Certified Network Defender

OUR LEARNING EXCLUSIVE

- Custom exam prep software and materials
- Exam delivery in the classroom, with a **98% success rate**
- Course-specific thinQtank® Learning publications to make the learning fun and engaging
- Extended hours of training, including immersive hands-on exercises
- **We do not teach the test.** We always deliver valuable hands-on experience
- All reading material and study guides sent to you when you register
- Every course taught by certified expert engineers

TRAINING CAMP FORMAT

thinQtank® Learning delivers this course as an **instructor-led training camp**, with the exam sat in the classroom as part of the camp. Camps are scheduled by cohort rather than to a fixed calendar, and the balance of lecture and practical lab work is set to suit the group and the delivery method. Contact us for the schedule covering your dates.

TARGET AUDIENCE

- System and network administrators, and system engineers
- Firewall administrators, network managers and IT managers
- Anyone interested in network security technologies
- Managers who need to understand cyber security core principles and practices
- Operations staff who need security grounding without security as their main role
- Network+ and Security+ holders, and Cisco, Microsoft or Juniper certified administrators, moving into a defensive security role

PREREQUISITES

- You should be well-versed in cyber security fundamentals
- Working knowledge of Windows and Linux administration
- Familiarity with TCP/IP networking, addressing and common protocols

DELIVERY METHODS

- Instructor-led training
- Immersive live-online training
- On-site and custom delivery

COURSE OVERVIEW

thinQtank® Learning offers a unique training camp for **EC-Council Certified Network Defender**. As with all our EC-Council training experiences, the exam is delivered in the classroom.

CND is a professional-level introduction to the cyber defense strategies needed in today's critical infrastructure. EC-Council reviewed the whole network-defense space — the Department of Defense workforce requirements and the NICE Framework knowledge, skills and abilities as they relate to day-to-day cyber operations — and built the exam blueprint and training scope from that.

The program is designed to help IT professionals take an active role in the **protection** of digital business assets, the **detection of** and **response to** cyber threats, and the use of threat intelligence to **predict** them before they happen.

The end goal is to help Blue Teams defend and win against network breaches — with coverage of cloud, IoT, virtualization and remote-worker threats, attack surface analysis, threat intelligence, software-defined networking, network function virtualization, and Docker, Kubernetes and container security.

EXAM

312-38 — Certified Network Defender

4 hours · 100 multiple-choice questions · delivered through the ECC exam portal. EC-Council sets the cut score per exam form, in a range of **60%–85%**.

One exam earns **Certified Network Defender** — ANSI/ISO/IEC 17024 accredited through ANAB, and approved under DoD Directive 8140 for the Cyber Defense work roles.

EXCLUSIVE LEARNING PACKAGE

- Comprehensive video training package
- Virtual Debian-derived distribution packed with digital forensics tools and utilities
- **68 guided lab exercises** during the course, mapped module by module
- Six months' access to the EC-Council virtual lab environment for CND
- After-course instructor coaching benefits
- Exam voucher included, and the exam delivered in the classroom

JOB ROLES IT QUALIFIES YOU FOR

- Entry-level network administrator
- Entry-level network security administrator
- Data security analyst
- Junior network security engineer
- Junior network defense technician
- Security analyst
- Security operator

Certified Network Defender

COURSE OBJECTIVES

This course will help you learn:

- Network security management, 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
- The basics of first response and forensics
- Indicators of compromise, attack and exposure (IoC, IoA, IoE)
- Threat intelligence capabilities
- Log management
- Endpoint security and firewall solutions
- IDS/IPS technologies
- Network authentication, authorization and accounting (AAA)

COURSE MODULES AND LABS

01 Network Attacks and Defense Strategies
- Understanding the Workings of SQL Injection Attacks
- Understanding the Workings of XSS Attacks
- Understanding the Workings of Network Scanning Attacks
- Understanding the Workings of Brute-Force Attacks

02 Administrative Network Security
- Implementing Password Policies Using Windows Group Policy
- Implementing Password Policies in Linux
- Monitoring Activities on a Remote User System

03 Technical Network Security
- Implementing Just Enough Administration to Secure Privileged Access
- Implementing Role-Based Access Control Using Windows Admin Center

04 Network Perimeter Security
- Network-Based Firewall: Blocking Unwanted Website Access Using pfSense
- Network-Based Firewall: Blocking Insecure Ports Using pfSense
- Network-Based Firewall: Blocking Internal FTP Server Access Using Smoothwall
- Host-Based Firewall Functionality Using Windows Firewall
- Host-Based Firewall Protection with iptables
- Network-Based IDS Functionality Using Suricata IDS
- Host-Based IDS Functionality Using Wazuh HIDS

05 Endpoint Security — Windows Systems
- Basic Network Administration and Troubleshooting Using Windows Command-Line Utilities
- Securing Windows File Share in Active Directory
- Analyzing Security Configuration Baseline Using Microsoft Security Compliance Toolkit
- Remote Patch Management Using BatchPatch
- Remote Patch Management Using ManageEngine Patch Manager Plus
- Delegating Admin Permission to a User Using the Delegation of Control Wizard
- Securing the Local Administrator Password Using LAPS

06 Endpoint Security — Linux Systems
- Implementing Linux Security Best Practices

07 Endpoint Security — Mobile Devices
- Implementing Enterprise Mobile Security Using Miradore MDM Solution

08 Endpoint Security — IoT Devices
- Securing IoT Device Communication Using TLS/SSL

09 Administrative Application Security
- Implementing Application Whitelisting Using AppLocker

10 Data Security
- Encrypting Data at Rest Using VeraCrypt
- Implementing Encryption on a SQL Server Database Using Transparent Data Encryption
- Implementing Always Encrypted in SQL Server
- Encrypting Data in Transit Using SSL
- Ensuring Secure Email Communication Using PGP
- Performing Data Backup Using AOMEI Backupper Standard
- File Recovery Using EaseUS Data Recovery Wizard
- File Recovery Using Kernel for Windows Data Recovery Tool
- Partition Recovery Using MiniTool Power Data Recovery Tool

11 Enterprise Virtual Network Security
- Auditing Docker Host Security Using the Docker-Bench-Security Tool
- Securing SDN Communication Between Switch and SDN Controller Using SSL

COURSE MODULES AND LABS CONTINUED

12 Enterprise Cloud Network Security
- Implementing Amazon Web Services Identity and Access Management
- Implementing Key Management Services in Amazon Web Services
- Securing Amazon Web Services Storage

13 Enterprise Wireless Network Security
- Configuring Security on a Wireless Router

14 Network Traffic Monitoring and Analysis
- Capturing Network Traffic Using Wireshark
- Analyzing and Examining Various Network Packet Headers Using Wireshark
- Analyzing and Examining Various Network Packet Headers in Linux Using tcpdump
- Applying Various Filters in Wireshark
- Detecting Clear-Text Traffic Using Wireshark
- Monitoring and Detecting Network Reconnaissance Attempts
- Detecting a Brute-Force Attempt Using Wireshark
- Detecting an SQL Attack Using Wireshark
- Network Traffic Monitoring Using PRTG
- Network Traffic Analysis Using Capsa
- Network Traffic Bandwidth Monitoring — NTOP in pfSense

15 Network Logs Monitoring and Analysis
- Configuring, Viewing and Analyzing Windows Event Logs
- Configuring, Viewing and Analyzing IIS Logs
- Configuring, Viewing and Analyzing Logs in a Centralized Location Using Splunk
- Identifying Suspicious Activities Using Log Monitoring and Analysis

16 Incident Response and Forensic Investigation
- Working with Incident Tickets in OSSIM

17 Business Continuity and Disaster Recovery
- Implementing Business Continuity and Disaster Recovery Using NLB

18 Risk Anticipation with Risk Management
- Vulnerability Management Using OSSIM
- Vulnerability Analysis Using Nessus
- Network Vulnerability Scanning Using GFI LanGuard
- Auditing Network Security with Nsauditor
- Application Vulnerability Scanning Using OWASP ZAP

19 Threat Assessment with Attack Surface Analysis
- System Attack Surface Analysis Using Windows Attack Surface Analyzer
- Analyzing Web Application Attack Surface Using OWASP Attack Surface Detector
- Attack Surface Mapping and Visualization Using Amass

20 Threat Prediction with Cyber Threat Intelligence
- Integrating OTX Threat Feeds in OSSIM

WHY THIS PROGRAM

Accredited and recognized
ANSI/ISO/IEC 17024 accredited through ANAB, built on common job-role frameworks recognized worldwide, and mapped to the NICE Framework.

Approved under DoD 8140
EC-Council maps CND to the DoD Cyber Workforce Framework work roles **511** Cyber Defense Analyst, **521** Cyber Defense Infrastructure Support Specialist and **531** Cyber Defense Incident Responder.

A blue-team pathway
The protect, detect, respond and predict approach defines the job roles of a blue-team professional. CND covers the base, so you can continue as a network defender or move into a specialist profile.

Mobile and IoT defense
Device-level and enterprise-level security in one program — useful in its own right to anyone moving into cybersecurity from another discipline.

Tactical defense of cloud services
Securing workloads across Amazon Web Services, Microsoft Azure and Google Cloud Platform.

Beyond the technical
A strong focus on the strategic domain — adaptive and defense-in-depth security, framing network policies, achieving compliance — and on the operational domain of implementing those decisions.

Perimeter defense skills
Modern networks have grown complex enough that perimeter defense needs deliberate attention; CND puts it in the spotlight.

68 guided lab exercises
Learning under simulated threat conditions, so the skills are practiced before you need them in production.