THE LEARNING CENTER
A TECHNICAL TRAINING INSTITUTION

C|ND™

CERTIFIED NETWORK DEFENDER

EC-Council Certified Network Defender

EC-Council's Certified Network Defender has been designed by industry experts to help IT Professionals play an active role in the Protection of digital business assets and to the Detection and Response to Cyber Threats, while leveraging Threat Intelligence to Predict them before they happen.

Skills measured

- Understanding of security concepts including deployments, security terminology, access control models and defense in depth strategies.
- Monitoring the environment identifying network, web application and endpoint-based attacks.
- Describe management concepts such as asset, configuration, and mobile device management.

EC-Council's Certified Network Defender is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements.

Our unique model follows a streamlined approach to workforce development and skills attainment

Assess: Assess each student to determine existing skill sets

Educate: Deliver goal-specific training utilizing all delivery modalities

Mentor: Expose students to instructors and mentors with front-line IT and cybersecurity experience

Certify: Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate: Validate student abilities through performance analytics and real-world exercises hosted on a cyber range

Exam Objectives: 312-38 CNDv2

Network Defense Management	10%
Network Perimeter Protection	16%
Endpoint Protection	15%
Application and Data Protection	13%
Enterprise Virtual, Cloud, and Wireless Network Protection	12%
Incident Detection	14%
Incident Response	10%
Incident Prediction	10%

Course Outline:

Chapter 1: Network Attacks and Defense Strategies
Chapter 2: Administrative Network Security
Chapter 3: Technical Network Security
Chapter 4: Network Perimeter Security
Chapter 5: Endpoint Security – Windows Systems
Chapter 6: Endpoint Security – Linux Systems
Chapter 7: Endpoint Security – Mobile Devices
Chapter 8: Endpoint Security – IoT Devices
Chapter 9: Administrative Application Security
Chapter 10: Data Security
Chapter 11: Enterprise Virtual Network Security
Chapter 12: Enterprise Cloud Network Security
Chapter 13: Enterprise Wireless Network Security
Chapter 14: Network Traffic Monitoring and Analysis
Chapter 15: Network Logs Monitoring and Analysis
Chapter 16: Incident Response and Forensic Investigation
Chapter 17: Business Continuity and Disaster Recovery
Chapter 18: Risk Anticipation with Risk Management
Chapter 19: Threat Assessment with Attack Surface Analysis
Chapter 20: Threat Prediction with Cyber Threat Intelligence

Included

40 hours of instructor-led training sessions
EC-Council authorized textbook and class materials
Practice questions and exam study tips