KOENIG SOLUTIONS · COURSE OUTLINE

Process Control Cybersecurity: IEC 62443 & SIEM

5 Days	5	37
DURATION	MODULES	TOPICS

LEARNING OBJECTIVES

- Explain differences and similarities between IT and OT environments
- Identify threats, vulnerabilities and attack methods in ICS
- Assess assets and evaluate their potential impact
- Apply the IEC 62443 security approach and its functional requirements
- Analyse risk through identification, classification and assessment
- Implement counter-measures such as firewalls, VPNs and access control
- Interpret device, OS and application alarms and event logs
- Plan incident response, investigation and system recovery procedures

COURSE SYLLABUS

5 Modules, 37 Topics

DAY 1

01

Introduction and Cybersecurity Fundamentals

TOPICS

- 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

02

Introduction to the IACS Cybersecurity Lifecycle and ISA99 / IEC 62443

TOPICS

- 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

03

Addressing Security Risks: Process Control Security Counter-measures

TOPICS

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

DAY 4

04

Application Diagnostics and Troubleshooting

TOPICS

- 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

05

IACS Cybersecurity Operating Procedures & Tools and Incident Response

TOPICS

- 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

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training | Live Online Classes (ILO) | Fly-Me-A-Trainer (FMAT) | Flexi (Self-Paced) | 1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com | info@koenig-solutions.com