Cybersecurity Risk Assessment and Management for Energy Sector

CSP003_S_E

PRESENTATION BY:

- **CRISTINA ALCARAZ**, UNIVERSITY OF MALAGA, SPAIN

Acknowledgement

- *Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.*
- *Project Agreement no. 101083594*

Protecting Charging Stations Against Specific Threats

01. Goals: Who-What-Why you need to take this training

02. Training logistics: When-Where-How

03. Learning outcomes

04. Training outlines

05. Exercises details

06. Practical information and requirements

07. Registration information and contacts

Goals: Who-What-Why you need to take this training

WHO

Anyone interested in learning about risk assessment and management applied to the energy sector, such as managers and directives. industrial engineers and IT/OT administrators, higher education students and cybersecurity aspirants

WHAT

Establishes the basis (though in a basic level) for understanding the relevance of cybersecurity in a specific field of the energy sector

WHY

To equip participants with the knowledge and skills to identify and implement risk management strategies, thereby helping to protect critical systems, their network infrastructures, data and critical resources

CSP Training Logistic: When-Where-How

WHEN

As the module is held several times, it is advisable to check the CyberSecPro DCM platform for updated information

2 hours in total

WHERE

Online, physical or both

All information on the connection mode will be published the DCM system

HOW

A module based on **synchronous classes** where each trainer will explain specific topics, and at the end of the seminar various activities will be proposed as two evaluation tests

Value Propositions

Benefits to Participants

- Exploration of a specific, but very common, field of application within the **Energy Sector**
- Level of training module: **Basic**
- **Cybersecurity professional training** in the field of energy control networks
- **Use case analysis and scenario analysis**
- Rooted with **European cybersecurity skills frameworks**
- Cutting-edge insights from industry-academic experts
- Providing **adequate support for skills development and career advancement**

WHO

Profile of Training Participants

- Network engineers
- IT/OT administrators
- Energy professionals, including operators, managers and directives, energy suppliers, and employees in general of the corporate network
- Researchers, educators and students
- Cybersecurity practitioners
- Cybersecurity enthusiasts

WHO

Profile of Trainer

- **Cristina Alcaraz**
  Associate Professor at University of Malaga, PhD. in computer Science with extended experience on cybersecurity and critical infrastructure protection in power grids and Smart Grids
- **Artsiom Yautsiukhim**
  Researcher at CNR, Italy, with extensive experience in cybersecurity, risk management and smart grid environments
- **Javier Lopez**
  Full Professor at University of Malaga, PhD. in computer Science with extended experience on cybersecurity and critical infrastructure protection

WHAT

Training Topics

- Threats and Vulnerabilities for Energy Sector
- Risk Assessment and Management Processes and Methodologies for Energy Sector

WHY (Knowledge)

Learning Outcomes

- **Knowledge of** risk management and its assessment for specific critical sectors such as energy and its operational systems
- **Knowledge of** phases and principles for an effective risk management methodology
- **Knowledge of** cyber threats, taxonomies and vulnerabilities repositories
- **Knowledge of** technical and organisational controls that appropriately mitigate cybersecurity risks in the energy sector and its operational systems

WHY-2 (Practical Skills)

Learning Outcomes

- **Identify and know** to apply an appropriate methodology for information security risk management and risk assessment according to the specific characteristics of the energy scenario

Training Outline

Trainers, sessions and estimated hours

Topic-1: Threats and Vulnerabilities for Energy Sector

- Cristina Alcaraz, Javier Lopez and Artsiom Yautsiukhim
- Session: approx. 1h

Topic-2: Common Security Weaknesses and Attacks in Energy Control Networks

- Artsiom Yautsiukhim, Cristina Alcaraz
- Session: approx. 1h, including activities

Topic-1: Threats and Vulnerabilities for Energy Sector

We will cover these skills

- Vulnerabilities for the energy sector, detailing various cyber security threats caused by internal and external attackers, as well as incidental and casual threats

- Security controls for the energy sector, considering some examples provided by ISO 27002

Topic-2: Risk Assessment and Management Processes and Methodologies for Energy Sector

We will cover these skills

- Risk assessment, related terms and process
- Risk analysis, describing the different forms of risk analysis and ways to perform it
- Tools for risk assessment
- Risk treatment to reduce risks or effects

Activities

Various types of activities will be offered throughout the entire module:

- **Analysis of case studies** focused on the energy sector

- **Evaluation tests**, one launched at the beginning of the seminar (pre-assessment), and another at the end of the seminar (post-assessment)

Evaluation method

Outline the evaluation elements and assessment process

Evaluation Element	How	Notes
Final report about a use case (REQUIRED)	Individual report submitted on time	Required analysis and discussion about a specific topic
Tests (REQUIRED)	Assessment test, which may integrate case studies where learners must show practical knowledge	In presence of the trainers (approx. 10-15 minutes)

Background Knowledge and Prerequisites

Background knowledge:

- Knowledge of cybersecurity fundamentals

Prerequisites:

- Basic knowledge of IT and cybersecurity essentials

Technical Tools and Other Requirement

Technical Tools

- Computer with Internet access for connection
- Access to the DCM platform
- Office software for reports

Other Requirements

- **Willingness to learn and experiment**
- **Active Participation**

Resources: Books and Reference Materials

1. ENISA, CIRAS, 2024
   URL: https://ciras.enisa.europa.eu

2. MITRE, MITRE CVE, 2024
   URL: https://cve.mitre.org

3. Figure source: MITRE, MITRE CVE, 2024
   URL: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=modbus

4. Source: NIST, NVD, 2024
   URL: https://nvd.nist.gov

5. Zografopoulos, Ioannis, Nikos D. Hatziargyriou, and Charalambos Konstantinou. "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations", IEEE Systems Journal (2023)

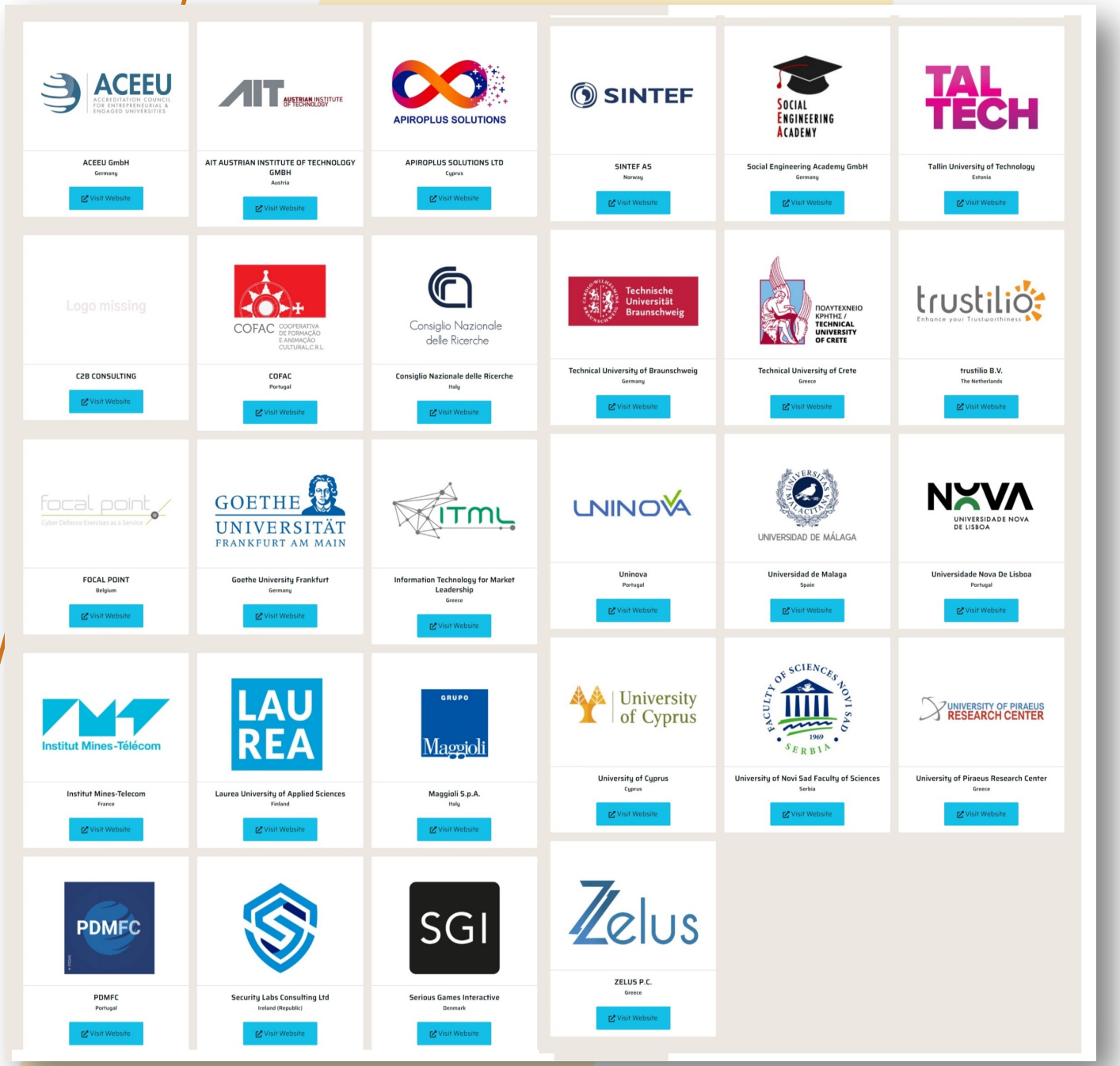
Registration: How to register and other practical information

The specific registration process may vary depending on the training provider, institution, or access conditions established for each module

Nonetheless, the general steps are explicitly detailed in the **DCM platform**

Connect with CyberSecPro:
How to register and other practical information

1. Website: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/



Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Thank you

If you have any questions, please do not hesitate to contact us:

- Cristina Alcaraz
  alcaraz@uma.es