

## Process Control Cybersecurity

### **DAY 1**

#### **Introduction and Cybersecurity Fundamentals**

- Introduction to Process Control Cybersecurity
- Understanding the Current Industrial Security Environment
- How IT and OT (Operational Technology) in the Plant Floor are Different and How They are the Same
- Overview of Process Control
- Overview of Industrial Communication Systems and Networks
- How Cyber-attacks Happen: Threats, Vulnerabilities, Attacks
- Asset Identification and Impact Assessment

### **DAY 2**

#### **Introduction to the IACS Cybersecurity Lifecycle and ISA99 / IEC 62443**

- Identification & Assessment Phase
- Design & Implementation Phase
- Operations & Maintenance Phase
- Limits of a Conventional IT Approach
- The IEC 62443 Security Approach and Standards
- Risk Analysis Risk Identification, Classification, and Assessment
- CAL (Cybersecurity Assurance Levels)
- Functional Requirements of IEC 62443

### **DAY 3**

#### **Addressing Security Risks: Process Control Security Counter-measures**

- Antivirus, Anti-spyware
- Firewalls, Traffic Analyzers
- Encryption, Virtual Private Networks (VPNs)
- Passwords - *Authentication Systems*
- Access Control - *Intrusion Detection / Prevention*
- Network Segmentation

## **DAY 4**

### **Application Diagnostics and Troubleshooting**

- Interpreting Device Alarms and Event Logs
- Early Indicators
- Network Intrusion Detection Systems
- Network Management Tools
- Interpreting OS and Application Alarms and Event Logs
- Application Management and Whitelisting Tools
- Antivirus and Endpoint Protection Tools
- Security Incident and Event Monitoring (SIEM) Tools

## **DAY 5**

### **IACS Cybersecurity Operating Procedures & Tools and Incident Response**

- Developing and Following an IACS Management of Change Procedures
- IACS Configuration Management Tools
- Developing and Following an IACS Patch & Antivirus Management and Cybersecurity Audit Procedures
- Patch Management Tools
- Antivirus and Whitelisting Tools
- Auditing Tools
- Developing and Following an IACS Incident Response Plan
- Incident Investigation and System Recovery