COURSE OUTLINE

EC-Council
Accredited
Training Center

Course Code: EC-CND

Course Name: CND: Certified Network Defender

DURATION	SKILL LEVEL	DELIVERY METHOD	TRAINING CREDITS	TECHNOLOGY
5 day (s)	Beginner	In Class	N/A	EC-Council

Course Overview

Organizational focus on cyber defense is more important than ever as cyber breaches have a far greater financial impact and can cause broad reputational damage.

Despite best efforts to prevent breaches, many organizations are still being compromised. Therefore, organizations must have, as part of their defense mechanisms, trained network engineers who are focused on protecting, detecting, and responding to the threats on their networks. Network administrators spend a lot of time with network environments, and are familiar with; network components; network traffic; performance and utilization; network topology; location of each system; and security policies etc.

The Certified Network Defender (CND) course is a vendor-neutral, hands-on, instructor-led comprehensive network security certification training program that prepares Network Administrators on network security technologies and operations to attain Defense-in-Depth network security skills. The course contains hands-on labs, based on major network security tools and techniques which will provide Network Administrators real world expertise on current network security technologies and operations.

Prerequisites

- The knowledge and skills that a learner must have before attending this course is as follows:
- Fundamental knowledge of Networking Concepts.

Target Audience

- Network Administrators
- Network Security Administrators
- Network Security Engineers
- Network Defense Technicians
- Security Analysts
- Security Operators
- Anyone who is involved in network operations

Topics

Module 01: Computer Network and Defense Fundamentals

Module 02: Network Security Threats, Vulnerabilities, and Attacks

Module 03: Network Security Controls, Protocols, and Devices

Module 04: Network Security Policy Design and Implementation

Module 05: Physical Security

Module 06: Host Security

Module 07: Secure Firewall Configuration and Management

Module 08: Secure IDS Configuration and Management

Module 09: Secure VPN Configuration and Management

Module 10: Wireless Network Defense

Module 11: Network Traffic Monitoring and Analysis

Module 12: Network Risk and Vulnerability Management

Module 13: Data Backup and Recovery

Module 14: Network Incident Response and Management

Exams and Certifications

At course completion

You will learn how to protect, detect and respond to network attacks. You will learn network defense fundamentals, the application of network security controls, protocols, perimeter appliances, secure IDS, VPN and firewall configuration. You will then learn the intricacies of network traffic signature, analysis and vulnerability scanning which will help you when you design greater network security policies and successful incident response plans. These skills will help you foster resiliency and continuity of operations during attacks.