Honeywell Academy

CYBERSECURITY: ADVANCED – CYBERSECURITY INCIDENT MANAGEMENT

COURSE OVERVIEW

Course number: CS-0005
Course duration: 2 days

Prerequisite courses: None

Required Skills: Basic understanding of cybersecurity

This cybersecurity incident management training provides overview of ICS/OT incident response and handling steps, an understanding of how incidents are responded to a high level by focusing on prioritizing the safety and reliability of security operations, as well as allow students to build important skills through the hands-on labs and exercise.

Throughout the course, the students can apply what they have learned to understand their ICS network, create baselines, monitor for threats, detect, and perform incident response and recover from cyber incidents in industrial environments.

This workshop is suited for cybersecurity managers, plant managers, asset owners, IT cybersecurity staff tasked with OT cybersecurity, plant engineers tasked with OT cybersecurity, plant operators and anyone responsible for IT/OT cybersecurity.

At the conclusion of the course, students will be provided a Certification of Completion which can be submitted to accrediting bodies to count towards CPE hours.

COURSE DELIVERY OPTIONS

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

COURSE OBJECTIVES

Key Concepts

- Overview of Incident Management
- Key challenges in ICS/OT Incident response capabilities for successful incident response and safe, reliable operations
- Analyzing attacks according to Cyber Kill Chain
- Threat Intelligence
- How to prepare and plan for Incident Response
- Building Cybersecurity Incident Response Plan
- Identifying and detecting Incident.
- Recommended detection approaches
- Incident categorization
- Evidence gathering and handling
- Chain of Custody
- Eradication and recovery
- Root Cause analysis and Lessons Learned
- Cyber forensics
- Reporting and evidence retention
- ICS Response Tabletops and How to Run them

Tools and Techniques

- Cyber Incident Response Plan
- Creating baseline
- Tabletop Exercise
- Cyber forensics
- General tools, e.g., SIEM, Application Whitelisting, etc.
- Investigation tools, e.g., Wireshark
- Analysis (log, etc.)

Honeywell