CNDv3

Course code: CNDv3

In this Certified Network Defender (CND) v3 training course, you will prepare to pass the EC-Council CND exam and learn the tactical skills needed to design and manage a secure network. You will gain a solid understanding of defensive security and hands-on capability to handle all types of network defense. You will learn to ensure data security, properly configure networking technologies and install defensive software to enhance confidentiality, integrity, and availability.EC-Council's Certified Network Defender (CND) training course is a comprehensive program designed to provide IT professionals with the skills and knowledge to effectively protect, detect, and respond to network security threats. The course focuses on the latest tools and techniques for network defense, emphasizing a holistic and proactive approach to securing modern network environments.

Who is the course for

The course is highly suitable for computer network security administrators, system administrators, graduates of ethical hacking courses such as GOC3 – Hacking in Practice and CEH – Certified Ethical Hacker, and anyone seeking effective defense against both ethical and unethical hacking.

What we teach you

In just 5 days, you'll learn about the tools, technologies and techniques needed to defend and strengthen your network against a new age of hackers. You'll also learn valuable skills like how to:

- Establish network security policies and procedures
- Set up mobile and IoT device security
- Determine cloud and wireless security

Required skills

We recommend completing the CompTIA Security+ course beforehand. A solid understanding of operating system administration and knowledge of network protocols at the level of GOC2 and GOC3 courses is a mandatory requirement.

Course outline

- Module 1: Network Attacks and Defense Strategies
- Module 2: Administrative Network Security
- Module 3: Technical Network Security
- Module 4: Network Perimeter Security
- Module 5: Endpoint Security-Windows Systems
- Module 6: Endpoint Security-Linux Devices
- Module 7: Endpoint Security-Mobile Devices
- Module 8: Endpoint Security-IoT Devices
- Module 9: 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

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk