EC-Council ICS/SCADA Cybersecurity + Exam voucher

Duration: 3 Days **Course Code: EICS-SCADA** **Delivery Method: Virtual Learning**

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.

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

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.
- SCADA Systems personnel.
- Business System Analysts who support SCADA interfaces.
- System Administrators, Engineers, and other IT professionals who are administering, patching, securing SCADA, and/or ICS.
- Security Consultants who are performing security assessments of SCADA and/or ICS.

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.

Content:

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

Additional Information:

The EC-Council Advantage
With EC-Council, you'll get a chance to learn ICS/SCADA from industry experts. The training program is spearheaded by renowned SCADA expert, Kevin Cardwell. EC-Council's SCADA training uses multimedia learning with interactive formats such as lectures, illustrations, and simulations.
Apart from this, the training program is interactive, and the learning module is activity-focused, which is helpful for skill development.

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/