Course Outline

Certified Network Defender
Course CND: 5 days Instructor Led

About this course
EC-Council has reviewed the entire CND space as designated by the Department of Defense as IAT I, II, III, and IAM I, II, III as well as the NICE Framework KSA's as they relate to cyber defense and day-to-day cyber operations. With each of these considered, they built their exam blueprint, and overall training scope, and got to work building the next certification we believe will be a game changer for cyber security professionals – Certified Network Defender. The class is a professional-level introduction to the cyber defense strategies needed in today's critical infrastructure.

Audience profile
- System administrators
- System engineers
- Firewall administrators
- Network managers
- IT managers
- IT professionals
- Anyone interested in network security technologies
- Managers who want to understand cyber security core principles and practices
- Operations personnel, who do not have security as their primary job function, will need an understanding of cyber security core principles and practices

At course completion
After completing this course, students will be able to:
- 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)

Course Outline

Module 01: Network Attacks and Defense Strategies
Module 02: Administrative Network Security
Module 03: Technical Network Security
Module 04: Network Perimeter Security

SHI | TRAINING & ADOPTION

Course Outline

Module 05: Endpoint Security-Windows Systems
Module 06: Endpoint Security-Linux Systems
Module 07: Endpoint Security- Mobile Devices
Module 08: Endpoint Security-IoT Devices
Module 09: 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