THE DataTech™ LABS
EMPOWERING TRANSFORMATION

EC-Council Certified Security Specialist

ECSS™
EC-Council Certified Security Specialist

Course Description

EC-Council Certified Security Specialist (ECSS) 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.

Why is ECSS Important?

01 It facilitates your entry into the world of Information Security

02 It provides professional understanding about the concepts of Information Security, Network Security, and Computer Forensics

03 It provides best practices to improve organizational security posture

04 It enhances your skills as a Security Specialist and increases your employability

Course Outline

01 Information Security Fundamentals

02 Networking Fundamentals

03 Secure Network Protocols

04 Information Security Threats and Attacks

05 Social Engineering

06 Hacking Cycle

07 Identification, Authentication, and Authorization

08 Cryptography

09 Firewalls

10 Intrusion Detection System

11 Data Backup

12 Virtual Private Network

13 Wireless Network Security

14 Web Security

15 Ethical Hacking and Pen Testing

16 Incident Response

17 Computer Forensics Fundamentals

18 Digital Evidence

19 Understanding File Systems

20 Windows Forensics

21 Network Forensics and Investigating Network Traffic

22 Steganography

23 Analyzing Logs

24 E-mail Crime and Computer Forensics

25 Writing Investigative Report

What will you Learn?

Students going through ECSS training will learn:

01 Key issues plaguing the information security, network security, and computer forensics

02 Fundamentals of networks and various components of the OSI and TCP/IP model

03 Various network security protocols

04 Various types of information security threats and attacks, and their countermeasures

05 Social engineering techniques, identify theft, and social engineering countermeasures

06 Different stages of hacking cycle

07 Identification, authentication, and authorization concepts

08 Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools

09 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

10 Fundamentals of IDS and IDS evasion techniques

11 Data backup techniques and VPN security

What will you Learn?

Students going through ECSS training will learn:

12. Wireless Encryption, wireless threats, wireless hacking tools, and Wi-Fi security
13. Different types of web server and web application attacks, and countermeasures
14. Fundamentals of ethical hacking and pen testing
15. Incident handling and response process
16. Cyber-crime and computer forensics investigation methodology
17. Different types of digital evidence and digital evidence examination process
18. Different type of file systems and their comparison (based on limit and features)
19. Gathering volatile and non-volatile information from Windows and network forensics analysis mechanism
20. Steganography and its techniques
21. Different types of log capturing, time synchronization, and log capturing tools
22. E-mails tracking and e-mail crimes investigation
23. Writing investigation report