



# CNDv2

## Certified Network Defender

Die Schulung „Certified Network Defender“ (CNDv2) ist ein herstellernerutrales, praktisches und umfassendes Netzwerksicherheit-Zertifizierungsprogramm. In diesem übungsintensiven, von einem Dozenten geführten Programm, das auf einer Analyse der Aufgabenanforderungen und Maßnahmen zur Internetsicherheit beruht und von der NICE-Arbeitsgruppe (National Initiative of Cybersecurity Education) vorgestellt wird, erlangen Sie alle Fertigkeiten, die Sie in puncto Cybersicherheit benötigen. Der Kurs ist außerdem auf globale Stellenanforderungen und Zuständigkeiten sowie auf Stellenanforderungen des amerikanischen Verteidigungsministeriums für System-/Netzwerkadministratoren ausgerichtet. Konzeption und Ausarbeitung des Kurses erfolgte anhand umfassender Marktforschungen und Umfragen. Im Rahmen dieses Programms lernen Netzwerkadministratoren Technologien und Vorgänge zur Netzwerksicherheit kennen, die sie auf den Aufbau einer tiefgreifenden Schutzarchitektur für ihre Netzwerke vorbereiten. Dabei wird der Netzwerksicherheitsansatz „Schutz, Erkennung und Reaktion“ behandelt. Der Kurs umfasst praktische Übungen zu den wichtigsten Tools und Techniken zur Netzwerksicherheit. Anhand dieser Übungen erhalten Netzwerkadministratoren praktische Erfahrungen mit aktuellen Netzwerksicherheitstechnologien und -vorgängen. Das über 10 GB umfassende Lernmaterial enthält bewährte Methoden, Bewertungen und Sicherheitstools zum Schutz von Netzwerken. Außerdem beinhaltet das Material Vorlagen für verschiedene Netzwerkrichtlinien sowie zahlreiche Whitepaper.

### Kursinhalt

- Understanding network security management
- Establishing network security policies and procedures
- Windows and Linux security administration
- Setting up mobile and IoT device security
- Implementing data security techniques on networks
- Embedding virtualization technology security
- Determining cloud and wireless security
- Deploying and using risk assessment tools
- Learn basics of first response and forensics
- Understanding indicators of Compromise, Attack, and Exposures (IoC, IoA, IoE)
- Building threat intelligence capabilities
- Establishing and monitoring log management
- Implementing endpoint security
- Configuring optimum firewall solutions
- Understanding and using IDS/IPS technologies
- Establishing Network Authentication, Authorization, Accounting (AAA)

### Zielgruppe

- Netzwerkadministratoren
- Netzwerksicherheitsadministratoren
- Netzwerksicherheitspezialisten
- Netzwerksicherheitstechniker
- CND-Analysten
- Sicherheitsanalysten
- Sicherheitstechniker
- Personen, die mit dem Netzwerkbetrieb zu tun haben

### Prüfung

Wenn Sie den Kurs abgeschlossen und bei EC-Council bewertet haben, erhalten Sie von uns ohne weitere Kosten einen Voucher für die Prüfung „Certified Network Defender 312-38“, die Sie im Nachgang in einem VUE Testcenter ablegen können.

Stand 10.03.2024

### Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: [www.expertech.ch/go/ECCN](http://www.expertech.ch/go/ECCN)

### Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

### Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

### Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

CNDv2

Training		Preise zzgl. MwSt.
<b>Termine in der Schweiz</b>		<b>5 Tage</b>
<b>Online Training</b>		<b>5 Tage CHF 4.395,-</b>
<b>Termin/Kursort</b>		Kurssprache Deutsch
01.07.-05.07.24 <input type="checkbox"/> Online		04.11.-08.11.24 <input type="checkbox"/> Online

EC-Council



EXPERTech



# Inhaltsverzeichnis

## CNDv2 – Certified Network Defender

**Module 01: Network Attacks and Defense Strategies**

**Module 02: Administrative Network Security**

**Module 03: Technical Network Security**

**Module 04: Network Perimeter Security**

**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**

