Training: Compendium CE

ICS Industrial Control Systems cyber-attacks and proactive defense

TRAINING GOALS:

The training aims is to provide participants with information related to the construction, organization of industrial systems, security and management of the ICS cybersecurity, presentation of "good practices" and international and sectoral standards related to the protection of industrial and critical systems. An element of the training is the presentation of selected vectors of attacks on ICS, tactics and techniques of operation of cybercriminal groups as well as methods of counteracting and managing the organization during an cyberattack.

CONSPECT:

- ICS industrial systems
  - Industrial environment, SCADA, HMI, PLC
  - Safety and security - reference model
  - Dependence and interoperability of OT / IT systems
  - Cybersecurity challenges
  - ICS risk analysis and management
  - Workshops - risk analysis according to NERC CIP (Critical Infrastructure Protection)
    - You are a "factory owner" and what you should know about the risks
    - Risk management, how to do it with CIP
    - What SHODAN and "others" know about my company
    - Cyberattack on the production system
- ICS systems' threats
  - Selected attacks on industrial systems
  - Cyberthreats - MITRE ATT@CK
  - Organization of system defense, "active defense"
  - Workshop - analysis of the ICS attack, designing a safe "environment"
    - PCAP analysis from Wireshark where the attacker left a trace
    - Analysis of the attack vector from MITRE ICS
    - Reconfiguration, response to a cyberattack, recommendations for change.
    - DRP and BCP in ICS
- ICS incident response and management

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Incident response and management
- SOC / CSIRT (CERT) organization and tasks
- BCP and DR in the cyberattack response organization system
- Workshops - ICS intrusion analysis
  - Forensic analysis - Remnux, IoC.
  - PDF analysis - SecurityOnion.
  - BlueTeam, CSIRT in MISP action, Yara rules.

- Organization and security of the ICS systems
  - Employee, managing the IT / OT environment - responsibility and cooperation
  - Standards and procedures, ICS cybersecurity strategy
  - Cybersecurity audit (NIST, CIP, UKSC)
  - Workshops - "case study" analysis after an incident – where is “smoking gun”, recommendations, strategy of undertaken changes / improvements
    - An owner of an industrial company builds a safe environment
    - Designing changes to the ICS environment
    - Segmentation, separation, diode, "zero-trust", "defense in depth", "air-gap" ICS
    - Pentests - does it work?

REQUIREMENTS:

Required competences of the participants: basic knowledge of cybersecurity terms; Windows, Linux operating systems; knowledge of TCP / IP protocols and the functioning of network devices, knowledge of the OSI model, issues related to the industry and safety requirements related to standards and good practices.

Difficulty level

CERTIFICATE:

The participants will obtain certificates signed by Compendium CE (course completion).

TRAINER:

Certified Compendium CE Trainer.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007