EC Council – CNDv2

Certified Network Defender v2

Days: *5*

Prerequisites: To be eligible to challenge the EC-Council CND certification examination, the candidate has 2 options:

Attend Official Network Security Training by EC-Council: If a Candidate has completed an official EC-Council training either at an Accredited Training Center, via the iClass platform, or at an approved academic institution, the candidate is eligible to challenge the relevant EC-Council exam without going through the application process.

Attempt the Exam without Official EC-Council Training: In order to be considered for the EC-Council CND v2 exam without attending official network security training, the candidate must have at least 2 years of work experience in the Information Security domain. If the candidate has the required work experience, they can submit an eligibility application form along with USD 100.00, a non-refundable fee.

Audience: CND v2 is for those who work in the network administration/cybersecurity domain in the capacity of Network Administrator/Engineer, Network Security Administrator/Engineer/Analyst, Cybersecurity Engineer, Security Analyst, Network Defense Technician, Security Operator. CND v2 is for all cybersecurity operations, roles, and anyone looking to build a career in cybersecurity.

Description: CND v2 is based on the cybersecurity education framework and work role task analysis presented by the National Infocomm Competency Framework (NICF). The program is also mapped to the Department of Defense (DoD) roles for system/network administrators as well as global work roles and responsibilities laid out by the revised NICE Framework 2.0

Course Objectives:

- Network security management
- Network security policies and procedures
- Windows and Linux security administration
- Mobile and IoT device security
- Data security techniques
- Virtualization technology security
- Cloud and Wireless Security
- Risk assessment tools
- Basics of first response and forensics
- Indicators of Compromise, Attack, and Exposures (IoC, IoA, IoE)
- Threat intelligence capabilities
- Log management
- Endpoint security
- Firewall solutions
- IDS/IPS technologies
- Network Authentication, Authorization, Accounting (AAA)

EC Council – CNDv2

Certified Network Defender v2

OUTLINE:

MODULE 1 – NETWORK ATTACKS AND DEFENSE STRATEGIES

MODULE 2 – ADMINISTRATIVE NETWORK SECURITY

MODULE 3 – TECHNICAL NETWORK SECURITY

MODULE 4 – NETWORK PERIMETER SECURITY

MODULE 5 – ENDPOINT SECURITY – WINDOWS SYSTEMS

MODULE 6 – ENDPOINT SECURITY – LINUX SYSTEMS

MODULE 7 – ENDPOINT SECURITY – MOBILE DEVICES

MODULE 8 – ENDPOINT SECURITY – IOT DEVICES

MODULE 9 – ADMINSTRATIVE 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 PROTECTION WITH CYBER THREAT INTELLIGENCE