

OTCS-1008 - OT Cybersecurity: USCG Maritime Cybersecurity Foundation Training

OEM: Honeywell • Code: OTCS-1008

COURSE DESCRIPTION

This course offers an awareness to cybersecurity challenges in maritime industries. The participant will learn the key OT cybersecurity concepts, the importance of securing control systems from cyber-attacks and mitigation strategies. The course offers an overview of OT cybersecurity plan, common maritime Cyber threats, internal and USCG reporting protocols and foundational requirements for good cybersecurity practices and helps to Securely operate and maintain maritime OT systems.

AUDIENCE PROFILE

- The course is intended for all Facility/Vessel Personnel with access to the IT or OT systems, including contractors, whether part-time, full-time, temporary, or permanent.

PREREQUISITES

- Prerequisite Courses: None
- Required Skills: None

COURSE OBJECTIVES

By the end of this course, participants will be able to:

- This section doesn't contain any content.

COURSE OUTLINE

Module 1: Basic Cybersecurity Fundamentals

- Marine OT Cybersecurity Awareness
- Overview of cybersecurity threats and vulnerabilities

Module 2: Threat Recognition & Detection

- Phishing, malware, and ransomware tactics
- Social engineering and suspicious behavior

- Real-world maritime incident case studies

Module 3: Circumvention Techniques Awareness

- Password attacks (brute force, credential stuffing)
- USB/removable media threats and safe handling

Module 4: Cybersecurity Plan (CSP) Familiarization

- Plan scope, structure, and key sections
- Roles and responsibilities
- Emergency contact and escalation procedures

Module 5: Incident Response and Reporting Procedures

- Incident Response & Reporting process
- Importance of timely reporting

Module 6: OT Cybersecurity Hygiene Best Practices

- Strong Password Management
- Multi-Factor Authentication (MFA)
- Safe Browsing Habits