Honeywell Academy

CYBERSECURITY: ADVANCED – INDUSTRIAL CYBERSECURITY STANDARDS AND BEST PRACTICES

COURSE OVERVIEW

Course number: CS-0003
Course duration: 3 days

Prerequisite courses: none

This trainings course helps expand the students understanding of industrial cybersecurity and global cybersecurity standards. The training will go over current cybersecurity trends and recent incidents in operational technology (OT).

The students are introduced to global cybersecurity standards and the cybersecurity lifecycle with its phases of assess, design, implement and maintain. The course will cover counter measures such as end point security, network security and cybersecurity processes to help reduce cyber risk.

The course is intended for cybersecurity managers, plant managers and asset owners, engineers or IT cybersecurity staff tasked with OT cybersecurity, plant operators and administrators, and anyone responsible for IT/OT cybersecurity.

COURSE DELIVERY OPTIONS

- Instructor-Led Training (ILT)
- Virtual Instructor-Led Training (VILT)

COURSE OBJECTIVES

Day 1: Introduction

- Introduction to OT cybersecurity
- Cyber-attacks against industrial control systems (ICS)
- OT cybersecurity challenges and security standards
- Key concepts of IEC 62443 standards
- Foundation requirements
- Security assurance level and protection level
- Zones and conduits
- Defense-in-depth strategy
- Security pillars: process, people, and technology
- ISA/IEC 62443 certifications

Day 2: Assessments

- Vulnerability assessment
- Gap assessment
- Penetration testing
- Risk assessment
- Vulnerability assessment process and tools
- Risk assessment process and exercise

Day 3: Addressing Risks

- Risk and security controls
- Design and maintenance of a cybersecurity program
  - Endpoint security
  - Network security
  - Access control
  - Physical security
- Existing cybersecurity standards (NIST, ISO 27001)
- Key takeaways and conclusion

Honeywell