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

Duration: 365 Days **Course Code: ECCT** **Delivery Method: e-Learning**

Overview:

EC-Council has developed the Certified Cybersecurity Technician certification:
- To validate hands-technician-level IT and cybersecurity skills.
- It's an entry-level cybersecurity program engineered by the creators of the Certified Ethical Hacker program to address the global demand for cybersecurity technicians.
- To prepare individuals with core security skills to pursue and develop their cybersecurity careers as cybersecurity specialists, consultants, network engineers, or IT administrators

Target Audience:

Job Roles:
Jr. Security administrator
Network administrator
Information technology (IT) Helpdesk
Jr. systems engineer
Jr. Security engineer
Systems administrator
Jr. Cybersecurity Technician
Network Security Technician

Objectives:

- Key issues plaguing the cyber security (information security and network security)
- Information security threats, vulnerabilities, and attacks
- Different types of malware
- Network security fundamentals
- Network security controls:
- - Administrative controls (frameworks, laws, acts, governance and compliance program, and security policies)
- - Physical controls (physical security controls, workplace security, and environmental controls)
- - Technical controls (network security protocols, network segmentation, firewall, IDS/IPS, honeypot, proxy server,
- - VPN, UBA, NAC, UTM, SIEM, SOAR, load balancer, and anti-malware tools)
- Network security assessment techniques and tools (threat hunting, threat intelligence, vulnerability assessment, ethical hacking, penetration testing, and configuration and asset management)
- Identification, authentication, and authorization concepts
- Application security design and testing techniques
- Fundamentals of virtualization, cloud computing, and cloud security
- Wireless network fundamentals, wireless encryption, and security measures
- Fundamentals of mobile, IoT, and OT devices and their security measures
- Cryptography and public key infrastructure concepts
- Data security controls, data backup and retention methods, and data loss prevention techniques
- Network troubleshooting, traffic monitoring, log monitoring and analysis for suspicious traffic
- Incident handling and response process
- Computer forensics fundaments, digital evidence, and forensic investigation phases
- Business continuity (BC) and disaster recovery (DR) concepts
- Risk management concepts, phases, and frameworks

Testing and Certification

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 Prefix: 212-82

Number of Questions: 60

Test Duration: 3 Hours

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

Test Delivery: EC-Council Exam Portal

Content:

- Information Security Threats and Vulnerabilities
- Information Security Attacks
- Network Security Fundamentals
- Identification, Authentication, and Authorization
- Network Security Controls – Administrative Controls
- Network Security Controls – Physical Controls
- Network Security Controls – Technical Controls
- Network Security Assessment Techniques and Tools
- Business Continuity and Disaster Recovery
- Application Security
- Virtualization and Cloud Computing
- Wireless Network Security
- Mobile Device Security
- IoT and OT Security
- Cryptography
- Data Security
- Network Troubleshooting
- Network Traffic Monitoring
- Network Logs Monitoring and Analysis
- Incident Response
- Computer Forensics
- 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/