ICS/SCADA Cybersecurity

Course Duration: 24 Hours (3 Days)

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.

Audience Profile

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

Course Syllabus

Module 1: Introduction to ICS/SCADA Network Defense

- IT Security Model
- ICS/SCADA Security Model

Module 2: TCP/IP Fundamentals

- 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

Module 3: Introduction to Hacking

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

Module 4: Vulnerability Management

- 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

Module 5: Cybersecurity Standards and Regulations

- 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)

Module 6: Securing the ICS Network

- 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

Module 7: Bridging the Air Gap

- 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

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

- 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 (Stealthing)

- Detecting and Responding to Intrusions