

Certified Security Specialist

Course Duration: 40 Hrs.

Course code: E|CSS

Course Overview

The EC-Council Certified Security Specialist (ECSS) course provides a foundational understanding of information security, network defense, ethical hacking, and digital forensics, equipping learners with practical skills to protect digital assets and respond to security incidents.

What you'll learn?

- ❖ **Information Security Basics:**
Understand the fundamentals of information security, including principles, policies, and best practices.
- ❖ **Network Security:**
Learn about network security fundamentals, including network protocols, firewalls, intrusion detection systems, and network traffic monitoring.
- ❖ **Vulnerability Management:**
Identify and assess system vulnerabilities and learn techniques to mitigate them.
- ❖ **Ethical Hacking & Penetration Testing:**
Explore ethical hacking techniques and learn how to conduct penetration testing to identify vulnerabilities.

Target Audience

The target audience for a Certified Security Specialist course typically includes individuals seeking to enhance their skills and build careers in information security, network security, and computer forensics, including those with an understanding of IT security and cybersecurity concepts.

Pre-Requisites

❖ **IT Fundamentals:**

A foundational knowledge of computer operating systems (Windows, Linux, Unix), networking concepts (OSI model, IP addressing), and basic network infrastructure is beneficial.

❖ **Cybersecurity Basics:**

Familiarity with common cybersecurity principles and the importance of protecting information assets is also recommended.

❖ **Experience:**

While not always mandatory, experience in related fields like network security, ethical hacking, or digital forensics can be advantageous.

Course content

- Module 1: Information Security Fundamentals
- Module 2: Networking 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: Wireless Network Security
- Module 14: Web Security
- Module 15: Ethical Hacking and Pen Testing
- Module 16: Incident Response
- Module 17: Computer Forensics Fundamentals
- Module 18: Digital Evidence
- Module 19: Understanding File Systems

Module 20: Windows Forensics

Module 21: Network Forensics and Investigating Network Traffic

Module 22: Steganography

Module 23: Analyzing Logs

Module 24: E-mail Crime and Computer Forensics

Module 25: Writing Investigative Report

Exam Preference

| | |
|---------------------|-------------|
| Exam Code | ECSS |
| Number Of Questions | 50 |
| Length Of Test | 120 Minutes |
| Passing Score | 70% |