

312-38: Certified Network Defender (CND)

Defend enterprise networks with layered controls, monitoring and incident response — and prepare for the CND 312-38 exam.

DURATION

5 days · 40 hours

LEVEL

Intermediate

CURRICULUM

14 modules · 7 labs

DELIVERY

Live online, Onsite,
Corporate

Course overview

Network defenders keep the organisation running while attackers probe it every day. Their work spans policy, perimeter controls, endpoints, applications, cloud and wireless networks, along with monitoring that spots trouble early and a response process that limits damage. This five-day course is exam-aligned preparation for the Certified Network Defender 312-38 exam, built on the protect, detect, respond and predict approach.

Day one covers network attacks and defence strategies, administrative security controls such as policies and compliance, and physical security. Day two focuses on technical controls at the perimeter and inside the network: firewalls, IDS and IPS, VPNs, network segmentation and access control. Day three addresses endpoint security for Windows, Linux, mobile and IoT devices, followed by application and data security.

Day four covers enterprise virtual networks, cloud and wireless security, then traffic and log monitoring to detect anomalies. Day five turns to incident response and forensic readiness, business continuity and disaster recovery, and anticipating threats through risk assessment, attack surface analysis and threat intelligence, finishing with exam readiness.

Labs give you practical experience configuring and monitoring defences in a lab network. This is independent, exam-aligned training; it does not use EC-Council courseware and Ace Skills Consulting does not claim to be an EC-Council Accredited Training Centre. Exam registration is handled through EC-Council's official channels, so confirm the current version and requirements with EC-Council before booking.

Highlights

- 40 hours of live, defence-focused training
- Protect, detect, respond and predict approach
- Firewall, IDS, endpoint and cloud security labs
- Monitoring and incident response exercises
- Practice questions mapped to the exam areas

What's included

- Layered defence labs in a lab network
- Firewall and IDS configuration exercises
- Endpoint hardening for Windows and Linux
- Log and traffic monitoring with a SIEM
- Incident response and continuity planning
- Practice questions with explanations
- Course completion certificate from Ace Skills Consulting

Who this course is for

Who should attend

- Network administrators and engineers
- Security operations and SOC staff
- System administrators responsible for network security
- IT professionals moving into defensive security

Prerequisites

- Networking fundamentals including TCP/IP and routing
- Familiarity with Windows and Linux administration

Detailed curriculum — 5 days, 40 hours, 14 modules, 7 hands-on labs

Day 1 Attacks, Strategy & Administrative Controls

8 hours

1.1 Network attacks and defence strategies

- Common network attack types
- Protect, detect, respond and predict approach
- Defence-in-depth strategy

1.2 Administrative network security

- Security policies and procedures
- Security awareness
- Regulatory frameworks and compliance

LAB Draft an acceptable use and remote access policy · 30 min

1.3 Physical security

- Physical access controls
- Workplace security
- Environmental controls

Day 2 Technical Network Security & Perimeter Defence

8 hours

2.1 Access control and segmentation

- Authentication and authorisation models
- Network access control
- Network segmentation and VLANs
- VPN technologies

LAB Segment a network and configure a site-to-site VPN · 50 min

2.2 Firewalls and IDS/IPS

- Firewall types and rule design
- Proxy servers and content filtering
- IDS and IPS deployment
- Honeypots

LAB Configure pfSense rules and Snort detection · 60 min

Day 3 Endpoint, Application & Data Security

8 hours

3.1 Endpoint security

- Windows hardening and group policy
- Mobile device management
- Linux hardening
- IoT device security

LAB Harden Windows and Linux endpoints against a baseline · 50 min

3.2 Application security

- Application allow listing
- Secure patch management
- Web application firewalls

3.3 Data security

- Data classification
- Data loss prevention
- Encryption at rest and in transit
- Backup and retention

LAB Encrypt data and configure backups · 30 min

Day 4 Virtual, Cloud & Wireless Security, Monitoring

8 hours

4.1 Virtual and cloud networks

- Virtualisation and container security
- Cloud security controls and shared responsibility
- Software-defined networking

4.2 Wireless security

- Wireless encryption standards
- Rogue access point detection
- Wireless intrusion prevention

4.3 Traffic and log monitoring

- Baselining normal traffic
- Centralised logging and SIEM
- Detecting anomalies with Wireshark
- Alert tuning

LAB Detect suspicious traffic and correlate logs in a SIEM · 60 min

Day 5 Incident Response, Continuity, Threat Prediction & Exam Readiness

8 hours

5.1 Incident response and forensic readiness

- Incident handling process
- Evidence preservation
- Forensic readiness planning

LAB Handle a simulated network intrusion · 45 min

5.2 Business continuity and disaster recovery

- Business impact analysis
- Testing plans
- Continuity and recovery planning

5.3 Anticipating threats and exam readiness

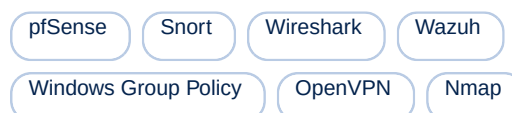
- Risk assessment and management
- Cyber threat intelligence
- Attack surface analysis
- Practice questions and review

Skills and tools

Skills you will build



Tools used in class



Certification exam

This course is aligned to the exam below and prepares you for it. The exam itself is booked and taken with the vendor.

Exam Certified Network Defender (CND)

Exam code	312-38
Format	Multiple choice
Official page	https://www.eccouncil.org/

Exam skill areas covered

Network security and defense strategies with a focus on

Exam details are pending verification. Confirm the current exam code, format and fee on the official vendor page before booking.

Frequently asked questions

How do I register for the CND exam?

You register through EC-Council's official channels, which also set eligibility requirements. We explain the steps, but vouchers and approvals come from EC-Council.

Is this official EC-Council training?

No. This is independent, exam-aligned preparation using our own material and labs.

How does CND compare with CEH?

CND focuses on defending networks, while CEH focuses on attack techniques. Many professionals take CND first, then CEH.

Is the course suitable for network engineers without security experience?

Yes. Networking knowledge is the main prerequisite, and security concepts are introduced from the basics.

Can you train our network operations team?

Yes. Private batches can use your firewall and monitoring platforms as examples.

Book a batch or talk to an advisor

Course page: aceskillsconsulting.com/course/312-38-certified-network-defender-cnd · Email: info@aceskillsconsulting.com

Chennai office

Guindy, Chennai, Tamil Nadu

Delhi office

B-95, Old Post Office Street, Shakarpur
New Delhi 110092
Office: 98180 12523

CEH, CHFI and CND are trademarks of the International Council of E-Commerce Consultants (EC-Council). All product names, logos, brands, trademarks and registered trademarks are the property of their respective owners. Ace Skills Consulting is an independent training provider; unless explicitly stated, it is not affiliated with, endorsed by or sponsored by any vendor mentioned on this site. Exam details are provided for guidance and may change — always confirm on the vendor's official website. Curriculum generated on 23 Oct 2026; topics and order may be adjusted by the trainer to suit each batch.