Honeywell Academy

CYBERSECURITY: ADVANCED – INDUSTRIAL OFFENSIVE AND DEFENSIVE CYBERSECURITY PRINCIPLES: RED TEAM / BLUE TEAM WORKSHOP

COURSE OVERVIEW

Course number: CS-0002
Course duration: 4 days

Prerequisite courses: none

This red team/blue team workshop provides a unique insight into the hacker's mindset and techniques, helping students develop defensive strategies. These can then be practiced in head-to-head competitions between blue team defenders and the red team attackers (hackers). Students will learn to understand the hacker's mindset, the attack principles, and the common attack sequences, as well as the available techniques that can be used to prevent and counter them.

Throughout the course, the students can apply what they have learned by defending critical infrastructure in accurately simulated operational technology (OT) environment against a live adversary.

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.

COURSE DELIVERY OPTIONS

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

COURSE OBJECTIVES

Key Concepts

- Overview on how the cybersecurity pieces work together
- Understanding vulnerabilities and attack vectors specific to industrial control systems (ICS)
- Practical OT cybersecurity concepts and applications
- How to respond to, adapt and defend against active attacks
- Analyzing emerging trends in attacks
- Identifying areas of vulnerability within the organization
- Preparing a risk assessment
- Reporting and recommending countermeasures

Tools and Techniques

- Developing risk scenarios
- Cyber forensics
- Vulnerability scanning
- General tools, e.g. SIEM, antivirus, allowlisting
- Investigation tools, e.g. Zenmap, Wireshark, Netcat
- Penetration tools, e.g. Mimikatz, Metasploit
- Log and memory analysis
- Malware analysis
- Reverse engineering
- Incident response

Honeywell