Certified Cybersecurity Technician (C|CT)

Price	Duration	Delivery Methods
$2,495.00	5 Daytime Classes or 10 Evening Classes	Virtual, Private Group,

CAREER SKILLS+™

EC-Council's C|CT certification immerses students in well-constructed knowledge transfer. Training is accompanied by critical thinking challenges and immersive lab experiences that allow candidates to apply their knowledge and move into the skill development phase in the class itself. Upon completing the program, C|CT-certified professionals will have a strong foundation in cybersecurity principles and techniques as well as hands-on exposure to the tasks required in real-world jobs.

Who Should Attend

Early-career IT professionals, IT managers, career changers, and career advancers Students and recent graduate

Course Prerequisites

No specific prerequisites are required for the C|CT certification, although previous knowledge and experience in IT and networking with a focus on cybersecurity can be an advantage. Candidates should have knowledge of computers and computer networks prior to entering the C|CT program, although core technologies are covered in the curriculum.

Course Objectives

Key concepts in cybersecurity, including information security and network security
Information security threats, vulnerabilities, and attacks
The different types of malware
Identification, authentication, and authorization
Network security controlsNetwork security assessment techniques and tools (threat hunting, threat intelligence, vulnerability assessment, ethical hacking, penetration testing, configuration and asset management)
Application security design and testing techniques
Fundamentals of virtualization, cloud computing, and cloud security
Wireless network fundamentals, wireless encryption, and related security measures
Fundamentals of mobile, IoT, and OT devices and related security measures
Cryptography and public-key infrastructure
Data security controls, data backup and retention methods, and data loss prevention techniques
Network troubleshooting, traffic and log monitoring, and analysis of suspicious traffic
The incident handling and response process
Computer forensics and digital evidence fundamentals, including the phases of a forensic investigation
Concepts in business continuity and disaster recovery
Risk management concepts, phases, and frameworks

Agenda

1 - Information Security Threats and Vulnerabilities
2 - Information Security Attacks
3 - Network Security Fundamentals
4 - Identification, Authentication, and Authorization
5 - Network Security Controls: Administrative Controls
6 - Network Security Controls: Administrative Controls
7 - Network Security Controls: Technical Controls
8 - Network Security Assessment Techniques and Tools
9 - Application Security
10 - Virtualization and Cloud Computing
11 - Wireless Network Security
12 - Mobile Device Security
13 - Internet of Things (IoT) and Operational Technology (OT) Security
14 - Cryptography
15 - Data Security
16 - Network Troubleshooting

17 - Network Traffic Monitoring
18 - Network Log Monitoring and Analysis
19 - Incident Response
20 - Computer Forensics
21 - Business Continuity and Disaster Recovery
22 - Risk Management
EC-Council