CCT: Certified Cybersecurity Technician

Course Code: CCT
Duration: 5 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

Certified Cybersecurity Technician

This ***Certified Cybersecurity Technician (C|CT)*** 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

SKILLS COVERED

By the end of this course, participants should be able to:

- 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

WHO SHOULD ATTEND?

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

PREREQUISITES

There are no prerequisites required to attend this course.

MODULES

Module 1: Information Security Threats and Vulnerabilities

Module 2: Information Security Attacks

Module 3: Network Security Fundamentals

Module 4: Identification, Authentication, and Authorization

Module 5: Network Security Controls – Administrative Controls

Module 6: Network Security Controls – Physical Controls

Module 7: Network Security Controls – Technical Controls

Module 8: Network Security Assessment Techniques and Tools

Module 9: Business Continuity and Disaster Recovery

Module 10: Application Security

Module 11: Virtualization and Cloud Computing

Module 12: Wireless Network Security

Module 13: Mobile Device Security

Module 14: IoT and OT Security

Module 15: Cryptography

Module 16: Data Security

Module 17: Network Troubleshooting

Module 18: Network Traffic Monitoring

Module 19: Network Longs Monitoring and Analysis

Module 20: Incident Response

Module 21: Computer Forensics

Module 22: Risk Management

END OF PAGE