Honeywell Academy

CYBERSECURITY: OT CYBERSEURITY GOVERNANCE

COURSE OVERVIEW

Course number: HCCM-OT7001
Course duration: 1 day

Prerequisite courses: None

Industrial Control Systems (ICS) and Operational Technology (OT) environments are confronted with a multitude of cybersecurity threats and vulnerabilities, with the attack surface continually expanding. This has led to an increased attractiveness for ransomware and the creation of targeted malware. As a result, we anticipate a rise in both the frequency and disruptive nature of attacks on OT systems.

Our OT Governance Training is specifically crafted for managers and executives who bear responsibility for OT/ICS Cybersecurity. This training equips participants with a deep understanding of critical topics, including the contemporary cybersecurity landscape, the imperative of fortifying OT against cyber threats, compliance with regulations, risk management, and the implementation of effective mitigation strategies.

This course is intended for individuals in roles such as cybersecurity managers, plant managers, asset owners, and cybersecurity personnel entrusted with OT Cybersecurity Governance and accountable for mitigating OT Cybersecurity risks.

COURSE DELIVERY OPTIONS

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

COURSE OBJECTIVES

Key Concepts

- Overview of Industrial Control Systems (ICS)
- Key principles and concepts
- Difference between IT and OT
- Risks and threats to OT systems
- Consequence of a successful cyberattack
- ICS technology trends
- Establishing OT security program
- Regulatory framework and compliance
- Establishing OT security managing system
- Security by design for OT systems
- Importance of security awareness training for all employees and building culture
- Cybersecurity hygiene for everyone
- Key roles and responsibilities
- Incident management overview
- Role playing exercise
- Key metrics and workshop

Honeywell