CCT – Certified Cybersecurity Technician (e-Learning)

EC-Council

- **Nível:**
- **Duração:** 26h

Sobre o curso

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

CCT – Become a Responsible Cyber Operator in Any IT Role:

The CCT program allows individuals to eventually grow their skills into various roles, including penetration testing, security consulting, auditor and administrator roles, and beyond. It establishes a foundation of technical skills required to create successful technologists who will advance across various work roles.

EC-Council has developed the Certified Cybersecurity Technician certification

- To validate hands-on 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

What is Unique About the C|CT Program?

- Only Baseline Cybersecurity Program Worldwide Offering – **85 Real Life Praticals Hands-on Labs**
- An immersive **Pratical Certification** Delivered in a Live Cyber Range
- **Performance-Based Exam,** combined with **Live Cyber Range** Activities
- 50% of Training Time: **Dedicated to Labs**
- Multidisciplinary Learnings: Network Defense, Ethical Hacking, Digital Forensics, Security Operations

CCT's 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!

How Will the Certified Cybersecurity Technician Credential Benefit You?

It facilitates your entry into the cybersecurity realm as a cybersecurity technician. It provides fundamental professional skills and solidifies the concepts of information security, network security, computer forensics, risk management, and incident handling.

It enhances your skills as a cybersecurity specialist and increases your employability chances. It provides hands-on practical skills essential for a cybersecurity technician or any role in IT with administrative privileges where security should be considered and practiced.

Job Description of a Cybersecurity Technician:

A professional who provides technical cybersecurity support, troubleshoots network security problems, monitors alerts, and follows policies, procedures, and standards to protect information assets.

Job Opportunities & Job Roles for C|CT Credential:

The Certified Cybersecurity Technician certification prepares IT and Cybersecurity professionals for a wide range of complex issues that focus on securing software, networks, and IT systems while understanding common threats and attacks. C|CT offers a multifaceted approach to network defense, ethical hacking, and security operations to ensure individuals use their strongest abilities to configure, analyze, and identify problems within their organization. This course will prepare and enhance skills in the following roles:

- IT Support Specialist;
- IT Networking Specialist;
- Cybersecurity Technicians;
- Network Engineers;
- SOC Analyst;
- IT Managers;

Aceda aqui à brochura para saber mais acerca do curso

Destinatários

- The C|CT course can be taken by students, IT professionals, IT managers, career changers, and any individual seeking a career in cybersecurity, or aspiring to advance their existing role.
- This course is ideal for those entering the cybersecurity workforce, providing foundational technician level, hands-on skills to solve the most common security issues organizations face today.

Objetivos

- 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

Condições

Cursos E-learning EC-Council não beneficiam de isenção de IVA. Ao valor apresentado acresce IVA.

O exame da EC-Council incluído no valor do curso é, por defeito, realizado em formato remoto (online), sem custos adicionais.

Pré-requisitos

- There are no specific prerequisites to take the C|CT course and attempt the C|CT certification exam. Although this is an entry-level course, a working knowledge of IT networking and basic cybersecurity concepts will be an advantage to anyone taking this course.

Metodologia

This E-Learning course includes:

- On Demand Instructor-led Training Videos
- Official E-Courseware
- Online CyberQ Labs
- Certification Exam
- Certificate of Completion

Programa

- 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