

# EC-Council



**C|CT**  
Certified Cybersecurity Technician

## CERTIFIED CYBERSECURITY TECHNICIAN (C|CT)

Kickstart Your Career in Cybersecurity with Skills-Based  
Labs and Exams

---

# AN EXCITING CAREER IN CYBERSECURITY AWAITS YOU

---

Companies and industries are growing increasingly dependent on technology as digital transformation becomes ubiquitous in today's business environment. Consequently, cybersecurity is now relevant for every system, device, and byte of data that organizations rely on to operate.

The COVID-19 pandemic has further augmented the need for skilled cybersecurity professionals to address the crisis organizations are facing as a result of digitalization and rising cybercrime. According to PayScale (2022), cybersecurity analysts in the United States earn a median annual salary of USD 77,000, with most positions offering between USD 54,000 and 116,000 per year. Despite this high demand and attractive compensation, however, there is not enough cybersecurity talent to fill open job positions and protect organizations' security postures.

## THE CYBERSECURITY TALENT DROUGHT

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 entry-level 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.



# THE CICT: AN INDUSTRY SOLUTION

## WHAT IS THE CICT CERTIFICATION?

---

The C|CT is an entry-level cybersecurity program engineered by EC-Council, the creator of the Certified Ethical Hacker (C|EH) certification, to address the global need and demand for cybersecurity technicians with strong foundational skills.

## WHAT IS UNIQUE ABOUT THE CICT?

---

Only Baseline  
Cybersecurity Program  
Worldwide, Offering

**85** Real-life  
Practical  
Hands-on Labs

An immersive  
**Practical  
Certification**  
Delivered in a  
Live Cyber Range

**50%**  
of Training Time:  
**Dedicated to Labs**

**Performance-Based  
Exam,**  
combined with  
**Live Cyber Range**  
Activities.

Multidisciplinary  
Learnings  
**Network Defense,  
Ethical Hacking,  
Digital Forensics &  
Security Operations**



WHAT DOES THE

## C|CT PROGRAM OFFER?

The C|CT provides the foundational skills essential for starting a career in cybersecurity, focusing on four disciplines: network defense, ethical hacking, digital forensics, and security operations.

### Key Offerings:

---

#### »» Strong Foundational Coverage

The C|CT certification provides total foundational cybersecurity domain coverage with key concepts in each domain combined with practical hands-on labs and critical thinking challenges producing world-class cyber security technologists.

#### »» Live Range Experience

Other popular programs rely on simulation and interactivity as practical-based assessment, the C|CT program is delivered on a live Cyber Range utilizing live targets and real attack systems for a truly immersive, real-life practice and assessment platform.

#### »» Capture the Flag

The C|CT certification offers capture the flag (CTF) style critical thinking challenges to accompany each lab exercise putting knowledge into practice and providing a proven record of skill demonstration. Candidates completing the C|CT program will earn the C|CT certification and have a proven track record of performing the tasks required in a live Cyber Range, proving to employers their ability to perform critical job duties.

#### »» Multiple Certifications

The course outline of the C|CT program goes above and beyond some of the more common entry-level cybersecurity programs, such as the Security+, in a completely hands-on cyber range environment instead of simulations to ensure cybersecurity skills development. We believe that candidates who successfully attain the C|CT certification will attain other leading cybersecurity certifications, including Security+, without further training

#### »» Most Affordable

Despite the unique design of the heavily hands-on course and its uses of real-world cyber range capability, the certification is one of the most affordable in the world!



# JOB ROLES FOR C|CT-CERTIFIED PROFESSIONALS

---

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:

- |                                   |   |
|-----------------------------------|---|
| ■ <b>IT networking specialist</b> | ■ <b>Network administrator</b>                    |
| ■ <b>Cybersecurity technician</b> | ■ <b>Network engineer</b>                         |
| ■ <b>IT manager</b>               | ■ <b>Security operations center (SOC) analyst</b> |

## CYBERSECURITY TECHNICIAN JOB DESCRIPTION

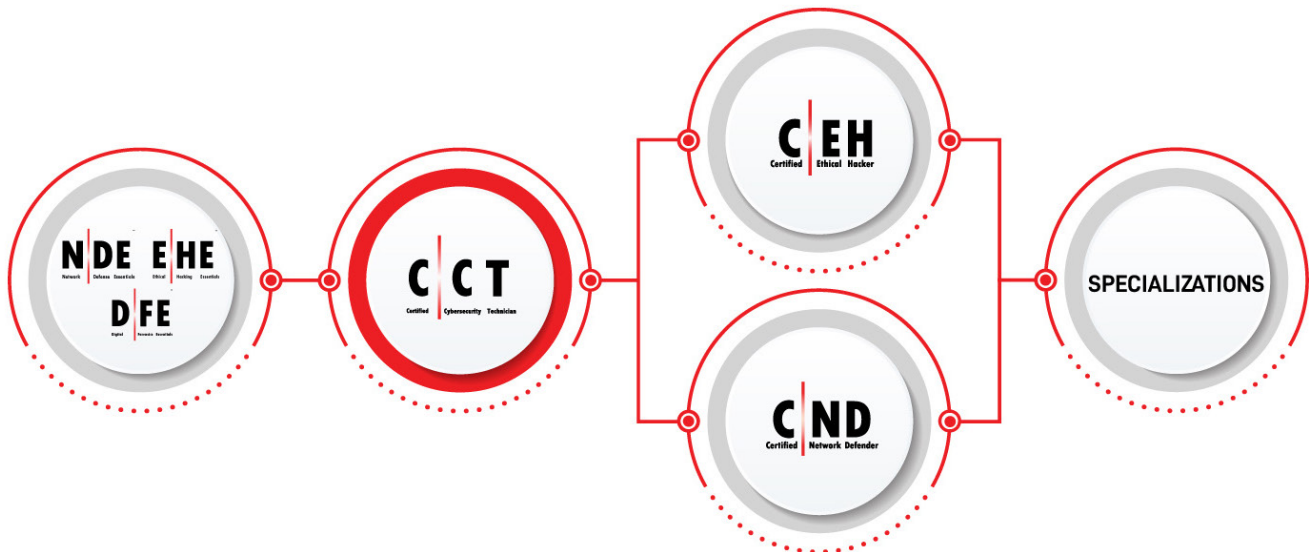
---

Cybersecurity technicians provide technical cybersecurity support, troubleshoot network security problems, monitor alerts, and follow relevant policies, procedures, and standards to protect organizations' information assets.



# CYBERSECURITY CAREER STARTER TRACK

---



Note: This is a suggested path only; courses can be taken in any order.

## C|CT COURSE DESCRIPTION

---

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.

# **CICT COURSE OUTLINE - TOPICS COVERED**

- 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**

# WHAT YOU WILL LEARN IN THIS COURSE

---

- » 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 balancers; anti-malware)
- » 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
- » 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



# WHO CAN TAKE THIS COURSE?

---

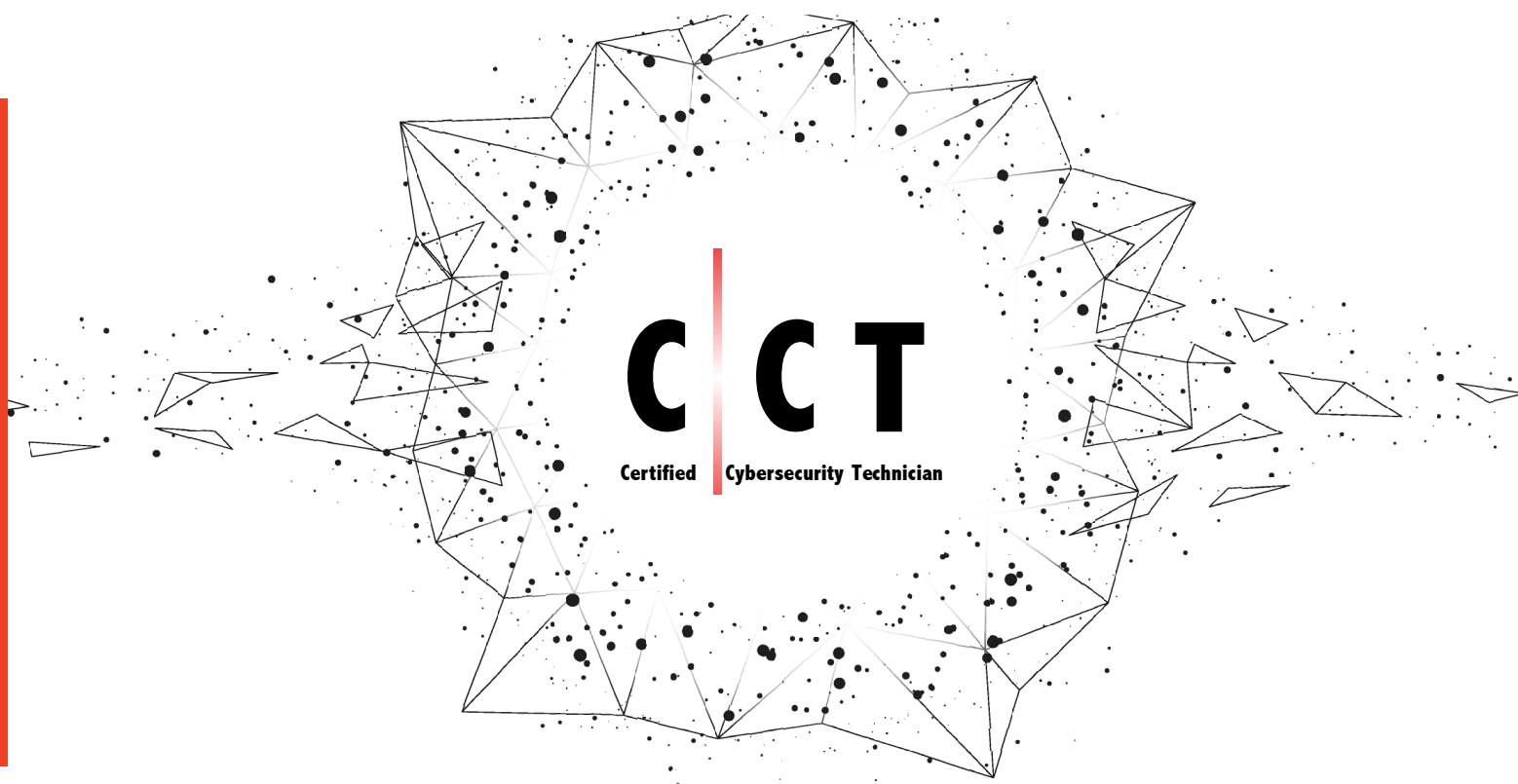
The C|CT is ideal for anyone looking to start their career in cybersecurity or add a strong foundational understanding of the cybersecurity concepts and techniques required to be effective on the job. The course is especially well suited to:

- » Early-career IT professionals, IT managers, career changers, and career advancers
- » Students and recent graduates

# WHAT ARE THE PREREQUISITES FOR THE C|CT?

---

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.



# EXAM & TRAINING INFORMATION

**Exam Title:** Certified Cybersecurity Technician

**Exam Code:** 212-82

**Number of Questions:** 60

**Duration:** 3 hours

**Exam Availability Locations:** ECC Exam Portal

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

**Exam Mode:** Remote Proctoring Services

**Passing Score:** 70%

**Training Duration:** 5 days

**Delivery Modes:** Instructor-led training

iWeek (synchronous online learning)

iLearn (asynchronous online learning)

CodeRed (asynchronous online learning)



# YOUR LEARNING PATHWAY TO A PROMISING CAREER IN CYBERSECURITY

**EC-Council**

Learning Track

Executive

Specializations

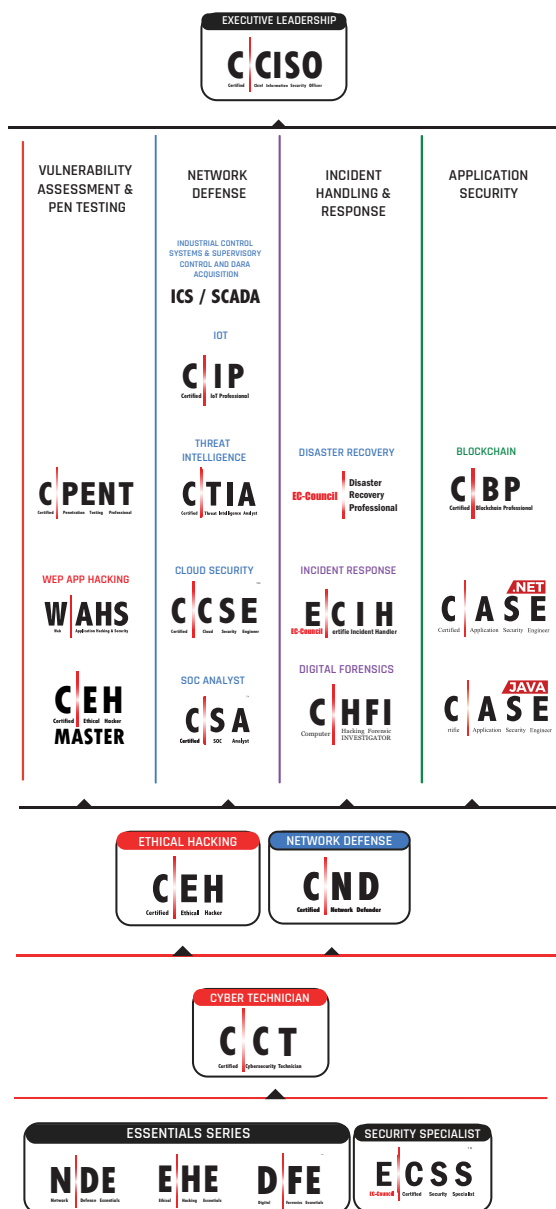
Core

Cyber Technician

Cyber Essentials

Knowledge Workers

Individual Courses



Cybersecurity Professionals

Cybersecurity Awareness

**CSCU**  
Certified Secure Computer User

Phishing Awareness

**aware**  
When Everyone Protects

**ECES**  
Certified Encryption Specialist

**codered**  
FROM EC-COUNCIL

Browse a catalog of over **10,000 courses**

# ABOUT EC-COUNCIL

---

We Set the Standards: C|ND, C|EH, C|HFI

EC-Council is trusted by seven of the Fortune 10, 47 of the Fortune 100, the Department of Defense (DoD), global intelligence communities, NATO, and more than 2,000 of the best universities, colleges, and training companies. EC-Council programs are available in more than 140 countries and set the bar in cybersecurity education.

EC-Council is an ANSI 17024-accredited organization and has earned recognition from the DoD under Directive 8140/8570, the GCHQ in the UK, CREST, and other authoritative bodies that influence the cybersecurity profession. Best known for the C|EH program, we are dedicated to equipping tomorrow's cybersecurity workforce with the knowledge, skills, and abilities required to fight malicious adversaries and win.

## EC-Council Accreditations and Recognition

---



# EC-Council



 Visit us: [www.eccouncil.org/programs/certified-cybersecurity-technician-certification/](http://www.eccouncil.org/programs/certified-cybersecurity-technician-certification/)

 Contact us: <https://www.eccouncil.org/contact-us/>

