Course Title:

ISA/IEC 62443 Cybersecurity Maintenance Specialist
Duration: 5 Days

Course Overview

This course provides the knowledge and skills required to maintain and continuously improve the cybersecurity posture of Industrial Automation and Control Systems (IACS) in accordance with ISA/IEC 62443 standards. Participants will learn how to operate, monitor, update, and review security measures throughout the system lifecycle, including handling incidents, applying patches, managing vulnerabilities, and performing periodic security reviews. The training emphasizes the integration of maintenance activities into day-to-day operations to ensure ongoing compliance, resilience, and risk reduction.

Prerequisites

- Understanding of IACS/OT environments and industrial control system components
- Basic knowledge of ISA/IEC 62443 standards and concepts
- Familiarity with cybersecurity fundamentals and operational security measures
- Recommended: Completion of ISA/IEC 62443 Cybersecurity Fundamentals Specialist course

---

Day 1 – Role of Maintenance in the Cybersecurity Lifecycle

1. **Course Introduction & Objectives**
2. **ISA/IEC 62443 Lifecycle Approach**
    - Where maintenance fits in the lifecycle
    - Links to design and operation phases
3. **Maintenance vs. Incident Response Activities**
4. **Security Operations in IACS Environments**
    - OT/IT collaboration in security operations
    - Impact of downtime and availability requirements

Day 2 – Security Monitoring & Detection

1. **Continuous Security Monitoring Concepts**
    - Logs, alerts, and monitoring strategies
2. **Monitoring Tools & Technologies**
    - IDS/IPS, SIEM, anomaly detection for OT
3. **Identifying and Investigating Security Events**
4. **Performance and Security Health Metrics**

Day 3 – Vulnerability & Patch Management

1. **Vulnerability Management in IACS**
    - Identifying, prioritizing, and tracking vulnerabilities
2. **Patch and Update Management**
    - Testing patches in OT environments
    - Scheduling to avoid operational disruption
3. **Configuration Management & Change Control**
4. **Vendor Coordination for Updates and Security Advisories**

Day 4 – Incident Handling & Recovery

1. **Incident Response Procedures**
    - Preparation, detection, containment, eradication, recovery
2. **Root Cause Analysis for Cyber Incidents**
3. **Backup and Restore Strategies**
    - Data integrity and system image backups
4. **Post-Incident Review and Lessons Learned**

Day 5 – Continuous Improvement & Compliance

1. **Periodic Security Reviews and Audits**
    - Assessing compliance against ISA/IEC 62443 requirements
2. **Updating Security Documentation**
    - Maintenance logs, change records, incident reports
3. **Training and Awareness for Operations Teams**
4. **Course Review & Exam Preparation**
    - Key concepts recap
    - Sample exam questions and discussion
5. **Final Assessment**
    - Mock exam & feedback