EC Council Certified Network Defender (v3) Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

The {*training} is the world's first **adaptive network security certification**, designed to help professionals build and manage resilient, threat-ready networks.

Developed by **EC-Council**, this ANSI-accredited and DoD-approved program provides hands-on, tactical skills to defend enterprise networks in real-world cyber environments.

CND v3 includes **100+ lab-based exercises** and aligns with the **National Initiative for Cybersecurity Education (NICE) Framework**, mapping directly to job roles such as **Network Security Engineer, Analyst, and Cyber Defense Specialist**.

The course covers **Zero Trust architectures, Cloud Defense (AWS, Azure, GCP), EDR/XDR, IoT Security**, and **Cyber Threat Intelligence** — ensuring learners are job-ready to meet today's network defense challenges.

The **EC-Council Certified Network Defender (CND) v3** course equips professionals with the essential defensive, analytical, and incident response skills required to protect modern network environments.

Graduates earn an **internationally recognized CND certification**, backed by **ANSI ISO/IEC 17024** accreditation and **US DoD approval**, validating their readiness to defend organizations against advanced cyber threats.

Bilginç IT Academy is an **Official Accredited Training Partner of EC-Council**, delivering EC-Council-authorized cybersecurity trainings and certification programs globally.

Prerequisites

There are no mandatory prerequisites. However, it is recommended that learners have:

- A **basic understanding of networking concepts** (TCP/IP, routers, switches, firewalls, etc.)
- Familiarity with general cybersecurity principles

EC Council Certified Network Defender (v3) Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Who Should Attend

- Network administrators and engineers
- Network security analysts and SOC personnel
- IT managers and cybersecurity specialists
- Security auditors and consultants
- System administrators managing secure environments

What You Will Learn

By the end of this {*training}, you will have gained knowledge and skills in the following areas:

- Plan and implement enterprise network defense strategies
- Identify threats, vulnerabilities, and Indicators of Compromise (IoCs)
- Implement IAM, encryption, and segmentation practices
- Secure Windows, Linux, Mobile, and IoT endpoints
- Protect virtual and cloud infrastructures (AWS, Azure, GCP)
- Configure and manage firewalls, IDS/IPS, and network monitoring systems
- Detect, analyze, and respond to network incidents
- Utilize threat intelligence for proactive cyber defense
- Apply Zero Trust and SOAR frameworks in real-world environments
- Support Business Continuity and Disaster Recovery (BC/DR) plans

Outline

Network Defense Management – Security fundamentals, adaptive defense, compliance, policies
Network Perimeter Security – IAM, encryption, firewalls, IDS/IPS, Zero Trust
Endpoint Protection – Windows, Linux, Mobile, IoT endpoint hardening
Application & Data Security – WAF, encryption, DLP, secure application management
Virtualization, Cloud, and Wireless Protection – AWS, Azure, GCP, SDN, wireless defense
Incident Detection – Network and log monitoring, Wireshark, anomaly detection
Incident Response & Forensics – First response, digital forensics, BC/DR
Threat Prediction – Risk management, attack surface analysis, threat intelligence