

EC-COUNCIL

CND — Certified Network Defender Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

INTERMEDIATE

40 HOURS

5 DAYS

At a glance

COURSE	CND — Certified Network Defender
TRACK	EC-Council
DOMAIN	Cyber Security
LEVEL	Intermediate
DURATION	40 hours (about 5 days)
DELIVERY	Classroom · Online live · On-site at your office
LANGUAGE	English
CLASS SIZE	Small cohorts — everyone gets lab time

WHAT IS INCLUDED

- ✓ Instructor-led delivery by practitioners who also work our SOC
- ✓ Hands-on lab access for the duration of the course
- ✓ Course materials and lab guides
- ✓ Hacky Security certificate of completion
- ✓ Post-course support by email

Who this is for

This is a intermediate course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

Twenty modules, mapped one-for-one to the official CND v3 blueprint and taught in the same order, so nothing on the exam is left uncovered.

CND is a defender's course, and v3 is built around four verbs: protect, detect, respond, predict. The first half is about building a network that holds. The second half is about seeing what is happening on it, reacting when something goes wrong, and anticipating the next thing rather than waiting for it. The last three modules — risk, attack surface, threat intelligence — are what separate v3 from the versions that stopped at monitoring.

Unlike CEH v13, CND v3 is not rebuilt around artificial intelligence. AI and machine learning appear where the blueprint places them, chiefly in how modern defensive tooling scores and prioritises what it sees, and we cover them there rather than padding every module with a claim the certification does not make.

Half the classroom time is hands-on. You configure, break and re-harden a working network estate rather than reading about one.

Module 01 — Network Attacks and Defense Strategies

Before you defend a network, you need an accurate picture of what is coming at it.

- Threat, attack and vulnerability terminology used consistently across the course
- Attack categories against networks, hosts, applications and users
- The cyber kill chain and MITRE ATT&CK as defensive planning tools
- Attacker motivations and how they change the controls you prioritise
- Defence-in-depth as a design principle rather than a slogan
- The protect, detect, respond and predict model that structures the rest of the course
- Mapping known attack techniques to the control that would have stopped them
- Building a defence strategy proportionate to the organisation you actually have

Module 02 — Administrative Network Security

The controls that are written down rather than configured.

- Regulatory frameworks, standards and their obligations on network security
- Security policy development, approval and enforcement
- Acceptable use, access control and password policy in practical terms
- Security awareness training and measuring whether it changed behaviour
- Asset inventory and classification as the basis for every other control
- Physical and environmental security requirements
- Vendor, third-party and supply chain security obligations
- Compliance auditing and evidencing that a control is operating

Module 03 — Technical Network Security

Access control and authentication, done properly.

- Access control principles, models and least privilege
- Identity and access management across users, services and devices
- Authentication, authorisation and accounting mechanisms

- Multi-factor authentication and where it genuinely reduces risk
- Network security controls: administrative, physical and technical
- Directory services, single sign-on and federated identity
- Cryptographic controls applied to network security
- Network segmentation and zero trust as an access strategy

Module 04 – Network Perimeter Security

The boundary controls, and their limits.

- Firewall types, architectures and placement decisions
- Firewall rule design, review and removing accumulated exceptions
- Intrusion detection and prevention systems, and tuning them to the estate
- Signature, anomaly and behaviour-based detection approaches
- Router and switch hardening and secure configuration
- Proxy servers, content filtering and egress control
- Honeypots and deception as perimeter instrumentation
- Recognising where the perimeter no longer exists, and what replaces it

Module 05 – Endpoint Security – Windows Systems

Hardening the hosts that carry most of the risk.

- Windows security architecture and its built-in controls
- User account management, privilege separation and local policy
- Group Policy as a hardening mechanism at scale
- Patch and update management, and closing the deployment gap
- Windows Defender, application control and execution restriction
- BitLocker, encryption and protecting data at rest
- Windows auditing, logging and what to collect centrally
- Hardening baselines, benchmarks and verifying drift

Module 06 – Endpoint Security – Linux Systems

The same discipline, different mechanisms.

- Linux security architecture, users, groups and permissions
- File system permissions, special bits and access control lists
- Service hardening and reducing the installed footprint
- Package management, patching and repository trust
- SELinux and AppArmor mandatory access control
- Host firewalling with iptables and nftables
- Linux logging, auditd and remote log shipping
- Hardening baselines and automated configuration verification

Module 07 – Endpoint Security – Mobile Devices

Corporate data on devices you do not fully control.

- Mobile device threats and the enterprise exposure they create

- Mobile operating system security models on Android and iOS
- Enterprise mobility management and Mobile Device Management
- BYOD, COPE and choosing an ownership model deliberately
- Containerisation and separating work data from personal data
- Application vetting, sideloading control and store policy
- Device encryption, remote lock and remote wipe
- Mobile security policy, enrolment and offboarding

Module 08 – Endpoint Security – IoT Devices

The devices nobody assigned an owner to.

- IoT architecture, components and communication models
- IoT-specific threats and why these devices are attractive targets
- Discovering and inventorying IoT devices already on the network
- Default credentials, firmware currency and update mechanisms
- Network segmentation and isolating IoT from production systems
- IoT protocol security and encrypting device communication
- Monitoring IoT devices for anomalous behaviour
- IoT security frameworks and procurement requirements

Module 09 – Administrative Application Security

Controlling what runs, and what it is allowed to do.

- Application-layer threats and the risk they carry into the network
- Application whitelisting, blacklisting and greylisting approaches
- Application sandboxing and isolation
- Patch management for applications rather than just operating systems
- Web application firewalls and their placement
- Secure application configuration and removing defaults
- Application-level access control and privilege management
- Auditing installed applications and enforcing an approved list

Module 10 – Data Security

The thing all the other controls exist to protect.

- Data security controls and the data lifecycle
- Data classification and handling requirements per class
- Encryption of data at rest, in transit and in use
- Disk, file and database encryption mechanisms
- Data masking, tokenisation and minimisation
- Data loss prevention: policy, deployment and tuning
- Backup strategy, retention and tested restoration
- Secure data destruction and disposal of media

Module 11 – Enterprise Virtual Network Security

Virtualisation changed the network, and the controls had to follow.

- Virtualisation concepts, hypervisors and the virtual network stack
- Virtual machine security, isolation and escape risk
- Virtual switch, virtual firewall and virtual network configuration
- Software-defined networking and its security implications
- Network function virtualisation and controller security
- Container and orchestration security fundamentals
- Micro-segmentation within virtualised environments
- Monitoring east-west traffic that never leaves the host

Module 12 – Enterprise Cloud Security

Where the estate is someone else's, but the responsibility is shared.

- Cloud service and deployment models, and the shared responsibility model
- Cloud-specific threats, misconfiguration and identity abuse
- Identity and access management in cloud environments
- Securing cloud storage, compute and network services
- Cloud network controls: security groups, network ACLs and private connectivity
- Encryption and key management in the cloud
- Cloud security posture management and continuous configuration checking
- Cloud logging, monitoring and compliance evidence

Module 13 – Enterprise Wireless Network Security

The network you can attack from the car park.

- Wireless networking concepts, standards and terminology
- Wireless encryption: WEP, WPA, WPA2 and WPA3
- Wireless threats: rogue access points, evil twin, deauthentication, jamming
- Wireless authentication with enterprise mechanisms and RADIUS
- Secure wireless network design, placement and power management
- Guest network isolation and captive portal controls
- Wireless intrusion detection and prevention
- Wireless security policy, audit and periodic site survey

Module 14 – Network Traffic Monitoring and Analysis

Knowing what normal looks like, so abnormal stands out.

- Network traffic monitoring concepts and where to place sensors
- Establishing a traffic baseline for the estate
- Packet capture, flow data and the trade-off between them
- Protocol analysis and dissecting a suspicious conversation
- Detecting scanning, exfiltration and command-and-control patterns
- Bandwidth, performance and capacity signals that indicate a problem
- Monitoring encrypted traffic and what remains observable

- Alerting thresholds and reducing false positives to a workable rate

Module 15 – Network Logs Monitoring and Analysis

Logs are only useful if they are collected, kept and read.

- Logging concepts, log types and sources across the estate
- Configuring logging on Windows, Linux and network devices
- Centralised log collection, transport and secure storage
- Log retention, integrity and tamper resistance
- SIEM deployment, correlation rules and use case design
- Manual and automated log analysis techniques
- Correlating events across sources to reconstruct an incident
- Where machine learning assists log triage, and what it misses

Module 16 – Incident Response and Forensics Investigation

What happens when the controls did not hold.

- Incident response concepts and the phases of a response
- Building an incident response plan and team
- Incident classification, severity and escalation criteria
- Detection, triage and initial containment decisions
- Eradication, recovery and verified return to service
- First responder actions and preserving evidence during response
- Forensic investigation fundamentals and chain of custody
- Post-incident review and feeding findings back into controls

Module 17 – Business Continuity and Disaster Recovery

Staying operational through the thing you could not prevent.

- Business continuity and disaster recovery concepts and the difference between them
- Business impact analysis and identifying critical processes
- Recovery time and recovery point objectives, set realistically
- Business continuity plan development and maintenance
- Disaster recovery site strategies and data replication
- Backup and restoration as a continuity control, not just a data control
- Plan testing, tabletop exercises and full rehearsal
- Standards and frameworks governing continuity planning

Module 18 – Risk Anticipation with Risk Management

Deciding what to fix first, defensibly.

- Risk management concepts, terminology and programme structure
- The risk management lifecycle from identification to monitoring
- Qualitative and quantitative risk assessment approaches
- Building and maintaining a risk register
- Risk treatment: mitigate, transfer, accept, avoid

- Vulnerability management as an input to risk decisions
- Risk management frameworks and standards
- Communicating risk to management in terms they can act on

Module 19 – Threat Assessment with Attack Surface Analysis

Seeing your organisation the way an attacker sees it.

- Attack surface concepts across network, application, human and physical layers
- Identifying and visualising the organisation's attack surface
- Attack surface analysis for systems, applications and cloud services
- Attack simulation and validating exposure rather than assuming it
- Indicators of exposure and prioritising what to close
- Attack surface reduction techniques and measuring the reduction
- Attack surface monitoring as a continuous activity
- Reporting exposure findings so they translate into work

Module 20 – Threat Prediction with Cyber Threat Intelligence

The predict half of the model, and the point of the whole course.

- Cyber threat intelligence concepts and the intelligence lifecycle
- Strategic, tactical, operational and technical intelligence levels
- Intelligence sources, feeds, sharing communities and their reliability
- Threat modelling and applying intelligence to your own estate
- Indicators of compromise, TTPs and the pyramid of pain
- Threat hunting driven by intelligence rather than alerts
- Where AI and machine learning contribute to threat prediction and prioritisation
- Turning intelligence into control changes rather than a reading list

Who should take this

Network administrators and engineers who have inherited the security of what they run, system administrators moving into a defensive security role, SOC analysts who want the network layer properly underneath them, and security officers responsible for network controls they need to assess rather than accept.

You will need working knowledge of TCP/IP, routing and switching, and administration experience on Windows or Linux. Prior security certification is not required.

The exam

- Certified Network Defender, exam code 312-38 – 100 multiple-choice questions, four hours

EC-Council sets the passing mark per exam form rather than at a single fixed figure, so the cut score varies between forms within the range they publish. The exam voucher is purchased separately from the certification body; we arrange it on your behalf and send you the code, and you book your own exam date.

The official blueprint also carries four self-study appendices – computer network fundamentals, physical network security, VPN security, and endpoint security for Mac systems. We cover them in the course materials and flag them as examinable rather than leaving you to find out.

How we deliver it

Five days, classroom or online live, or at your office for a private group. Half the time is hands-on, configuring and defending a live network estate. Small cohorts, so everyone gets lab time rather than watching someone else have it.

Mapped to the official CND v3 blueprint. Taught from Hacky Security's own curriculum and lab estate by instructors who also work our security operations centre.

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

Priced per cohort. Tell us how many people and which delivery mode and we will send a quote the same working day.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 • info@hackysecurity.com

<https://hackysecurity.com/courses/cnd/>

CHANDIGARH • SHIMLA • DELHI • DUBAI • LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 11 September 2026.