# EC-Council CCT: Certified Cybersecurity Technician

**Category:** Networking & Security | **Vendor:** EC-Council

**Duration:** 5.00 hours (1 days) **4.1 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

## Course Information

| | |
|---|---|
| **Delivery Format:** | vILT |
| **Certification:** | Certified Cybersecurity Technician (CCT) |
| **Related Exam:** | CCT |

## Course Overview

The course is for beginners who want to make a career in cybersecurity. It educates professionals on security concepts, threat types, network security, app security, virtualization, computer forensics, etc. Learners can take up cybersecurity careers with practical training and new skill development.

## About This Course

The course is for beginners who want to make a career in cybersecurity. It educates professionals on security concepts, threat types, network security, app security, virtualization, computer forensics, etc. Learners can take up cybersecurity careers with practical training and new skill development.

# Learning Outcomes

**Upon successful completion of this course, participants will be able to:**

Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile,

IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud

computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network

securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management

concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer

forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork

troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security

measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices and related security measuresCryptography and public-key infrastructureData security controls, data backup and retention methods, and data loss prevention techniquesNetwork troubleshooting, traffic and log monitoring, and analysis of suspicious trafficThe incident handling and response processComputer forensics and digital evidence fundamentals, including the phases of a forensic investigationConcepts in business continuity and disaster recoveryRisk management concepts, phases, and frameworks, Course ObjectivesKey concepts in cybersecurity, including information security and network securityInformation security threats, vulnerabilities, and attacksThe different types of malwareIdentification, authentication, and authorizationNetwork 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 techniquesFundamentals of virtualization, cloud computing, and cloud securityWireless network fundamentals, wireless encryption, and related security measuresFundamentals of mobile, IoT, and OT devices

## Detailed Course Outline

Incident Response, Incident Response, Network Logs Monitoring and Analysis, Network Logs Monitoring and Analysis, Network Traffic Monitoring, Network Traffic Monitoring, Computer Forensics, Computer Forensics, Risk Management, Risk Management, Virtualization and Cloud Computing, Virtualization and Cloud Computing, Application Security, Application Security, Mobile Device Security, Mobile Device Security, Wireless Network Security, Wireless Network Security, Data Security, Data Security, Network Troubleshooting, Network Troubleshooting, Cryptography,

Cryptography, IoT and OT Security, IoT and OT Security, Network Security Assessment Techniques and Tools, Network Security Assessment Techniques and Tools, Network Security Controls – Technical Controls, Network Security Controls – Technical Controls, Business Continuity and Disaster Recovery, Business Continuity and Disaster Recovery, Network Security Controls – Physical Controls, Network Security Controls – Physical Controls, Network Security Controls – Administrative Controls, Network Security Controls – Administrative Controls, Information Security Threats and Vulnerabilities, Information Security Threats and Vulnerabilities, Identification, Authentication, and Authorization, Identification, Authentication, and Authorization, Network Security Fundamentals, Network Security Fundamentals, Information Security Attacks, Information Security Attacks

### □□ Certification Path

Certified Cybersecurity Technician (CCT)

Exam: CCT

# Frequently Asked Questions

### Q: What delivery options are available for EC-Council CCT: Certified Cybersecurity Technician?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

---

### Q: What certification does this course prepare me for?

The EC-Council CCT: Certified Cybersecurity Technician course helps prepare you for the Certified Cybersecurity Technician (CCT) certification path.

---

### Q: Which exam does this course prepare me for?

This course prepares you for the CCT official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

---

### Q: How many CPD hours does this course provide?

The 1-day EC-Council CCT: Certified Cybersecurity Technician course provides up to 4.1 CPD hours of structured learning. CPD certificates can be provided upon request.

---

### Q: What is the duration of the EC-Council CCT: Certified Cybersecurity Technician training?

The training takes place over 1 day(s), with each day lasting approximately 5.00 hours including breaks for lunch and refreshments.

---

### Q: Do you provide corporate training for EC-Council CCT: Certified Cybersecurity Technician?

Yes, we provide corporate training, dedicated training, and closed classes for EC-Council CCT: Certified Cybersecurity Technician. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

---

### Q: What related terms do people search for?

Popular related searches include: EC-Council CCT: Certified Cybersecurity Technician, EC-Council, vILT, EC-Council CCT

---

### Q: Why choose Nexus Human for EC-Council CCT: Certified Cybersecurity Technician?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

---

### Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your EC-Council CCT: Certified Cybersecurity Technician training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.


## Nexus Human

**Professional Training & Development**

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)