EC-Council Certified Network Defender (CND) + Exam voucher

Duration: 5 Days **Course Code: CND** **Version: 3.0** **Delivery Method: Company Event**

Overview:

EC-Council's Certified Network Defender (C|ND) is a comprehensive, vendor-neutral network security certification designed for IT professionals and system administrators who need to operate with a security-focused mindset.

This program equips learners with the essential skills required to protect networks and operating environments across local networks, endpoints, cloud infrastructure, applications, operational technology (OT), and mobile environments. Participants will gain practical knowledge in log analysis, network traffic monitoring, basic investigation and incident response, business continuity, and disaster recovery.

The course also explores modern cybersecurity threats, attack surface analysis, threat prediction, and threat intelligence to strengthen administrative and defensive capabilities. Often referred to as "blue teaming," the C|ND program enables professionals to implement effective defense and countermeasure strategies that support attack prevention, detection, response, and remediation while maintaining secure network and system operations.

Designed by industry experts, the C|ND program combines strategic, technological, and operational security concepts with extensive hands-on practice through more than 100 labs conducted on live target machines. By the end of the course, participants will have the skills needed to design, develop, manage, and maintain secure enterprise networks.

Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

Target Audience:

The following individuals can consider EC-Council's Network Security Certifications as the next move in their career:

- Students/IT Professionals/Other industry professionals planning a career in cybersecurity
- Anyone who wants to start a career in blue team and network security

Objectives:

- **What You Will Learn?**
- Planning and administering network security for organizations
- Recognizing security risks, threats, and vulnerabilities
- Ensuring compliance with regulatory standards
- Designing and implementing network security policies
- Applying security principles in distributed and mobile computing environments
- Implementing Identity and Access Management (IAM), encryption, and network segmentation
- Managing Windows and Linux security administration
- Addressing security risks in mobile devices and IoT environments
- Implementing strong data security techniques
- Managing security in virtualization technologies and cloud platforms
- Managing proxy services, content filtering, and troubleshooting network issues
- Hardening endpoint security and selecting firewall solutions
- Configuring IDS/IPS solutions for enhanced security
- Maintaining an inventory of network devices
- Providing security awareness guidance and training
- Managing AAA (Authentication, Authorization, and Accounting) for network devices
- Reviewing audit logs and analyzing security anomalies
- Maintaining and configuring security platforms
- Evaluating security products and operational procedures
- Identifying and classifying organizational assets
- Implementing system integrity monitoring tools
- Understanding EDR/XDR and UEBA solutions

- Implementing wireless network security
- Conducting risk and vulnerability assessments
- Providing first response to security incidents
- Identifying Indicators of Compromise (IoCs) and attack patterns
- Integrating threat intelligence for proactive defense
- Conducting attack surface analysis
- Assisting in business continuity and disaster recovery planning
- Monitoring network traffic and performing log management
- Conducting Privacy Impact Assessment (PIA) processes
- Collaborating on threat hunting and incident response activities
- Understanding SOAR platforms in cybersecurity operations
- Integrating Zero Trust principles into security architectures
- Staying updated on emerging cyber threats
- Understanding the role of AI and Machine Learning in cyber defense

Prerequisites:

Recommended Prerequisites for the C|ND:

- Basic IT and networking knowledge
- Interest in cybersecurity and blue team operations

Testing and Certification

- **Exam Code:** 312-38
- **Duration:** 4 Hours
- **Availability:** EC-Council Exam Portal
- **Test Format:** Multiple Choice

Content:

Module 1:

- The World's First Network Security Program with a Continual/Adaptive Security Strategy:
- Protect
- Detect
- Respond
- Predict
- Policies, Procedures, and Awareness
- Physical
- Perimeter
- Internal Network
- Host
- Application
- Data
- Preventive Approach
- Reactive Approach
- Retrospective Approach
- Proactive Approach
- Identify
- Protect
- Detect
- Respond
- Recover

Module 2:

Covers Defense-In-Depth Security Strategy:

- Protect
- Detect
- Respond
- Predict
- Policies, Procedures, and Awareness
- Physical
- Perimeter
- Internal Network
- Host
- Application
- Data
- Preventive Approach
- Reactive Approach
- Retrospective Approach
- Proactive Approach
- Identify
- Protect
- Detect
- Respond
- Recover

Module 3:

Covers Four Security Approaches:

- Protect
- Detect
- Respond
- Recover

Module 4:

Covers All Five Functions of the NIST Cybersecurity Framework (CSF):

- Protect
- Detect
- Respond
- Predict
- Policies, Procedures, and Awareness
- Physical
- Perimeter
- Internal Network
- Host
- Application
- Data
- Preventive Approach
- Reactive Approach
- Retrospective Approach
- Proactive Approach
- Identify
- Protect
- Detect
- Respond
- Recover

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/