Document Generated: 11/02/2026

Learning Style: Virtual Classroom

Technology: EC-Council

Difficulty: Intermediate

Course Duration: 3 Days

EC-Council ICS/SCADA Cybersecurity



About This Course:

Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems run power grids, water treatment plants, manufacturing lines, and pipelines. They’re high-value targets, and securing them takes more than standard IT security. Legacy hardware, specialized protocols, and the demand for constant uptime create challenges that traditional security approaches weren’t designed for.

Course Objectives:

- Compare IT and ICS/SCADA security models and explain how their priorities differ
- Perform risk assessments and apply risk management practices in ICS/SCADA environments
- Develop security policies suited to industrial control systems
- Explain TCP/IP protocol architecture and the protocols unique to ICS/SCADA networks
- Apply the hacking methodology, including footprinting, scanning, enumeration, and exploitation, to understand how attackers target ICS/SCADA systems
- Analyze real-world ICS/SCADA attacks and attack methodologies
- Identify ICS/SCADA vulnerabilities and address the challenges of vulnerability management in industrial environments
- Understand the cybersecurity standards and regulations that apply to ICS/SCADA systems
- Secure ICS-specific protocols and harden industrial networks
- Analyze ICS malware and deploy network monitoring and intrusion detection for ICS/SCADA environments
- Prepare for the EC-Council ICS/SCADA Cybersecurity exam

Audience:

- IT professionals who manage or direct their organization’s IT infrastructure
- Security professionals responsible for information security policies, practices, and procedures
- ICS/SCADA engineers, operators, and administrators
- Operational technology (OT) and plant network engineers
- Security consultants who perform assessments of ICS/SCADA environments
- Network security administrators and incident responders in critical infrastructure sectors such as energy, utilities, oil and gas, water, and manufacturing

Prerequisites:

- Linux operating system fundamentals, including basic command-line usage
- Conceptual knowledge of programming or scripting
- A solid understanding of networking concepts, including the OSI model, TCP/IP, networking devices, and transmission media
- An understanding of basic security concepts such as malware, intrusion detection systems, firewalls, and vulnerabilities

Course Outline:

Module 1: Introduction to ICS/SCADA Network Defense

IT security model

- ICS/SCADA security model
- Security posture and risk management
- Risk assessment and types of risk
- Security policies
- Labs: Security Model and Allowing a Service

Module 2: TCP/IP 101

- Introduction to TCP/IP networks
- Internet RFCs and standards
- TCP/IP protocol architecture
- Protocol layering concepts
- TCP/IP layers
- Components of TCP/IP networks
- ICS/SCADA protocols
- Lab: TCP/IP and ICS/SCADA Protocols

Module 3: Introduction to Hacking

- Hacking process and methodology
- Intelligence gathering and footprinting
- Scanning and enumeration
- Vulnerability identification
- Exploitation and covering tracks
- How ICS/SCADA systems are targeted
- ICS/SCADA attack methodologies and case studies
- Lab: Hacking ICS/SCADA Network Protocols

Module 4: Vulnerability Management

- Challenges of vulnerability assessment
- System, desktop and ICS/SCADA vulnerabilities
- Interpreting security advisories
- Common Vulnerabilities and Exposures (CVE)
- ICS/SCADA vulnerability resources
- Vulnerability and exploit lifecycle
- Zero-day vulnerabilities
- Vulnerability scanners
- Vulnerability assessment challenges in ICS/SCADA
- Vulnerability prioritization, CVSS and OVAL
- Labs: Vulnerability Assessment and Vulnerability Severity

Module 5: Standards and Regulations for Cybersecurity

- ISO 27001
- ICS/SCADA security
- NERC CIP
- CFATS
- ISA99
- IEC 62443
- NIST SP 800-82

Module 6: Securing the ICS Network

- Physical security
- Establishing security policies and an ISO roadmap
- Securing ICS-specific protocols
- Performing vulnerability assessments
- Selecting and applying risk-mitigation controls
- Security monitoring
- Mitigating risks associated with legacy machines

Module 7: Bridging the Air Gap

- Considerations when bridging an air gap
- Advantages and disadvantages
- Security guards
- Data diodes
- Next-generation firewalls
- Event monitoring to mitigate ICS risks
- Implementing strong authentication

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

- Capabilities and limitations of IDS
- Types of IDS: network, host and network-node
- IDS advantages and limitations

- Stealth techniques and intrusion detection
- Log analysis
- ICS malware analysis
- Essential malware-mitigation techniques
- ICS/SCADA network monitoring and IDS
- Lab: Intrusion Detection
- Lab: ICS Malware Analysis
- Case study: Configuring essential rules within ICS/SCADA