while keeping the control over its distribution at the same time.  
 Version: 1  
 Enabled:  (click)

ID	Exportable	Name	Taxonomy	Tagged	Actions
6	<input checked="" type="checkbox"/>	APT		31	<input type="checkbox"/> <input type="checkbox"/>
7	<input checked="" type="checkbox"/>	Actionable-IO		5	<input type="checkbox"/> <input type="checkbox"/>
3	<input checked="" type="checkbox"/>	TLP-AMBER	tp	101	<input type="checkbox"/> <input type="checkbox"/>
8	<input checked="" type="checkbox"/>	TLP-B-COM	tp	11	<input type="checkbox"/> <input type="checkbox"/>
9	<input checked="" type="checkbox"/>	TLP-GREEN	tp	550	<input type="checkbox"/> <input type="checkbox"/>
4	<input checked="" type="checkbox"/>	TLP-RED	tp	3	<input type="checkbox"/> <input type="checkbox"/>
2	<input checked="" type="checkbox"/>	TLP-WHITE	tp	651	<input type="checkbox"/> <input type="checkbox"/>
10	<input checked="" type="checkbox"/>	TO-HIDE		2	<input type="checkbox"/> <input type="checkbox"/>
9	<input checked="" type="checkbox"/>	TODO		9	<input type="checkbox"/> <input type="checkbox"/>
11	<input checked="" type="checkbox"/>	TODO-ENFORCEMENT		8	<input type="checkbox"/> <input type="checkbox"/>
1	<input checked="" type="checkbox"/>	Trust-COMM		652	<input type="checkbox"/> <input type="checkbox"/>
18	<input checked="" type="checkbox"/>	advisory-scale-information-credibility-1	advisory-scale	0	<input type="checkbox"/> <input type="checkbox"/>
20	<input checked="" type="checkbox"/>	advisory-scale-information-credibility-2	advisory-scale	0	<input type="checkbox"/> <input type="checkbox"/>
15	<input checked="" type="checkbox"/>	advisory-scale-information-credibility-3	advisory-scale	0	<input type="checkbox"/> <input type="checkbox"/>
21	<input checked="" type="checkbox"/>	advisory-scale-information-credibility-4	advisory-scale	0	<input type="checkbox"/> <input type="checkbox"/>
22	<input checked="" type="checkbox"/>	advisory-scale-information-credibility-5	advisory-scale	0	<input type="checkbox"/> <input type="checkbox"/>
23	<input checked="" type="checkbox"/>	advisory-scale-information-credibility-6	advisory-scale	0	<input type="checkbox"/> <input type="checkbox"/>

**TLP Taxonomy Library**

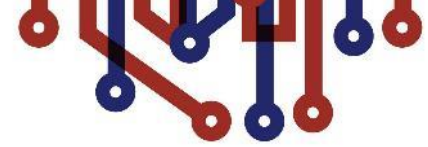
TLP-Expendable: Information is exclusively and directly given to (or group of) individual recipients. Sharing outside is not possible. 3 TLP-RED

TLP-Operational: Information is exclusively given to an organization, sharing is restricted within the organization to be effectively scaled upon. 101 TLP-AMBER

TLP-Approved: Information is given to a community or a group of organizations, at large. This information cannot be publicly released. 400 TLP-GREEN

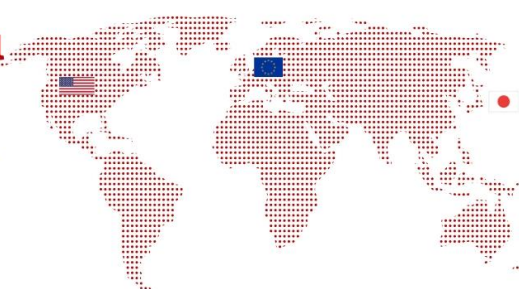
TLP-Approved: Information can be shared publicly in accordance with the law. 301 TLP-WHITE

TLP-Operational: Information is intended with a specific tag called "Channel Trust" (CT) which is specific to the tag in compliance with the information protection policy of the organization. This additional rule is at the discretion of the initial sender who can decide to apply or not the CT tag. 11 TLP-B-COM






# Global collaboration with Japan & US

**Trilateral MoU**



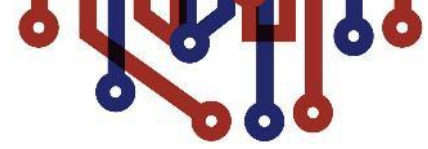
October 17  
2018  
Las Vegas


Physical

Digital

Topics



# Global & Cross sector collaboration



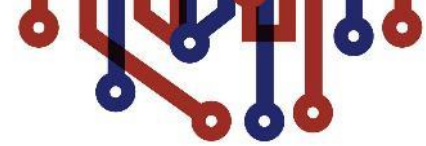
Physical

Digital

Topics







# Global & Cross sector collaboration



INTER EU ISAC group

Physical

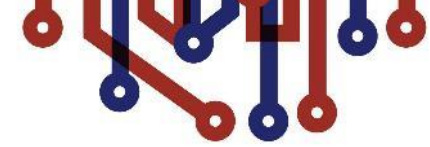
Digital

Topics



**EE-ISAC**





# Webinars

**ENISA** organizes webinars and collect surveys with the members to select the webinar topics. Past **webinars** were planned according to the following list of preferences:

- Secure Substation – **Siemens**
- Asset inventory for ICS-SCADA - **PAS ICS cybersecurity**
- Securing the human element - how to prepare your organization against phishing attacks - **CERT PSE**
- Best build-up SOC for utilities – **RambiCo**
- Discovering and Defending Against Vulnerabilities in Building Automation Systems - **Forescout**

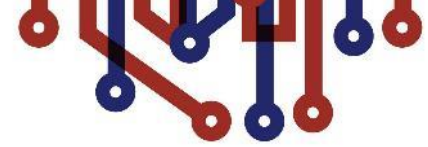


Physical

Digital

Topics





# White Papers

## Cyber Security Risk Management for Digitalized Energy Systems: Challenges & Solutions

Massimo Rocca, Stefan Schauer, Paul Smith, Reinder Wolthuis (2018)

The challenges and solutions of cyber security risk management for digitalised energy systems are presented and discussed in EE-ISAC's white paper (2018). Developed by members who are lead researchers selected from academia and the sector's solution providers, it gives an ultimate overview of standards and methodologies and that can be taken as the cutting edge for experts who are designing advanced threat identification and analysis in their companies. The tools and methods described here can offer a useful vision to work towards and contribute to more effective management of risks for the energy sector.

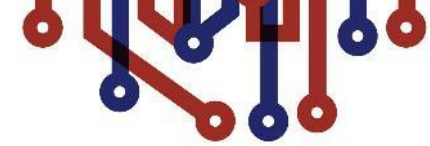
[Read the full report here!](#)



Physical

Digital

Topics



# White Papers

## Developing Novel Solutions to Realise the EE-ISAC

Rafal Leszczynski\*, Tania Wallis<sup>†</sup>, Michal R. Wróbel<sup>‡</sup>

\*Gdańsk University of Technology, Narutowicza 11/12, 80-263 Gdańsk, Poland  
<sup>†</sup>University of Strathclyde, 16 Richmond Street, Glasgow, G1 1RQ, United Kingdom

### Abstract

For more effective decision making in preparation for and response to cyber-events in the energy sector, multilevel situation awareness, from technical to strategic is essential. With an uncertain picture of evolving threats, sharing of the latest cybersecurity knowledge among all sector stakeholders can inform and improve decisions and responses. This paper describes two novel solutions proposed during the formation of the European Energy – Information Sharing & Analysis Centre (EE-ISAC) to build situation awareness and support information sharing. The development of EE-ISAC towards regular information sharing among members is described. This demonstrates the foundations achieved so far upon which a situation awareness network can be built for the energy sector.

**Keywords:** cybersecurity, situation awareness, information sharing, ISAC, critical infrastructures, power systems, energy sector

### 1. Introduction

In the last years a significant extension of the cyberthreat landscape has been observed. Modern, advanced cyberattacks are multi-vectored and multi-staged, often extending over a longer period of time (advanced persistent threats – APTs) Tsionis and Rais (2018); Shopik et al. (2016); Chen et al. (2018). Moreover,

\*Corresponding author  
 Email addresses: r.leszczynski@p.p.gda.pl (Rafal Leszczynski), tania.wallis@strath.ac.uk (Tania Wallis), wrobel@e1.pg.ubs.pl (Michal R. Wróbel)

Preprint submitted to Elsevier

January 31, 2019

## Developing Novel Solutions to Realise the EE-ISAC

Rafal Leszczynski, Tania Wallis, Michal R. Wróbel (2019)

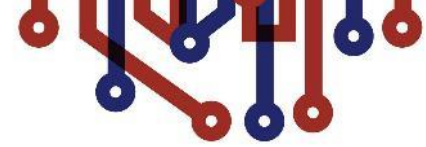
For more effective decision making in preparation for and response to cyber-events in the energy sector, multilevel situation awareness, from technical to strategic is essential. With an uncertain picture of evolving threats, sharing of the latest cybersecurity knowledge among all sector stakeholders can inform and improve decisions and responses. This paper describes two novel solutions proposed during the formation of the EE-ISAC to build situation awareness and support information sharing. The development of EE-ISAC towards regular information sharing among members is described. This demonstrates the foundations achieved so far upon which a situation awareness network can be built for the energy sector.

[Read the full report here!](#)

Physical

Digital

Topics



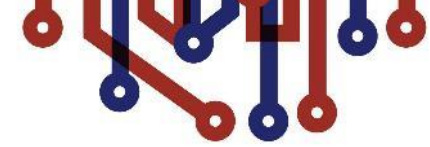
# Sharing Incident Topics

During past Plenaries, members shared reports and analysis on the following incidents:

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

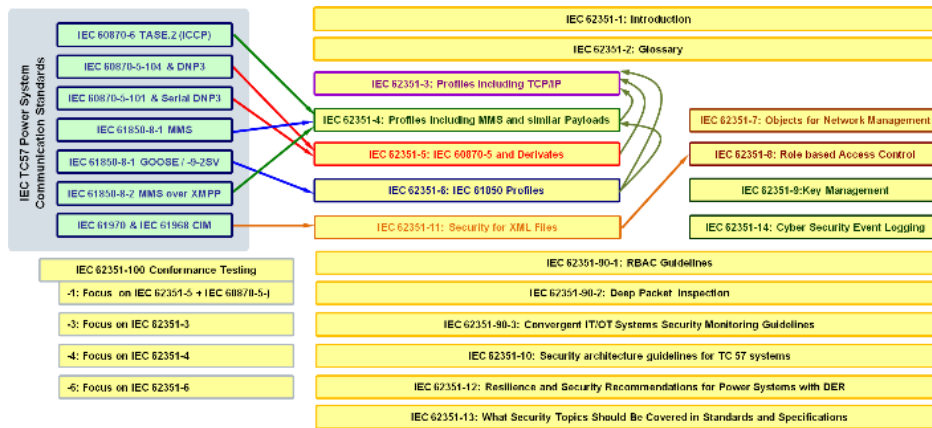






# Analysis of Standards

## EE-ISAC ran an in-depth analysis of IEC 62351 Standard



### Security means defined:

- Authentication and authorization (RBAC)
- Secure IP- based and serial communication
- Secure application level exchanges
- Security monitoring and event logging
- Test case definition
- Guidelines for applying specific security measures

### by utilizing or profiling

- existing standards and recommendations

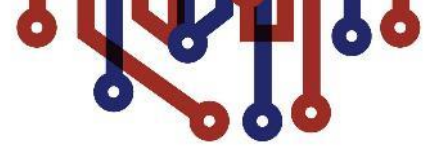
### The objective is End-to-end security:

“A set of security policies, procedures, and technologies that provides a high degree of assurance that data exchanged between a sender and a receiver is protected from unauthorized access and/or modifications, while being transferred from one end to the other through intermediate nodes.”

Physical

Digital

Topics



# 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 & PREPAREDNESS**

Physical

Digital

Topics

# Have a look online! [www.ee-isac.eu](http://www.ee-isac.eu)

[Home](#)[About EE-ISAC](#)[Members & Board](#)[Insights](#)[Contact](#)

## Bridging the gaps between disciplines



### Members

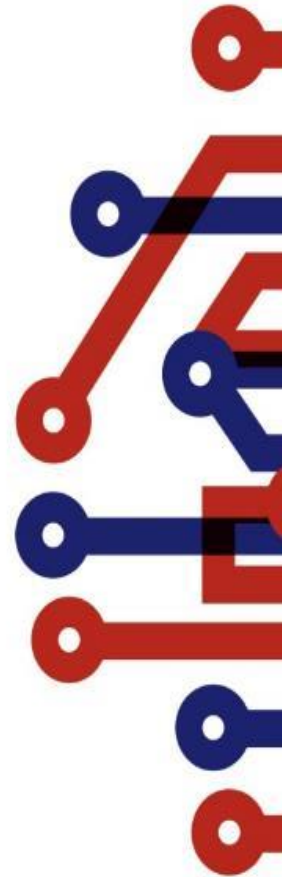
The *European Energy - Information Sharing & Analysis Centre* (EE-ISAC) brings together key industry players representing the following categories:

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](#).



# EE-ISAC

# Let's discuss further

**Johan Rambli**  
**+31611879945**

**CONTACT US**



**contact@ee-isac.eu**  
**www.ee-isac.eu**

