COURSE TABLE OF CONTENTS

OTCS-2006 - OT Cybersecurity: USCG Maritime Cybersecurity Professional Training

OEM: Honeywell • Code: OTCS-2006

COURSE DESCRIPTION

This course offers in depth knowledge about OT cybersecurity standards and best practices. The participant will learn the key OT cybersecurity concepts, awareness of threats and risks in maritime industries. This course offers an overview of OT cybersecurity standards and best practices for 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. This course also provides in depth knowledge and understanding of Incidence response plan and strategy along with the step-by-step process of efficient recovery from cybersecurity incidence.

AUDIENCE PROFILE

- The course is intended for Key Technical Personnels, including cybersecurity engineers or control system engineers who are responsible for cyber security of IT and OT systems for the facility or vessel and have access to the IT or remotely accessible OT systems.

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: Develop Cybersecurity Plan (CSP)

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

Module 5: Operational Technology (OT) Cybersecurity

- Introduction to OT cybersecurity
- Best practices for securing OT systems
- Differences between IT and OT cybersecurity

Module 6: OT Cybersecurity Standards and Best Practices

- CIA and AIC concepts
- Cyber-attacks against industrial control systems

Module 7: ISO/IEC 62443 Standards

- Key concepts of ISA/IEC 62443 standards
- Security assurance and protection levels
- Zones and conduits
- Defense-in-depth approach

Module 8: Three Pillers of OT Cybersecurity2443 Standards

- People
- Process
- Technology

Module 9: CSMS (Cybersecurity Management Systems)

- Cybersecurity Management System
- IEC 62443 Foundational Requirements
- IEC 62443 Policies Alignment
- ISA/IEC 62443 certifications

Module 10: Cybersecurity Assessments and Audit Practices

- Gap assessment
- Passive/Active vulnerability assessment
- Vulnerability assessment process and tools
- Risk assessment process

Module 11: OT Cybersecurity Risks and Mitigation Practices

- Addressing Cyber Risk
- Deter
- Detect
- Delay
- Deny
- Defeat

Module 12: Advancing Knowledge on Cyber Threats

- Emerging trends in cybersecurity
- New technologies and defensive strategies

Module 13: Overview of Incident Management

- Definition and Importance
- Key Components of the Framework

Module 14: Key Challenges in ICS/OT Incident Response Capabilities

- IT-OT Security Integration
- Skills Gap and Resource Constraints

Module 15: Analyzing Attacks According to Cyber Kill Chain

- Cyber Kill Chain Stages
- Case Studies in OT Context

Module 16: Threat Intelligence

- Sources for OT Threat Intelligence
- Analyzing and Applying Intelligence

Module 17: Threat Hunting

- Proactive Threat Hunting Techniques
- Integration with Incident Response

Module 18: Incident Response Plan and Reporting Procedures

- Developing the Incident Response Team
- Incident Response & Reporting process
- Importance of timely reporting

Module 19: Building Cybersecurity Incident Response Plan

- Standards and Frameworks
- Essential Elements to Include

Module 20: Identifying and Detecting Incidents

- Indicators of Compromise in OT
- Automated Detection Tools

Module 21: Recommended Detection Approaches

- Behavioral vs. Signature-Based Detection
- Role of Anomaly Detection

Module 22: Incident Categorization

- Criteria for Categorization
- Importance for Response Priorities

Module 23: Evidence Gathering and Handling

- Best Practices for Evidence Collection
- Legal Considerations

Module 24: Chain of Custody

- Importance of Chain of Custody
- Steps for Documentation

Module 25: Eradication and Recovery

- Strategies for Threat Eradication
- Recovery Planning

Module 26: Incident Response Roles & Responsibilities

- Incident command structure and Effective Communication strategy
- Evidence preservation and forensics handoff

Module 27: ICS Response Drills and Exercises

- Designing Effective IR Drill / Tabletop Exercises
- Metrics for Evaluating Effectiveness

Module 28

- Key takeaways and conclusion