Building a network of trust among European Utilities
Security in a Global Energy Company

A quickly evolving scenario in the world have determined a drastic increase of the attack surface

**Market liberalization** resulting in a competitive scenario

**Globalization** of the production and sale of energy

**Interconnection with public networks** of the power distribution and production control networks

Spreading of **smart-grids** and **smart-metering systems**

**IoT world:** sensors, appliances, cars, buildings

Protection of **Critical Infrastructure** and compliance to NIS Directive

**CERT** creation is a must

You can buy or rent, affordable malware packages, especially Trojans (e.g., Zeus), Zero-day exploits, but also tutorials and online manuals for implementation: the same exploit kit may costs between 1000 $ - 2000 $ and could be rented for $200 - $600 per week or 600 $ -1200 $ per month,

(source CINI – Italian Cybersecurity National Lab)
Security in a Global Energy Company

According to a recent report by McKinsey, \textbf{75\% of Top Executives considers cyber security one of the priorities to address},

but only \textbf{16\%} of these states that they have a well-prepared organization to meet this challenge.

The growth of cyber attacks, the increase in level of sophistication and media coverage, have led to a significant \textit{increase of the awareness} in companies about the risks associated with this type of threat.
Security Management

Success factors

- **Do not wait** for something to happen
- Collect and interpret the "**weak signals**"
- Evaluate trends in threats and **weak points** in the organization

- Talk internally with **all the components** of the organization
- Knowing the business and the **strategic objectives** of the company
- Analyze the **external context**

- Define and implement a security-oriented **behavior model** (not just "rules")
- Promoting training: teaching "**know how**" and not "knowing how"

- Define, measure and **monitor performance indicators**, useful for continuous improvement
Security Management

Process steps

- Intelligence
- Risk assessment and evaluation
- Incident and critical events management

Risk mitigation:
- People protection
- Infrastructures protection
- Intangible assets protection

- Residual risk evaluation
- Event detection
Internal CERT

Main activities

1. Cyber Incident Response
   - Key process to Prevent, Detect and Respond to Cyber Incidents.
   - Key aspects:
     - Inclusive of all multi disciplinary roles and capabilities
     - Full integration policies (i.e. Emergency and Crisis Policy)

2. Cyber Threat Surveillance
   - Process to harvest privileged information related to cyber threats and attacking actors from multiple open, closed and commercial sources.
   - Key aspects:
     - Create actionable information, relevant for early warning
     - Early detection of cyber threats with potential impact to Constituency

3. CERT Information Sharing
   - Trusted communication process among all involved Internal Stakeholders and related External Counterparts.
   - Key aspects:
     - CERT Communication Workflow and Information Dissemination
     - Confidentiality management (Traffic Light Protocol)
The private operator of critical infrastructures has reduced autonomy in mitigating risks and in countering threats due to:

- limited resources
- nature of threats
- legal implications
- influence on the supply chain
Information sharing in network of trust
EE-ISAC launched in December 2015
EE-ISAC starts from an EU project

EE-ISAC is the outcome of Distributed Energy Security Knowledge (DENSEK) project, which had the objectives of Improving the 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);
- Information Sharing Platform;
- Situational Awareness Network.

The EE-ISAC:
- Enables an interactive information sharing community;
- Is operational as a Belgian no-profit since November 2015.
EE-ISAC today

23 MEMBERS
Utilities
Vendors
EU/Public Bodies
Academia
Research Labs

10 EVENTS
Signed agreements with Japan E-ISAC & US E-ISAC

10 TASK FORCES
1 Published White Paper
3 Expected Webinars
Main focus of the EE-ISAC

- A closed community of communities
  - 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
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 IT and OT systems
- Threat/Risk analysis information
- Incidents
- Lessons learned / best practices
- Alerts and (patch)notifications
- Use of standards (ISO, IEC, NIST, NERC etc.)
- Research (H2020) topics
Community meetings

- Confidentiality (TLP protocol)
- Transparency
- Task forces monitoring
- Lead by the utilities
## EE-ISAC members, agreements and relations

### International info-sharing communities
- EASE
- KRAFT
- JE-ISAC
- US E-ISAC
- ICS-ISAC
- Energy-ISAC NL

### EU Institutions
- DG ENER
- DG CONNECT

### EU Associations
- EDSO for smart grids
- ECSO

### International Organisations
- OECD
- WEF
- USAID
- EPRI

### Topics of Information Sharing

**Physical Info Sharing Community**

**Digital Info Sharing Community**

**Topics of Information Sharing**
Activities & channels

Ready for the European Resilient Cyber Security Single Market?

October 18, 2018 - The European Energy Information Sharing & Analysis Center (EE-ISAC) has organized at the European Parliament its first conference titled “Ready for the European Resilient Cyber Security Single Market?” to debate with DG ENER, DG CNECT and ENSI for Smart Grids on the future of cybersecurity in the Energy sector. The conference has been co-organized in the framework of the European Cyber Security Month (ECySM) to raise awareness on cyber threats, promote cyber security among citizens and organizations as well as resources to be protected online, through education and sharing of good practices.

During the conference the first EE-ISAC white paper on Cyber Security Risk has been presented as well as the multilateral agreement to be signed the day after with the US E-ISAC and Japanese E-ISAC in Las Vegas, and those recently signed with the Energy Analytic Security Exchange (EAIE) and the Norwegian KraftCERT organization.

Physical Info Sharing Community  Digital Info Sharing Community  Topics of Information Sharing
Digital info sharing community

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
Our sharing platform, powered by BroadVision, permits to share documents, posts and chat among members and external peers.
ENISA organizes surveys with the Members to select the webinar topics. This year the webinars were planned according to the following list of preferences:

1. Secure Substation – Siemens

2. Asset inventory for ICS-SCADA - PAS ICS cybersecurity

3. Securing the human element - how to prepare your organization against phishing attacks - CERT PSE
EE-ISAC promotes secure by design

EE-ISAC run an in-depth analysis of IEC 62351 Standard

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.”

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
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

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.