Corporate Readiness Certificate.

SYLLABUS

Operational Technology (OT) and Internet of Things (IoT) Security

[Number of hours: 7 h]

DESCRIPTION OF THE COURSE

This course is designed for IT, industrial automation and cybersecurity students who wants to extend their knowledge on the cyber security aspects of the OT and IoT environments, with particular focus on protection of critical infrastructure.

The aim of the course is provide an understanding of cyber threats to the modern digital environment involved in industrial control and monitoring, and those utilizing internet of things technologies. The course will also provide an overview on methods and strategies to protect against such threats

REQUIREMENTS

- Basic knowledge of IT networks

- English language – at least at level allowing to read and understand technical documentation

REQUIRED BACKGROUND

Dedicated to students from IT and OT faculties, such us: Information Technology, Electronics, Mechatronics, Industrial Automation, Cybersecurity.

PASSING CRITERIA

Highest scores in the entrance exam

ADDITIONAL INFORMATION ON COURSE

EY is a globally operating consulting company with 300 000 employees around the world. Since 2008, EY has established in Poland a competence hub dedicated to cyber security aspects of industrial automation / Operating Technologies (OT), which is now covering also a fast developing area of Internet of Things. Since 2017, EY hub is operating one of the biggest security laboratory specializing in the OT/IoT security area. Students participating in the course will have an opportunity to learn on the important, practical aspects of OT and IoT security, focusing on typical attack scenarios utilized by hackers and possible protection strategies. Course will be led by EY experts with years of practical experience in OT and IoT security gained on the large programs conducted for companies from oil and gas, power and utilities and manufacturing sectors.

CONTENT & LITERATURE

NIST 800-82 Revision 2

ENISA Publications:

- Good Practices for Security of Internet of Things in the context of Smart Manufacturing
- Industry 4.0 - Cybersecurity Challenges and Recommendations
- Guidelines on Securing the IoT Supply Chain

TECHNICAL REQUIREMENTS FOR UNIVERSITY

N/A – the course will utilize remote connection to EY OT Security Lab in Warsaw

COURSE OVERVIEW

1. Principles of OT and IoT security
    a) structuring the classification of IT, OT and IoT terminology
    b) examples of systems and devices associated with IT, OT and IoT

c) Typical vectors utilized by hackers to attack OT and IoT

2. Case studies of cyber-attacks on OT and IoT
   a) Stuxnet (2010)
   b) Ukrainian Power Grid Incident (Black Energy 3 – 2015)
   c) Triton (2018)
   d) WannaCry and Not-Petya ransomwares (2017)
   e) Solar Winds (2020)
   f) IoT focused attacks
3. Evolution of Internet of Things and security consequences
4. Leading OT and IoT security standards
   a) IEC 62443 standards family
   b) NIST 800-82
   c) ENISA publications
5. Showcase of typical attack technics
   a) OT kill chain
   b) MITRE Att&CK ICS
   c) Live hacking showcase
6. Typical security measures utilized in OT and IoT
   a) Security Governance
   b) Procedural Measures
   c) Technical Measures
7. Typical processes of OT security operations
   a) SOC definition and role in the organization
   b) Typical SOC models for OT environment
   c) Basic processes (security logging and monitoring, incident response, vulnerability management)