EC-Council ICS/SCADA Cybersecurity

Category: Networking & Security | **Vendor:** EC-Council

Duration: 24.00 hours (3 days) **19.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

The ICS/SCADA Cybersecurity course is a hands-on training module that teaches the foundations of security and defending network architectures from attacks. Students will learn to think like a malicious hacker to defend their organizations.

ICS/SCADA teaches powerful methods to analyze risks possessed by network infrastructure in IT and corporate spaces. Once your foundation or basic concepts are clear, you will learn a systematic process of intrusion and malware analysis. After this, you will learn about digital forensic process and incident response techniques upon detecting a breach.

About This Course

- Module 1: Introduction to ICS/SCADA Network Defense
- Module 2: TCP/IP 101
- Module 3: Introduction to Hacking
- Module 4: Vulnerability Management
- Module 5: Standards and Regulations for Cybersecurity
- Module 6: Securing the ICS Network
- Module 7: Bridging the Air Gap
- Module 8: Introduction to Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

Who Should Attend

This course is designed for IT professionals who manage or direct their organization’s IT infrastructure and are responsible for establishing and maintaining information security policies, practices, and procedures. The focus in the course is on the Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) Systems.

Prerequisites & Entry Requirements

General Prerequisites:

- Linux operating system fundamentals, including basic command line usage.
- Conceptual knowledge of programming/scripting.
- Solid grasp of essential networking concepts (OSI model, TCP/IP, networking devices, and transmission media).
- Understanding of basic security concepts (e.g., malware, intrusion detection systems, firewalls, and vulnerabilities).
- Familiarity with network traffic inspection tools (Wireshark, TShark, or TCPdump) is highly recommended.

Detailed Course Outline

Module 1: Introduction to ICS/SCADA Network Defense

- IT Security Model
- ICS/SCADA Security Model
- LAB: Security Model
- Security Posture
- Risk Management in ICS/SCADA
- Risk Assessment
- Defining Types of Risk
- Security Policy
- LAB: Allowing a Service

Module 2: TCP/IP 101

- Introduction and Overview
- Introducing TCP/IP Networks
- Internet RFCs and STDs
- TCP/IP Protocol Architecture
- Protocol Layering Concepts
- TCP/IP Layering
- Components of TCP/IP Networks
- ICS/SCADA Protocols

Module 3: Introduction to Hacking

- Review of the Hacking Process
- Hacking Methodology
- Intelligence Gathering

- Footprinting
- Scanning
- Enumeration
- Identify Vulnerabilities
- Exploitation
- Covering Tracks
- LAB: Hacking ICS/SCADA Networks Protocols
- How ICS/SCADA Are Targeted
- Study of ICS/SCADA Attacks
- ICS/SCADA as a High–Value Target
- Attack Methodologies In ICS

Module 4: Vulnerability Management

- Challenges of Vulnerability Assessment
- System Vulnerabilities
- Desktop Vulnerabilities
- ICS/SCADA Vulnerabilities
- Interpreting Advisory Notices
- CVE
- ICS/SCADA Vulnerability Sites
- Life Cycle of a Vulnerability and Exploit
- Challenges of Zero-Day Vulnerability
- Exploitation of a Vulnerability
- Vulnerability Scanners
- ICS/SCADA Vulnerability Uniqueness
- Challenges of Vulnerability Management Within ICS/SCADA
- LAB: Vulnerability Assessment
- Prioritizing Vulnerabilities
- CVSS
- OVAL

Module 5: Standards and Regulations for Cybersecurity

- ISO 27001

- ICS/SCADA

- NERC CIP

- CFATS

- ISA99

- IEC 62443

- NIST SP 800-82

Module 6: Securing the ICS Network

- Physical Security

- Establishing Policy – ISO Roadmap

- Securing the Protocols Unique to the ICS

- Performing a Vulnerability Assessment

- Selecting and Applying Controls to Mitigate Risk

- Monitoring

- Mitigating the Risk of Legacy Machines

Module 7: Bridging the Air Gap

- Do You Really Want to Do This?

- Advantages and Disadvantages

- Guard

- Data Diode

- Next Generation Firewalls

Module 8: Introduction to Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

- What IDS Can and Cannot Do

- Types IDS

- Network

- Host

- Network Node
- Advantages of IDS
- Limitations of IDS
- Stealthing the IDS
- Detecting Intrusions
- LAB: Intrusion Detection
- Log Analysis
- ICS Malware Analysis
- LAB: ICS Malware Analysis
- Essential Malware Mitigation Techniques
- ICS/SCADA Network Monitoring
- ICS/SCADA IDS

Frequently Asked Questions

Q: What delivery options are available for EC-Council ICS/SCADA Cybersecurity?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 3-day EC-Council ICS/SCADA Cybersecurity course provides up to 19.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the EC-Council ICS/SCADA Cybersecurity training?

The training takes place over 3 day(s), with each day lasting approximately 24.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for EC-Council ICS/SCADA Cybersecurity?

Yes, we provide corporate training, dedicated training, and closed classes for EC-Council ICS/SCADA Cybersecurity. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: EC-Council ICS/SCADA Cybersecurity, Specialist, ICS-SCADA

Q: Why choose Nexus Human for EC-Council ICS/SCADA Cybersecurity?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your EC-Council ICS/SCADA Cybersecurity training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)