Certified Cybersecurity Technician Certification (C|CT)

Duration 5 days

COURSE DESCRIPTION

According to a report by the Centre for Strategic & International Studies, 82% of employers are facing a shortage of cybersecurity talent (Crumpler & Lewis, 2019). The industry urgently needs IT and cybersecurity professionals who can tackle the ever-growing global threat of cybercrime. To address the cybersecurity skills gap, EC-Council has developed the Certified Cybersecurity Technician (C|CT) certification. The C|CT goes beyond teaching fundamental cybersecurity concepts by validating course participants' IT and cybersecurity skills through extensive hands-on practice and assessment. Establishing this strong technical foundation in cybersecurity lays the groundwork for a future career in a variety of existing IT roles. The knowledge and skills gained through the C|CT can create pathways for further specialization in many cybersecurity domains, including ethical hacking, penetration testing, digital forensics, and application security. EC-Council has developed the C|CT to provide individuals starting their careers in IT and cybersecurity with a certification that validates their practical technician-level skills. With the C|CT, EC-Council aims to equip entrylevel cybersecurity professionals with the core technical skills they need to pursue and advance in careers as cybersecurity analysts, consultants, engineers, IT administrators, and more. The C|CT creates a foundation that enables individuals to grow their skills in specialized domains like penetration testing, security consulting, auditing, and system and network administration.

COURSE OBJECTIVES

- Key concepts in cybersecurity, including information security and network security
- Information security threats, vulnerabilities, and attacks
- The different types of malwares
- Identification, authentication, and authorization
- Network security controls
- Network 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

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

- 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

COURSE OUTLINE

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: Physical 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

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.

WHO SHOULD ATTEND

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
- IT manager
- Network engineer

EXAM DETAILS

Exam Title: Certified Cybersecurity Technician
Exam Code: 212-82
Number of Questions: 60
Duration: 3 hours
Test Format: Multiple choice and Real Life hands-on Practical Exam
Passing Score: 70%

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th