APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

EC-Council ICS SCADA Cybersecurity Training

EC-Council Authorized Training · Applied Technology Academy

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.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	**3 Days**	**Linux fundamentals, networking & scripting**	**$106,170**	**Yes**

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.

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

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

  - 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

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

  - 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

Intended 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.

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

Follow-On Courses

Certified Network Defender

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.