

KOENIG SOLUTIONS • COURSE OUTLINE

ICS/SCADA Cybersecurity

Learn to secure ICS and SCADA networks against cyber threats, from TCP/IP fundamentals and hacking methods to vulnerability management and intrusion detection.

3 Days

24 HOURS

8

MODULES

59

TOPICS

COURSE OVERVIEW

The ICS/SCADA Cybersecurity course is designed to equip learners with a robust understanding of cybersecurity principles specifically tailored to industrial control systems (ICS) and supervisory control and data acquisition (SCADA) networks. This comprehensive training covers the unique challenges and Security models of ICS/SCADA environments, providing insights into TCP/IP fundamentals, Hacking methodologies, Vulnerability management, and relevant standards and regulations. Key lessons include securing ICS networks, managing vulnerabilities, and understanding Intrusion detection and prevention systems. By completing the course, participants will be prepared to earn their ICS security certification and gain practical skills for ICS cybersecurity training. The curriculum is ideal for professionals seeking to enhance their expertise in protecting critical infrastructure and ensuring the resilience of industrial operations against cyber threats.

Who Should Attend

The ICS/SCADA Cybersecurity course equips professionals with the skills to defend critical infrastructure against cyber threats.

IT Security Professionals and Analysts

Industrial Control Systems (ICS) Engineers

SCADA Systems Engineers

Cybersecurity Consultants specializing in ICS/SCADA

Network Security Administrators

Infrastructure Protection Analysts

Risk Management Professionals

Compliance Officers responsible for cybersecurity standards

Government and Defense Personnel focused on critical infrastructure security

Incident Responders and Forensic Analysts

Operational Technology (OT) Professionals

Electrical Engineers specializing in industrial control systems

Research and Development (R&D) Personnel in industrial cybersecurity

Corporate Security Officers managing both physical and cybersecurity risks

Systems Integrators implementing security solutions in industrial environments

LEARNING OBJECTIVES

- Compare IT and ICS/SCADA security models
- Explain TCP/IP protocol architecture and layering for ICS networks
- Identify ICS/SCADA protocols within TCP/IP-based networks
- Analyse the hacking process from footprinting to covering tracks
- Assess ICS/SCADA vulnerabilities using CVE and vulnerability databases
- Interpret standards such as NERC CIP, ISA99 and NIST SP 800-82
- Apply risk mitigation controls to secure ICS networks
- Evaluate methods for bridging the air gap and detecting intrusions

COURSE SYLLABUS

8 Modules, 59 Topics

01

Introduction to ICS/SCADA Network Defense

TOPICS

IT Security Model · ICS/SCADA Security Model

02

TCP/IP Fundamentals

TOPICS

- Introduction and Overview
- Understanding TCP/IP Networks
- Internet RFCs and Standards (STDs)
- TCP/IP Protocol Architecture
- Concepts of Protocol Layering
- TCP/IP Layering Model
- Components of TCP/IP Networks
- ICS/SCADA Protocols

03

Introduction to Hacking

TOPICS

- Overview of the Hacking Process
- Hacking Methodology
- Intelligence Gathering
- Footprinting Techniques
- Scanning Methods
- Enumeration Techniques
- Identifying Vulnerabilities
- Exploitation Techniques
- Covering Tracks

04

Vulnerability Management

TOPICS

- Challenges in Vulnerability Assessment
- System Vulnerabilities
- Desktop Vulnerabilities
- ICS/SCADA Vulnerabilities
- Interpreting Advisory Notices
- Common Vulnerabilities and Exposures (CVE)
- ICS/SCADA Vulnerability Databases
- Lifecycle of a Vulnerability and Exploit
- Challenges of Zero-Day Vulnerabilities
- Exploiting a Vulnerability
- Vulnerability Scanners
- Unique Challenges of ICS/SCADA Vulnerabilities
- Difficulties in Vulnerability Management for ICS/SCADA

05

Cybersecurity Standards and Regulations

TOPICS

- ISO 27001
- ICS/SCADA Security Frameworks
- NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection)
- CFATS (Chemical Facility Anti-Terrorism Standards)
- ISA99 / IEC 62443 (Industrial Automation and Control Systems Security)
- NIST SP 800-82 (Guide to Industrial Control Systems Security)

06

Securing the ICS Network

TOPICS

- Physical Security Measures
- Establishing Security Policies - ISO Roadmap
- Securing ICS-Specific Protocols
- Performing a Vulnerability Assessment
- Selecting and Implementing Risk Mitigation Controls
- Continuous Monitoring and Threat Detection
- Mitigating Risks Associated with Legacy Systems

07

Bridging the Air Gap

TOPICS

Should You Bridge the Air Gap? · Advantages and Disadvantages · Security Guards for Network Traffic · Data Diodes for One-Way Communication · Next-Generation Firewalls for ICS Security

08

Introduction to Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

TOPICS

- Capabilities and Limitations of IDS
- Types of IDS
- Network-Based IDS (NIDS)
- Host-Based IDS (HIDS)
- Network Node IDS (NNIDS)
- Advantages of IDS
- Limitations of IDS
- Evasion Techniques to Bypass IDS (Stealth)
- Detecting and Responding to Intrusions

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