Certified Network Defender v3 (CND)

Course Duration: 40 Hours (5 Days)

Overview

The Certified Network Defender (CNDv2) course, offered by EC-Council, is a comprehensive program designed to equip learners with the necessary skills to defend, detect, and respond to Network attacks. It is a professional-level certification that focuses on creating network administrators versed in protecting, detecting, and responding to threats on the network. The course covers a wide range of topics from Network attacks and Defense strategies, to securing both the perimeter and the endpoint devices, including Windows and Linux systems, mobile and IoT devices. Learners will also delve into administrative and technical security controls, Application security, Data security, Virtual network security, Cloud network security, and Wireless security. The program includes training on network traffic and logs monitoring, incident response, Forensic investigation, business continuity, Disaster recovery, risk management, Attack surface analysis, and Cyber threat intelligence. By completing the Certified Network Defender v2 training, participants will gain practical, hands-on experience that will enable them to effectively manage and protect their network environments. This certification is a part of the EC-Council's cyber security track and is highly regarded in the industry for its depth and real-world applicability.

Audience Profile

The Certified Network Defender (CNDv2) course equips IT professionals with skills in defending, detecting, and responding to network threats. Target Audience for the Certified Network Defender (CNDv2) course:

- Network Defense Technicians
- CND Analysts
- Security Analysts
- Security Operators
- Anyone involved in network operations
- IT Professionals looking to enhance their network defense skills
- IT Managers overseeing network and security operations
- Incident Response Team Members
- Cybersecurity Consultants
- Infrastructure and Cloud Security Personnel
- Risk Management Professionals
- Government and Military Defense Personnel with network security duties

Course Syllabus

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 device

Module 8

- Endpoint Security-IoT Devices

Module 9

- 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