EC-Council Certified Cybersecurity Technician (CCT) + Exam voucher

Duration: 5 Days **Course Code: ECCT** **Delivery Method: Virtual Learning**

Overview:

This EC-Council training will prepare you for the Certified Cybersecurity Technician certification (C|CT). It is an entry-level cybersecurity program created by EC-Council, the creator of the Certified Ethical Hacker (C|EH) certification, to address the global demand for a qualified cybersecurity workforce.
EC-Council developed the C|CT to provide individuals starting their careers in IT and cybersecurity with a certification that validates their hands-on technical skills.To equip individuals with the skills they need to pursue and develop their careers as cybersecurity specialists, consultants, network engineers, IT administrators, and more.
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.

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

The C|CT is ideal for anyone looking to start their career in cybersecurity or add a strong foundational understanding of the cybersecurity concepts and techniques required to be effective on the job.

The course is especially well suited to: Early-career IT professionals, IT managers, career changers, and career advancers Students and recent graduates

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 controls
- - Administrative controls (frameworks, laws, acts, governance and compliance programs, security policies)
- - Physical controls (physical and workplace security policies, environmental controls
- - Technical controls (network security protocols; network segmentation; firewalls; intrusion detection and prevention systems; honeypots;
- proxy servers; VPNs; user behavior analytics; network access control; unified threat management; security information and event
- management; security orchestration, automation, and response; load baancers; anti-malware
- 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

- Network security assessment techniques and tools (threat hunting, threat intelligence, vulnerability assessment, ethical hacking, penetration testing, configuration and asset management)

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.

Testing and Certification

Exams:

Exam Title: Certified Cybersecurity Technician

Exam Code: 212-82

Number of Questions: 60

Duration: 3 hours

Exam Availability Locations: ECC Exam Portal

Languages: English

Test Format: Multiple Choice and Real Life hands-on Practical Exam

Passing Criteria:

In order to maintain the high integrity of our certification exams, EC-Council Exams are provided in multiple forms (i.e., different question banks). Each form is carefully analyzed through beta testing with an appropriate sample group under the purview of a committee of subject matter experts that ensure that each of our exams not only have academic rigor but also have “real world” applicability. We also have a process to determine the difficulty rating of each question. The individual rating then contributes to an overall “Cut Score” for each exam form. To ensure each form has equal assessment standards, cut scores are set on a “per exam form” basis. Depending on which exam form is challenged, cut scores can range from 60% to 85%.

Exam Mode: Remote Proctoring Services

Certification:

Certified Cybersecurity Technician certification

The C|CT certification prepares IT and cybersecurity professionals to handle a wide range of complex issues related to securing software, networks, and IT systems against common cyberthreats and attacks.

The C|CT offers a multifaceted approach that incorporates network defense, ethical hacking, and security operations to ensure that certification holders have a strong, well-rounded background that enables them to configure, analyze, and identify problems within an organization.

The C|CT course equips participants with the skills required for the following roles:

- - IT networking specialist
- - Cybersecurity technician
- - Network administrator
- - Security operations center (SOC) analyst
- - Network engineer
- - IT manager

Content:

- Module 01: Information Security Threats and Vulnerabilities
- Module 02: Information Security Attacks
- Module 03: Network Security Fundamentals
- Module 04: Identification, Authentication, and Authorization
- Module 05: Network Security Controls – Administrative Controls
- Module 06: Network Security Controls – Physical Controls
- Module 07: Network Security Controls – Technical Controls
- Module 08: Network Security Assessment Techniques and Tools
- Module 09: Application Security
- Module 10: Virtualization and Cloud Computing
- Module 11: Wireless Network Security
- Module 12: Mobile Device Security
- Module 13: IoT and OT Security
- Module 14: Cryptography
- Module 15: Data Security
- Module 16: Network Troubleshooting
- Module 17: Network Traffic Monitoring
- Module 18: Network Logs Monitoring and Analysis
- Module 19: Incident Response
- Module 20: Computer Forensics
- Module 21: Business Continuity and Disaster Recovery
- Module 22: Risk Management

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/