# The Credential that Sets the Global Benchmark for Network Security Skills And Builds Careers in Network Security & Blue Team

C|ND Certified Network Defender

EC-Council
Building A Culture Of Security

## C|ND Program Overview

In C|ND students will learn the critical skills required to defend their networks and operating environments across local networks, endpoints, cloud infrastructure, applications, OT, and mobile. They will also acquire knowledge of effective proper log analysis, network traffic monitoring, basic investigation and response, as well as business continuity and disaster recovery. Additionally, they will dive into threats, analyzing the attack surface, and studying threat prediction and threat intelligence as it relates to their administration and defense responsibilities. C|ND's can apply defense and countermeasure strategies in their organizations, playing a critical role in attack prevention, detection, response, and remediation as they configure networks and systems to operate securely. The C|ND program will cover the concepts and fortify skills through hands-on practice across over 100+ labs delivered on live target machines.

## Learn Latest Concepts

- Asset Management
- System Integrity Monitoring
- Endpoint Detection and Response (EDR)
- Extended detection and response (XDR)
- User and Entity Behavior Analytics (UEBA)
- Privacy Impact Assessment (PIA)
- Threat Hunting
- Security Orchestration Automation and Response (SOAR)

## C|ND Key Features

- World's first network security program with continual/adaptive security strategy: **1. Protect 2. Detect 3. Respond 4. Predict**
- Covers defense-in-depth security strategy: **1. Policies, Procedures, and Awareness 2. Physical 3. Perimeter 4. Internal Network 5. Host 6. Application 7. Data**
- Covers four critical security approaches: **1. Preventive Approach 2. Reactive Approach 3. Retrospective Approach 4. Proactive Approach**
- Covers all five functions of the NIST Cybersecurity Framework (CSF): **1. Identify 2. Protect 3. Detect 4. Respond 5. Recover**
- 100+ hands-on labs—the highest number of labs compared to any globally recognized network security certification.
- Accredited by the ANAB (ANSI) ISO/IEC 17024 National Accreditation Board
- Approved by the US Department of Defense (DoD) under Directive 8570/8140

## C|ND Course Outline:

- Network Attacks and Defense Strategies
- Administrative Network Security
- Technical Network Security
- Network Perimeter Security
- Endpoint Security-Windows Systems
- Endpoint Security-Linux Systems
- Endpoint Security- Mobile Devices
- Endpoint Security-IoT Devices
- Administrative Application Security
- Data Security
- Enterprise Virtual Network Security
- Enterprise Cloud Network Security
- Enterprise Wireless Network Security
- Network Traffic Monitoring and Analysis
- Network Logs Monitoring and Analysis
- Incident Response and Forensic Investigation
- Business Continuity and Disaster Recovery
- Risk Anticipation with Risk Management
- Threat Assessment with Attack Surface Analysis
- Threat Prediction with Cyber Threat Intelligence

## Learn Modern Technologies:

- Cloud, IoT, and Virtualization
- Remote Worker Threats
- Attack Surface Analysis
- Threat Intelligence
- Software Defined Networks (SDN)
- Network Function Virtualization (NFV)
- Docker
- Kubernetes
- Container security

## Exam Details:

**Exam Code:** 312-38
**Number of Questions:** 100
**Duration:** 4 hours
**Availability:** EC-Council Exam Portal
**Test Format:** Multiple Choice