

EC-Council Certified Network Defender (CND) + Exam voucher

Duration: 5 Days **Course Code: CND** **Version: 2.0** **Delivery Method: Virtual Learning**

Overview:

Certified Network Defender (CND) is a vendor-neutral, hands-on, instructor-led comprehensive network security certification training program. It is a skills-based, lab intensive program based on the security education framework and work role task analysis presented by the National Infocomm Competency Framework (NICF) as well as a job-task analysis and cybersecurity education framework by the National Initiative of Cybersecurity Education (NICE). The course has also been mapped to global job roles and to the Department of Defense (DoD) job roles for system/network administrators.

The program prepares network administrators how to identify what parts of an organization need to be reviewed and tested for security vulnerabilities and how to reduce, prevent, and mitigate risks in the network. CND covers the protect, detect, respond and predict approach to network security.

More than 50% of the CND course contains hands-on labs dedicated to helping students learn practical skills in live ranges designed to cover domains such as Network Defense Management, Network Perimeter Protection, Endpoint Protection, Application and Data Protection, Enterprise Virtual, Cloud, and Wireless Network Protection, Incident Detection and response and Threat Prediction which will provide network administrators real world expertise that can be applied to current network security technologies and operations.

CND Course Benefits:

- A dedicated focus on IoT security
- Network virtualization practices for the remote workforce
- Enhanced Cloud Security & IoT and Operational Technology (OT) Modules
- Introduction to threat intelligence
- In-depth Attack Surface Analysis

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

Who Should Attend?

Network Administrators
Network security Administrators
Network Security Engineer
Network Defense Technicians
CND Analyst
Security Analyst
Security Operator

Job Roles

Security Analyst III
Cyber Security Analyst, Senior
Cyber Security Analyst, Principal
Vulnerability Analyst, Principal
Security Analyst II
Security Analyst I
Network Administrator
Staff Network Engineer
Information Systems Security Manager
Mid Level Penetration Tester
Staff Network Engineer
Sr. Digital Forensics Analyst
Penetration Tester
Linux System Administrator
Cybersecurity Engineer II Red Team

Testing and Certification

EXAM

Passing Score

In order to maintain the high integrity of our certifications exams, EC-Council Exams are provided in multiple forms (I.e. different question banks). Each form is carefully analyzed through beta testing with an appropriate sample group under the purview of a committee of subject matter experts that ensure that each of our exams not only has academic rigor but also has "real world" applicability. We also have a process to determine the difficulty rating of each question. The individual rating then contributes to an overall "Cut Score" for each exam form. To ensure each form has equal assessment standards, cut scores are set on a "per exam form" basis. Depending on which exam form is challenged, cut scores can range from 60% to 78%.

Exam Prefix: 312-38 (ECC EXAM)

Number of Questions: 100

Test Duration: 4 Hours

Test Format: Multiple Choice

Test Delivery: ECC Exam

Content:

Module 01: Network Attacks and Defense Strategies

Module 02: Administrative Network Security

Module 03: Technical Network Security

Module 04: Network Perimeter Security

Module 05: Endpoint Security-Windows Systems

Module 06: Endpoint Security-Linux Systems

Module 07: Endpoint Security- Mobile Devices

Module 08: Endpoint Security-IoT Devices

Module 09: Administrative Application Security

Module 10: Data Security

Module 11: Enterprise Virtual Network Security

Module 12: Enterprise Cloud Network Security

Module 13: Enterprise Wireless Network Security

Module 14: Network Traffic Monitoring and Analysis

Module 15: Network Logs Monitoring and Analysis

Module 16: Incident Response and Forensic Investigation

Module 17: Business Continuity and Disaster Recovery

Module 18: Risk Anticipation with Risk Management

Module 19: Threat Assessment with Attack Surface Analysis

Module 20: Threat Prediction with Cyber Threat Intelligence

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo