CND - Certified Network Defender Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Learn about hackers and cyber defense strategies required in today's critical infrastructure.

EC-Council's Certified Network Defender (C|ND) is an essential vendor-neutral network security certification for every IT and systems administrator who needs to operate with a secure mindset.

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.

Often referred to as blue-teaming, C|NDs will be able to apply defense and countermeasure strategies in their organizations, playing a critical role not only in attack prevention but also in 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.

The C|ND v3 program designed by industry experts prepares network defenders with strategic, technological, and operational network security capabilities, enabling them to design, develop, and maintain secure networks.

This course includes one exam voucher for the CND - Certified Network Defender exam (312-38).

Who Should Attend?

- System administrators
- System engineers
- Firewall administrators
- Network managers
- IT managers
- IT professionals
- Anyone interested in network security technologies
- Managers who want to understand cyber security core principles and practices
- Operations personnel, who although do not have security as their primary job function, will need an understanding of cyber security core principles and practices

Prerequisites

You should be well-versed in cyber security fundamentals.

CND - Certified Network Defender Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

- Network security management
- Network security policies and procedures
- Windows and Linux security administration
- Mobile and IoT device security
- Data security techniques
- Virtualization technology security
- Cloud and wireless security
- Risk assessment tools
- Basics of first response and forensics
- Indicators of Compromise, Attack, and Exposures (IoC, IoA, IoE)
- Threat intelligence capabilities
- Log management
- Endpoint security
- Firewall solutions
- IDS/IPS technologies
- Network Authentication, Authorization, Accounting (AAA)

Training Outline

1. Network Attacks and Defense Strategies
2. Administrative Network Security
3. Technical Network Security
4. Network Perimeter Security
5. Endpoint Security - Windows Systems
6. Endpoint Security - Linux Systems
7. Endpoint Security - Mobile Devices
8. Endpoint Security - IoT Devices
9. Administrative Application Security
10. Data Security
11. Enterprise Virtual Network Security
12. Enterprise Cloud Network Security
13. Enterprise Wireless Network Security
14. Network Traffic Monitoring and Analysis
15. Network Logs Monitoring and Analysis
16. Incident Response and Forensic Investigation
17. Business Continuity and Disaster Recovery
18. Risk Anticipation with Risk Management
19. Threat Assessment with Attack Surface Analysis
20. Threat Prediction with Cyber Threat Intelligence