Advanced Cybersecurity for Industry 4.0

COURSE OUTLINE

Catalogue Number	77-3301-0017
Category	Industry 4.0
Duration	15 Hours
Prerequisites	Level 1 Industry 4.0 Courses

Activity 1: Cybermonitoring Tools

Defining Cybersecurity Monitoring

How Monitoring Works

Creating a Monitoring Plan

Common Cybersecurity Tools

Activity 2: Firewalls

Defining Firewalls

Protecting through Firewalls

Types of Firewalls

Components of a Firewall System

Activity 3: Switch Protection

Network Switches – Definition and Function

How Switches Work

Logging on to a Network Switch

Switch Security

VLANs

Spanning Tree Protocols

Virtual Machines

Activity 4: Antivirus Installation and Configuration

ICS Cybersecurity Vulnerabilities

Antivirus Software in ICSs

Modes of Installation

Antivirus Software Maintenance

Activity 5: Managing Ports and Services

OT Security

Ports, Protocols, and Services

TCP and UDP Ports

Security Risks in Ports

Detecting and Removing Open Ports

Activity 6: Cryptography

Defining Cryptography

Cryptography in IoT Security

Encryption and Decryption

Hashes

Digital Signature

BLE and Zigbee Security

Activity 7: IoT Vulnerabilities, Attacks, and Countermeasures

ICS and IoT Vulnerabilities

Attack Vectors and Countermeasures

Root of Trust

Secure Boot

Mutual Authentication

Activity 8: Secure Design of IoT Devices

Secure by Design

Cybersecurity Standards

Secure Device Configuration

Secure Network Infrastructure

Activity 9: Operational Security Lifecycle

Security Lifecycle Model Overview and Function

Security Lifecycle Model Steps: Identify, Assess, Protect, Monitor,

Activity 10: Identity and Access Management Solutions for the IoT

Identity and Access Management: Definition and Function

IDoT

The Identity Lifecycle of an IoT Device

Authorization and Access Control

Activity 11: Mitigating IoT Privacy Concerns

IoT Privacy Challenges

Privacy Design

Privacy Engineering

Organizational Privacy

Activity 12: IoT Compliance Monitoring

IoT Compliance

IoT Compliance Programs

IoT System Approval

Policies

Creating IoT Testing Environments

Internal Compliance Monitoring

Activity 13: Cloud Security for IIoT

Integrating IoT Clouds in SCADA Systems

Attacks on Connected SCADA Systems

Securing IoT-Based SCADA Systems

IoT-Based SCADA Cybersecurity Best Practices

Activity 14: Incident Response and Forensic Analysis

Defining Incident Management

Developing a Misuse Case

Building an Incident Response Plan

Tools for Digital Forensics

Incident Escalation and Monitoring