
# Cybersecurity Essentials and Management for the Energy Sector

# CSP001_C_E

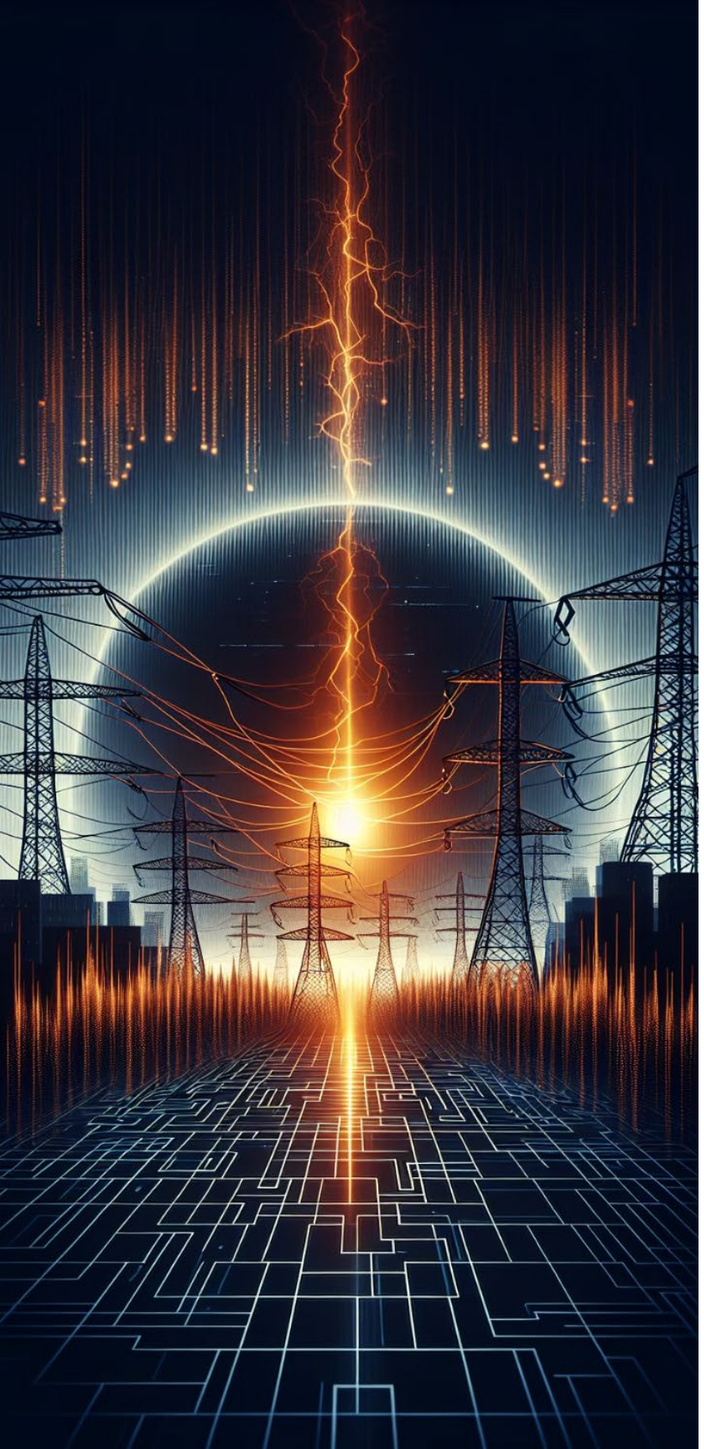
PRESENTATION BY:
Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin

CyberSecPro


# Acknowledgement


- 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


CyberSecPro

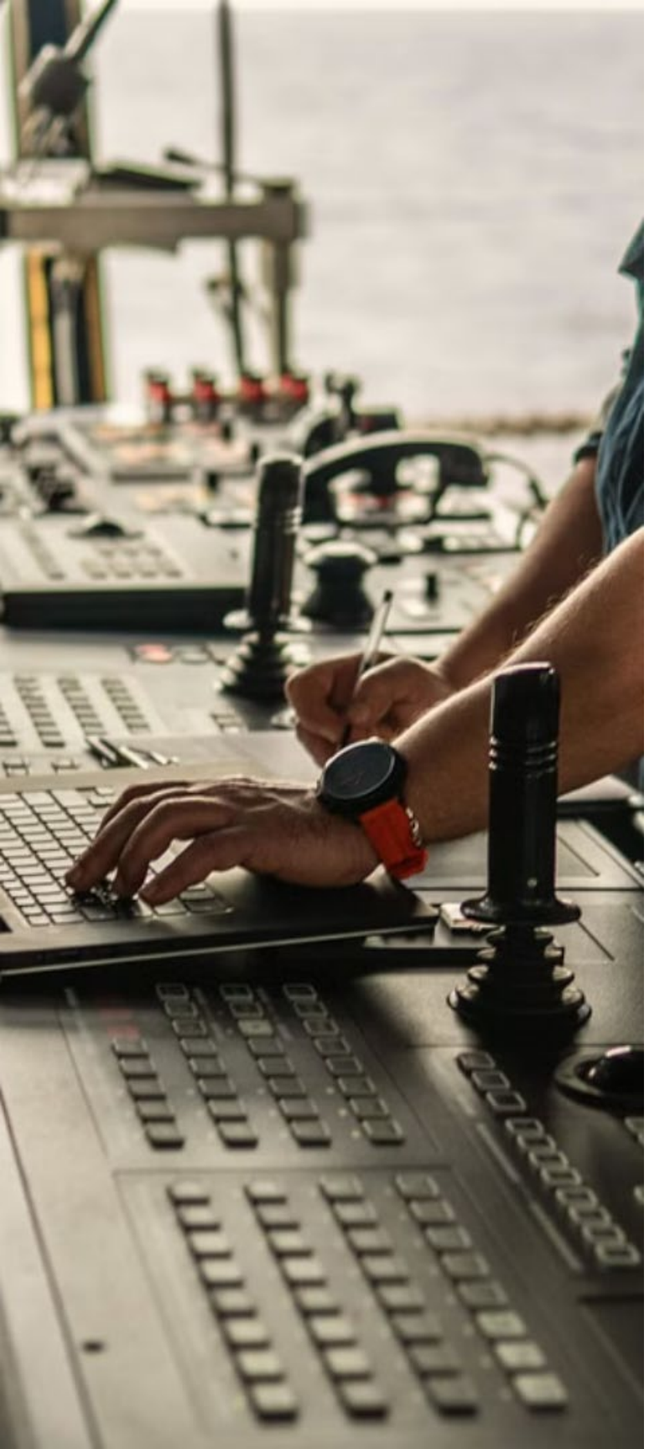


CyberSecPro Professional Training Module-1:

# Cybersecurity Essentials and Management for Energy Sector

Welcome to CyberSecPro's comprehensive training module that equips energy professionals with the essential with the essential knowledge and skills to defend against evolving cyber threats. Tailored specifically for the specifically for the energy industry, this program addresses the unique challenges faced by energy providers, energy providers, arming you with the tools necessary to safeguard critical infrastructure and operations. Get operations. Get ready to embark on a journey through the intricate world of cybersecurity, learning from learning from trainers, industry experts and gaining a deep understanding of the cyber landscape targeting targeting energy infrastructure.

Trainers: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin



# Understanding the Importance of Cybersecurity in Energy Sector

1

## Essential Knowledge

Participants will gain essential knowledge to identify, prevent, and respond to cyber threats, ensuring the safety and security of energy infrastructures.

2

## Accessible Learning

The program is crafted to be accessible for individuals with a basic understanding of computers and network.

3

## Comprehensive Overview

By the end of this module, learners will have a comprehensive overview of cybersecurity's role in the energy environment.

Trainers: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin

# Meet Your Trainers

## Paresh Rathod

Specializing in Cybersecurity Education and Thematic RDI Leader at Laurea, Finland. He  brings a wealth of knowledge to the technology and training

## Pasi Kämppi

Specializing in Cybersecurity Education and Degree Coordinator at Laurea, Finland. He  brings a wealth of knowledge to the network infrastructure and training

## Cristina Alcaraz

Specializing in Cybersecurity and currently a Marie-Curie postdoctoral and associate professor, working in the Network, Information and Computer Security (NICS) Lab research group at the University of Malaga (UMA)

## Stylianos Karagiannis

Technical Expert in PDM, Portugal, contributing practical insights. Possesses a robust academic background and practical expertise in cyber ranges and attack-defend security scenarios.

# Meet Your Trainers

## Ricardo Gregorio Lugo

Specializing in Human Aspects of the Cybersecurity Education and Post-doctoral and senior researcher at TalTech, Estonian Maritime Academy.

## Kitty Kioskli

Specializing in Human Aspects of the Cybersecurity Education and CEO and co-founder of trustilio BV, Netherlands. She holds a Ph.D. in Health Psychology from King’s College London.

## Paulinus Ofem

Specializing in Cybersecurity and currently also a project manager in EU AI project-MONELO at Laurea, Finland.

## Louise Præstiin

Game Designer in SGI, Denmark, contributing practical insights using games in cybersecurity scenarios.

# CyberSecPro Trainers

# Who Should Attend?

## 1 Higher Education Students

Higher education students (EQF Level 6, 7 or higher) and future talent aspiring career in technologies and/or critical sectors cybersecurity

## 2 ICT Personnel

Individuals in energy companies and authorities will understand how to manage cyber risks.

## 3 Energy Security Professionals

Those responsible for port and terminal security will deepen their knowledge of cyber threats.

## 4 Newcomers to Energy Cybersecurity

Aspiring professionals will acquire a foundational understanding of cybersecurity in the energy sector.


Trainers: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin


# Value Propositions

## Benefits to Participants

- Level of Training Module: Basic / Advance
- Cybersecurity Professional Training
- Hands-on and Practical Skills Development
- Rooted with European Cybersecurity Skills Framework
- Cutting-edge insights from industry-academic experts
- Certificate of the completion
- Helps with skills development and career advancement

Trainers: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin

# Training Syllabus Overview

1 **Topic-1**
Ethical Conduct and Professionalism in Cybersecurity Field

2 **Topic-2**
Foundational Knowledge of Cybersecurity and Body of Knowledge

3 **Topic-3**
Threats and vulnerabilities (including Energy sector specific)

4 **Topic-4**
Human Factor Considerations in Cybersecurity

5 **Topic-5**
Secure Architecture Design and Implementation



Trainers: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin

CyberSecPro

# Training Syllabus Overview

6 **Topic-6**

Security Controls Selection and Implementation

7 **Topic-7**

Data security and Privacy by design (SDPbd) for the energy sector

8 **Topic-8**

Cybersecurity Governance for Energy Organizations

9 **Topic-9**

Energy Cybersecurity Compliance and Regulations

10 **Topic-10**

Transferable Skills and Continuous Learning in Cybersecurity Profession

CyberSecPro

Trainers: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin

# Expected Outcomes

## Foundation Concepts

Describe the fundamental concepts of cybersecurity and their importance in the energy sector.

## Common Threats

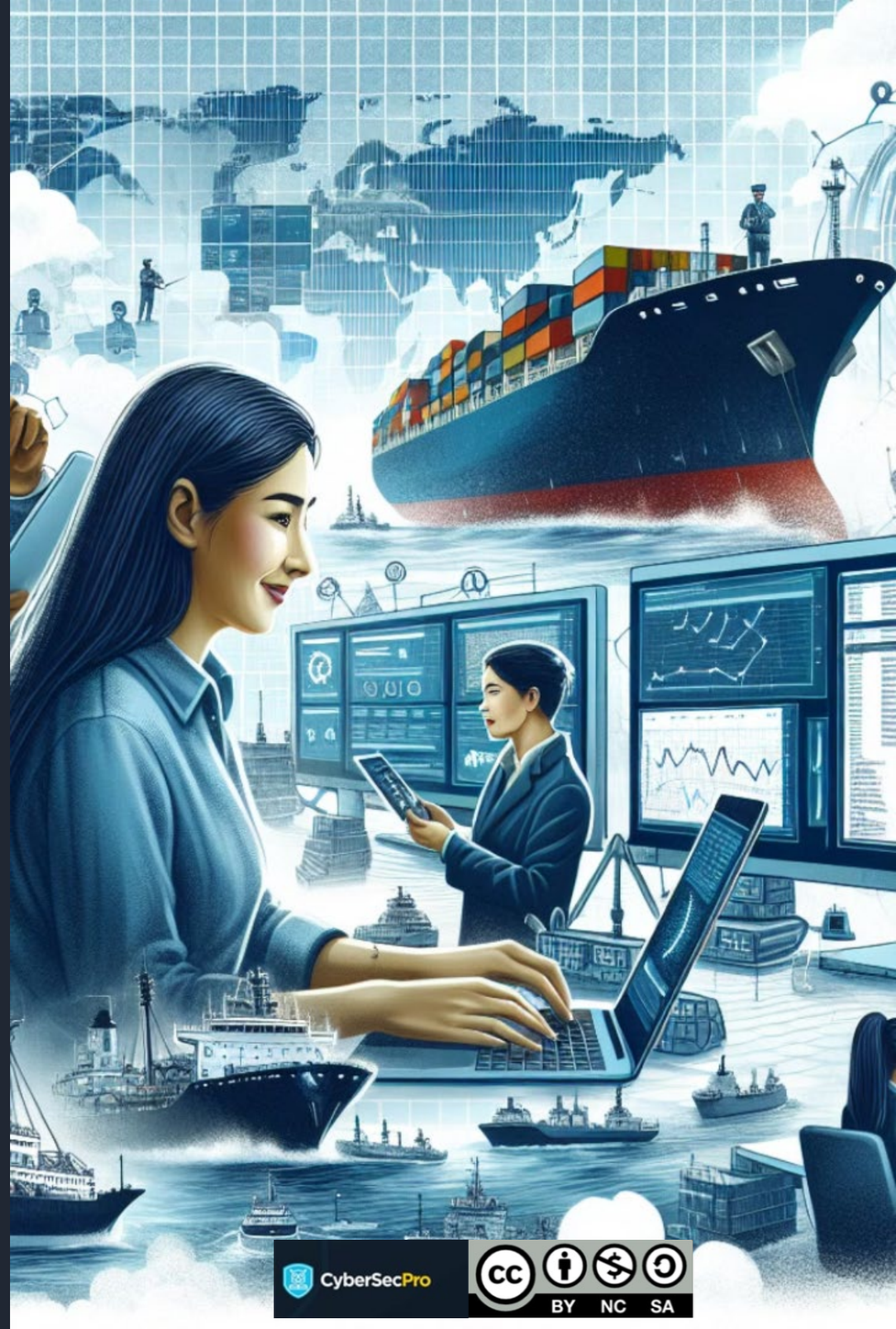
Identify common cyber threats, vulnerabilities, and risks specific to energy sector

## Impact of Cyberattacks

Explain the impact of cyberattacks on energy security.

## Best Practices

Apply cybersecurity best practices for securing energy systems and networks.




Trainers: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin

# Ethical Conduct and Professionalism

## Ethics and Integrity

Develop an unwavering ethical foundation, fostering trust, accountability, and responsible behavior in the cybersecurity domain.

## Professional Conduct

Uphold the highest standards of of professional conduct, demonstrating respect, objectivity, objectivity, and dedication to safeguarding critical energy systems. systems.

## Confidentiality and Privacy Privacy

Prioritize the protection of sensitive sensitive information, ensuring confidentiality and preserving the the privacy of individuals and organizations.

Trainers: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin

# Cybersecurity Fundamentals

1

## Defining Cybersecurity

Explore the essence of cybersecurity, its significance in the energy sector, and the crucial role it plays in protecting critical infrastructure and operations.

2

## Threat Landscape

Gain insights into the evolving threat landscape, including industry-specific threats, vulnerabilities targeting SCADA systems, smart grids, and other critical energy assets.

3

## Risk Management

Master the principles of cybersecurity risk management, enabling you to identify, assess, and mitigate risks effectively within the energy sector.

Trainers: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin

# Secure Architecture and Controls

## Network Security

Delve into the principles of network segmentation, firewall configuration, and access control, learning how to design and implement secure network architectures for energy systems.

## Data and Access Security

Explore the importance of password security, multi-factor authentication (MFA), data encryption, and patch management, ensuring the protection of sensitive information and systems.

## Security Controls

Learn to deploy and manage essential security controls for energy systems, including intrusion detection and prevention systems, antivirus software, and other protective measures.

Trainers: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin

# Incident Response and Business Continuity

1

## Preparation

Develop comprehensive incident response plans and procedures tailored to the energy sector, ensuring readiness for potential cyber incidents.

2

## Detection and Analysis

Enhance your ability to detect and analyze cyber threats, leveraging advanced monitoring tools and techniques to identify potential incidents promptly.

3

## Containment and Eradication

Implement effective containment and eradication strategies to minimize the impact of cyber incidents and restore normal operations efficiently.

4

## Recovery and Resilience

Establish robust recovery and resilience measures, ensuring business continuity and minimizing downtime in the event of a successful cyber attack.

Trainers: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin

# Compliance and Regulations

## 1 Industry Standards

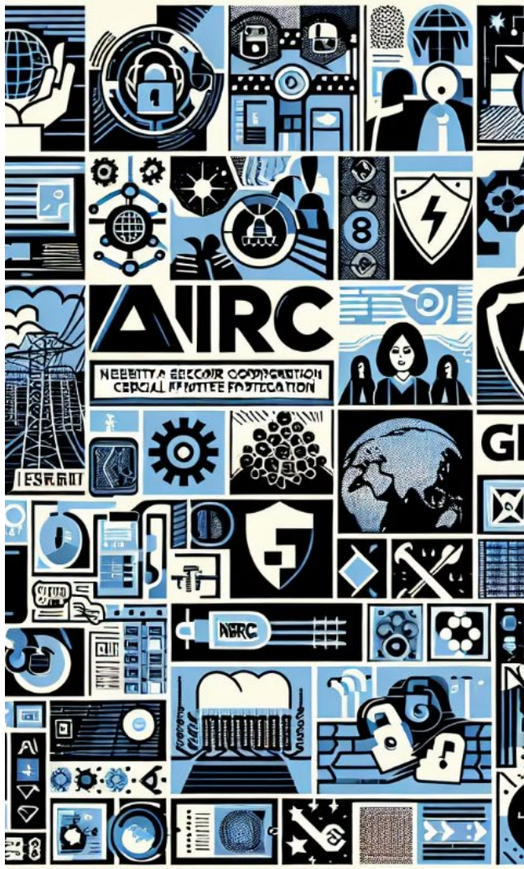
Gain insight into industry-specific standards and best practices, such as the NERC Critical Infrastructure Protection (CIP) standards, ensuring compliance and adherence to regulatory requirements.

## 2 Data Privacy and Protection

Understand the importance of data privacy and protection regulations, including the General Data Protection Regulation (GDPR) and sector-specific laws, ensuring the secure handling of sensitive information.

## 3 Audit and Reporting

Learn effective audit and reporting processes, enabling you to demonstrate compliance, identify areas for improvement, and communicate cybersecurity measures effectively to stakeholders.




Trainers: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin

# Human Factor in Cybersecurity

## Awareness and Training

Recognize the pivotal role of human awareness and training in cybersecurity, equipping employees with the knowledge and skills to identify and mitigate risks, fostering a culture of security within the organization.

## Social Engineering

Explore the techniques employed in social engineering attacks, such as phishing, pretexting, and baiting, and develop countermeasures to protect against these threats.

## Insider Threats

Understand the risks posed by insider threats, whether intentional or unintentional, and implement strategies to detect, prevent, and respond to such incidents effectively.

## Access Management

Learn best practices for access management, including principles of least privilege, separation of duties, and user lifecycle management, to mitigate the risks associated with human factors.

Trainers: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin

# Cybersecurity Governance

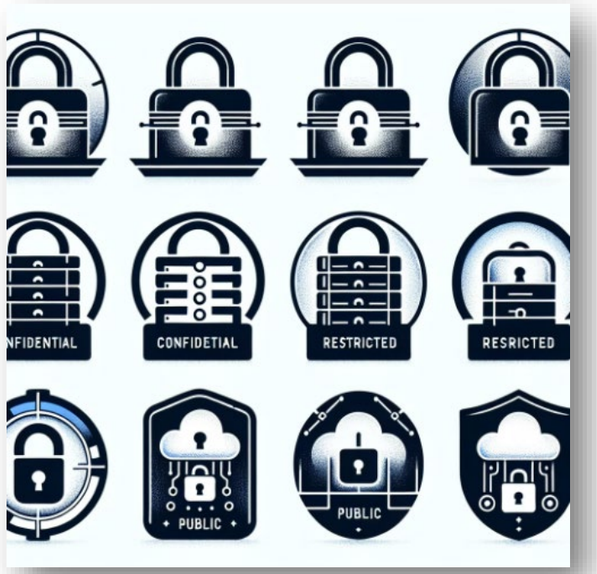
| Aspect | Description |
| --- | --- |
| Policies and Procedures | Develop and implement comprehensive cybersecurity policies and procedures tailored to the energy sector, providing a framework for effective security management. |
| Risk Management | Establish a robust risk management process, identifying, assessing, and mitigating cybersecurity risks to critical energy infrastructure and operations. |
| Roles and Responsibilities | Define clear roles and responsibilities for cybersecurity within the organization, ensuring accountability and effective coordination of security efforts. |
| Continuous Improvement | Foster a culture of continuous improvement, regularly reviewing and updating cybersecurity measures to stay ahead of evolving threats and industry best practices. |

Trainers: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin

# Data Security and Privacy by Design

## Data Classification

Implement a comprehensive data classification system, ensuring proper handling and protection of sensitive information based on its criticality and sensitivity.




## Encryption and Key Management

Explore encryption techniques and key management practices, safeguarding data at rest, in transit, and in use, while ensuring secure access and storage of encryption keys.

## Privacy by Design

Incorporate privacy principles and data protection measures into the design and implementation of energy systems, ensuring compliance with regulations and safeguarding individual privacy.

Trainers: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin

# Continuous Learning and Professional Development

1

2

3

4

**Threat Intelligence**

Stay informed about the latest cybersecurity threats, vulnerabilities, and attack vectors specific to the energy sector by leveraging threat intelligence sources and industry reports.

**Industry Collaboration**

Engage in industry collaboration and knowledge sharing, participating in conferences, workshops, and professional communities to exchange best practices and lessons learned.

**Certifications and Training**

Pursue relevant certifications and continuous training opportunities to enhance your skills, stay up-to-date with emerging technologies and trends, and maintain a competitive edge in the cybersecurity field.

**Research and Innovation**

Contribute to research and innovation efforts, exploring new technologies, methodologies, and solutions to address the evolving cybersecurity challenges faced by the energy sector.

Trainers: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin

# Real-World Case Studies

## 1 Stuxnet Attack

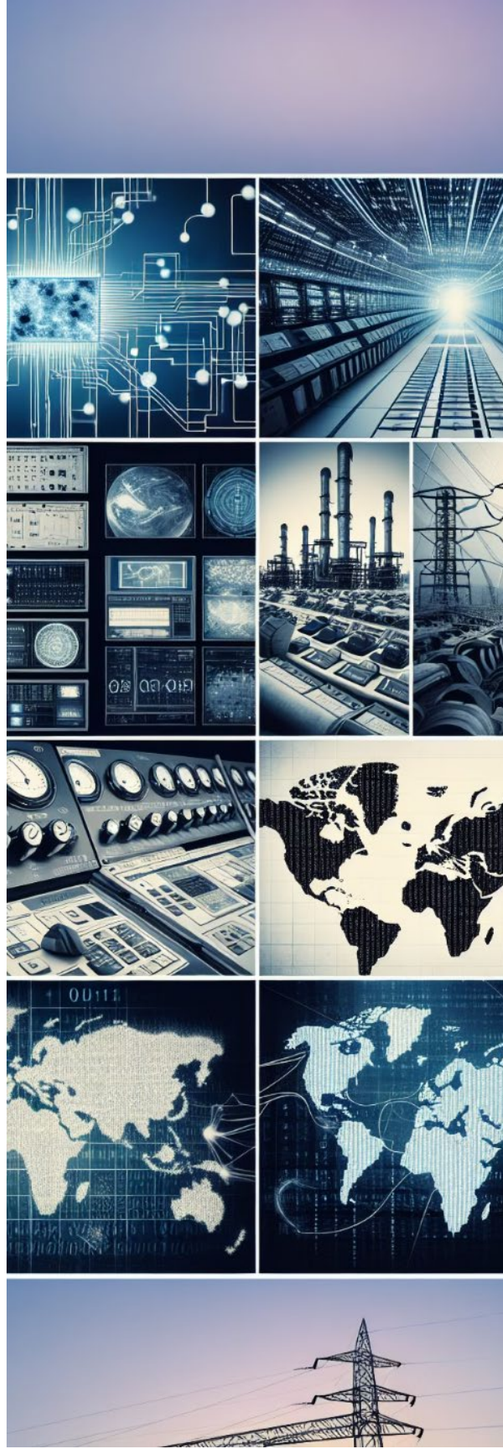
Analyze the notorious Stuxnet attack, a sophisticated malware targeting industrial control systems, and its implications for the energy sector, drawing valuable lessons for incident response and preparedness.

## 2 Colonial Pipeline Ransomware Attack

Explore the high-profile ransomware attack on the Colonial Pipeline Company, which disrupted fuel supply across the United States, and examine the measures taken to mitigate the impact and enhance cybersecurity measures.

## 3 Ukraine Power Grid Cyber Attack

Investigate the cyber attacks targeting Ukraine's power grid, which resulted in widespread power outages, and study the techniques employed by the attackers and the subsequent defensive measures implemented.



Trainers: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin

# Hands-On Activities and Simulations

## Hands-on Practices

Engage in hands-on activities and scenarios focused on network security, where you will learn foundation of how to implement secure network architectures, configure firewalls, and practice access control measures.

## Game Based Learning

Participate in a realistic game-based learning, where you will apply your knowledge and skills in detecting, analyzing, and responding to simulated cyber attacks on energy infrastructure.

## Scenarios

Various scenario base learning during the entire CSP module training by instructors and provided materials. This gives insights on real-work situation.

Trainers: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin

# Matching with ECSF CISO Profile

| CSP Module-1 Topic | ECSF CISO Tasks | ECSF CISO Skills | ECSF CISO Knowledge |
|---|---|---|---|
| Topic-1: Ethical Conduct and Professionalism | Define, implement, communicate and maintain cybersecurity goals, requirements, strategies, policies, aligned with the business strategy to support the organisational objectives | Assess and enhance an organisation's cybersecurity posture | Cybersecurity policies |
| Topic-2: Foundational Knowledge of Cybersecurity | Develop, champion and lead the execution of a cybersecurity strategy | Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks | Cybersecurity standards, methodologies and frameworks |
| Topic-2: Cybersecurity Body of Knowledge | Monitor advancement in cybersecurity | Analyse and comply with cybersecurity-related laws, regulations and legislations | Cybersecurity related laws, regulations and legislations |
| Topic-3: Threats and vulnerabilities | Identify and solve cybersecurity-related issues | Analyse and implement cybersecurity recommendations and best practices | Cybersecurity recommendations and best practices |
| Topic-4: Human Factor Considerations | Develop relationships with cybersecurity-related authorities and communities | Identify and enhance an organisation's cybersecurity posture | Ethical cybersecurity organisation requirements |
| Topic-5: Secure Architecture Design and Implementation | Review, plan and allocate appropriate cybersecurity resources | Manage cybersecurity resources | Cybersecurity procedures |

# Matching with ECSF CISO Profile

| CSP Module-1 Topic | ECSF CISO Tasks | ECSF CISO Skills | ECSF CISO Knowledge |
|---|---|---|---|
| Topic-6: Security Controls Selection and Implementation | Review and enhance security documents, reports, SLAs and ensure the security objectives | Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing | Cybersecurity policies |
| Topic-7: Data Security and Privacy by Design | Establish a cybersecurity plan | Implement cybersecurity recommendations and best practices | Cybersecurity recommendations and best practices |
| Topic-8: Information Security Governance (ISG) and Information Security Risk Management (ISRM) | Negotiate the cybersecurity budget with the senior management | Manage cybersecurity resources | Risk management standards, methodologies and frameworks |
| Topic-9: Security Auditing and Compliance | Communicate, coordinate and cooperate with internal and external stakeholders | Anticipate required changes to the organisation's information security strategy and formulate new plans | Cybersecurity auditing standards, procedures, and guidelines |
| Topic-9: Legal and Ethical Compliance | Anticipate cybersecurity threats, needs and upcoming challenges | Ensure the senior management approves the cybersecurity risks of the organisation | Ethical cybersecurity organisation requirements |
| Topic-9: Security Management Standards and Frameworks | Motivate and encourage people | | |

# References


1. European Union Agency for Cybersecurity. (2022). ECSF, European cybersecurity skills framework. Publications Office. https://doi.org/10.2824/859537
2. R. Schoon and S. Kleinaltepohl, Cybersecurity in the Electricity Sector: Managing Critical Infrastructure (SpringerLink, 2018).
3. J. R. Vacca, Industrial Cybersecurity for Engineers (Elsevier, 2015).
4. ECSO, “Energy Networks and Smart Grids”, Cyber Security for the Energy Sector, WG3, Sectoral Demand, November 2018 URL: https://ecs-org.eu/ecso-uploads/2022/10/5fdb2673903c6.pdf
5. ENISA, “Smart Grid Threat Landscape and Good Practice Guide”, December 2013 URL: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide
6. Other references listed in each topics of the CSP module

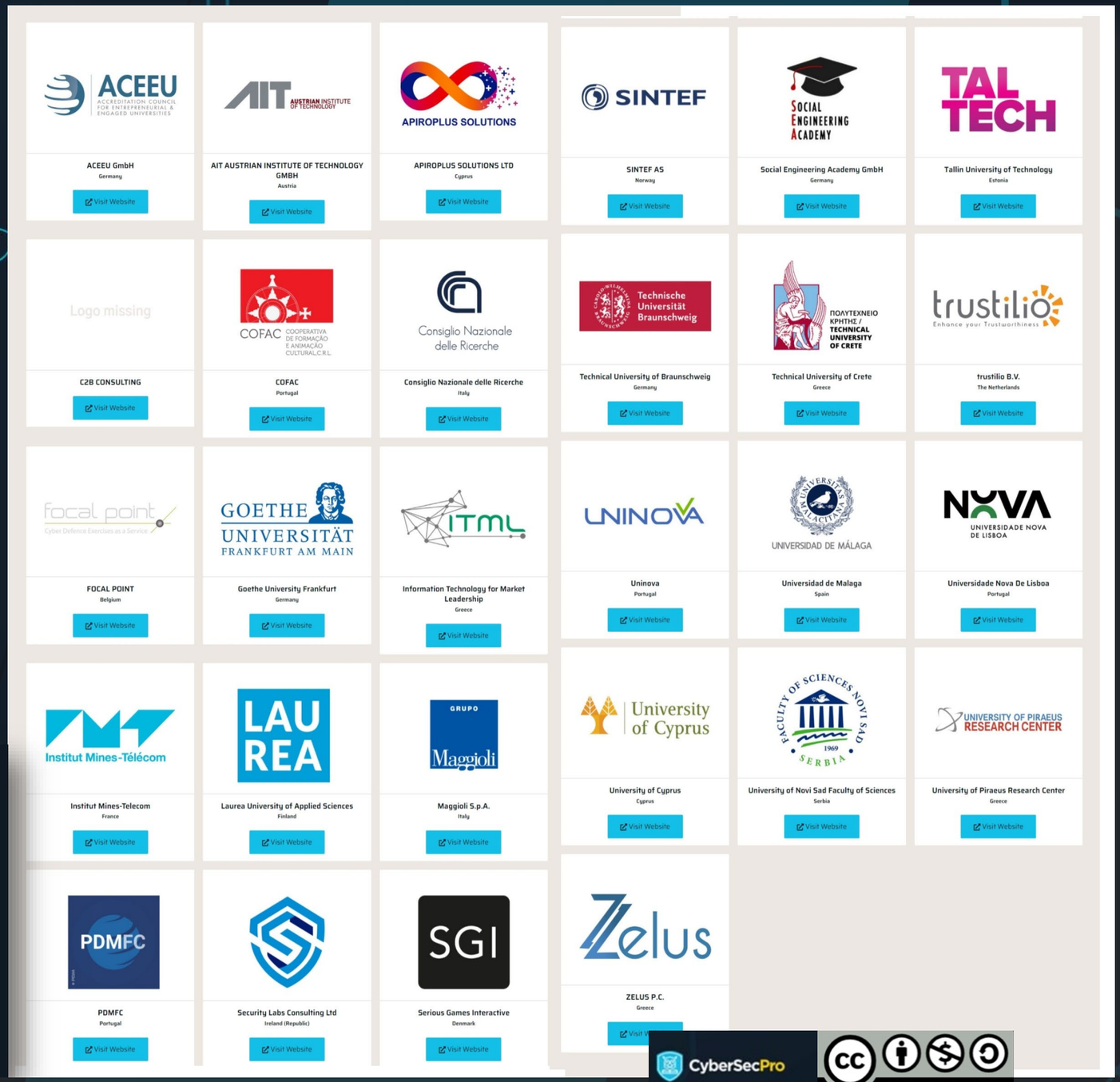
# Transparency: Sources

1. Content for Teaser Video: The content of this teaser video is based on the CyberSecPro project's Work Package 3 Deliverables with valuable contributions from CyberSecPro partners.
2. Language Expertise: The deliverable D3.1 underwent rigorous linguistic proofreading. This involved utilizing Grammarly AI and the meticulous review by a native English speakers.
3. Multimedia Content: Any used engaging images, videos, and audio were sourced from the Pictory, Getty images and other open stock multimedia database.
4. Partner Collaboration: We acknowledge the contributions of our CyberSecPro partners, including the trainer photos featured in the program.
5. Learning Materials: The training materials for this CyberSecPro module were supplied by a listed trainer, and due credit is given to the authors.
6. Creative credit: Video teaser created using these resources by European Cybersecurity Professional Paresh Rathod.
7. Materials of the training created using academic, research literatures and Open Education Material(OEM) with due credits to authors
8. Some of the material used AI based tools including voice simulators (with due credits to authors) to provide best learning experiences to participants

Trainers: Prof. Nineta Polemi, Dr. Paresh Rathod & Dimitris Koutras

# 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/





Funded by the European Union

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

Please send all questions to trainers (and/or):
paresh.rathod@laurea.fi

Trainers: Paresh Rathod, Pasi Kämppi, Cristina Alcaraz, Stylianos Karagiannis, Ricardo Gregorio Lugo, Kitty Kioskli, Paulinus Ofem & Louise Praestiin

CyberSecPro