Current Technologies
Computer Learning Centers

EC-Council

6210 Central Ave, Portage, IN. 46368 Phone: 219.764.3800 Fax: 219.764.3805 Web: http://www.ctclc.com

Certified Security Specialist (ECSS v 9)

This course is an entry level security program covering the fundamental concepts of information security, computer forensics, and network security. It enables students to identify information security threats which reflect on the security posture of the organization and implement general security controls. This program will give a holistic overview of the key components of information security, computer forensics, and network security. This program provides a solid fundamental knowledge required for a career in information security.

How you'll benefit

This class will help you:

- Enhance their skills in three different areas namely information security, network security, and computer forensics.
- Prepare you for the ECSS exam

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10%
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs Run up to Date Code for all our courses

Objectives

Upon completing this course, the student will be able to meet these objectives:

- Key issues plaguing the information security, network security, and computer forensics
- Fundamentals of networks and various components of the OSI and TCP/IP model
- Various network security protocols
- Various types of information security threats and attacks, and their countermeasures
- Social engineering techniques, identify theft, and social engineering countermeasures
- Different stages of hacking cycle
- Identification, authentication, and authorization concepts
- Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools
- Fundamentals of IDS and IDS evasion techniques
- Data backup techniques and VPN security

Course Duration

5 day

Course Price

$2,895.00

Methods of Delivery

- Instructor Led
- Virtual ILT
- On-Site

Certification Exam

ECSS

- Fundamentals of firewall, techniques for bypassing firewall, and firewall technologies such as Bastion Host, DMZ, Proxy Servers, Network Address Translation, Virtual Private Network, and Honeypot
- Fundamentals of IDS and IDS evasion techniques
- Data backup techniques and VPN security
- Wireless Encryption, wireless threats, wireless hacking tools, and Wi-Fi security
- Different types of web server and web application attacks, and countermeasures
- Fundamentals of ethical hacking and pen testing
- Incident handling and response process
- Cyber-crime and computer forensics investigation methodology
- Different types of digital evidence and digital evidence examination process
- Different type of file systems and their comparison (based on limit and features)
- Gathering volatile and non-volatile information from Windows and network forensics analysis mechanism
- Steganography and its techniques
- Different types of log capturing, time synchronization, and log capturing tools
- E-mails tracking and e-mail crimes investigation
- Writing investigation report

Who Should Attend

The job roles best suited to the material in this course are:

- This course is designed for anyone who want to enhance their skills and make career in information security, network security, and computer forensics fields.

AGE REQUIREMENTS AND POLICIES CONCERNING MINORS

- The age requirement for attending the training or attempting the CSCU exam is restricted to any candidate that is at least 13 years old.
- If the candidate is under the age of 13, they are not eligible to attend the official training or eligible to attempt the certification exam unless they provide the accredited training center (ATC) or EC-Council a written consent of their parent or their legal guardian and a supporting letter from their institution of higher learning. Only applicants from nationally accredited institutions of higher learning shall be considered.

Disclaimer

- EC-Council reserves the right to impose additional restriction to comply with the policy. Failure to act in accordance with this clause shall render the authorized training center (ATC) in violation of their agreement

with EC-Council. EC-Council reserves the right to revoke the certification of any person in breach of this requirement.

Perquisites

To fully benefit from this course, you should have the following knowledge:

- End-user skills with Windows-based PCs
- Basic knowledge of computing concepts

Outline

Module 1: Information Security Fundamentals

Module 2: Network Fundamentals

Module 3: Secure Network Protocols

Module 4: Information Security Threats and Attacks

Module 5: Social Engineering

Module 6: Hacking Cycle

Module 7: Identification, Authentication, and Authorization

Module 8: Cryptography

Module 9: Firewalls

Module 10: Intrusion Detection System

Module 11: Data Backup

Module 12: Virtual Private Network

Module 13: Web Security

Module 14: Ethical Hacking and Pen Testing

Module 15: Incident Response

Module 16: Computer Forensics Fundamentals

Module 17: Digital Evidence

Certified Security Specialist (ECSS v 9)

Module 18: Understanding File Systems

Module 19: Windows Forensics

Module 20: Network Forensics and Investigating Network Traffic

Module 21: Steganography

Module 22: Analyzing Logs

Module 23: E-mail Crime and Computer Forensics

Module 24: Writing Investigative Report