Certified Network Defender (C|ND) Training Course

Certified Network Defender (C|ND) is a cybersecurity course focused on enhancing skills in network security, threat detection, and defense strategies.

SEC-203

Course Outcomes

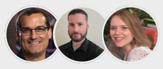
Professional, practical, & hands-on live instructor-led training

Further your skills and graduate as a certified professional, with the skills, experience, and job-search know how to get your career started.

Start Today

Potential Career Tracks

- Network Security Administrator
- Cybersecurity Analyst
- Information Security Manager
- IT Security Specialist
- Security Operations Center (SOC) Analyst
- Network Defense Technician



Taught by Industry Veterans & World Class Instructors

Introduction to Certified Network Defender (C|ND)

Course Overview

The Certified Network Defender (C|ND) Training Course at Intellectual Point is meticulously designed to equip you with the essential skills needed to protect, detect, and respond to network security threats. This course focuses on hands-on training to ensure you understand the critical balance between managing vulnerabilities and implementing robust defenses in a network environment.

By integrating practical experiences with foundational cybersecurity theories, the course prepares you for the C|ND certification exam and real-world network defense scenarios. Throughout the course, you will explore the art of risk management, network policies, security controls, and threat intelligence strategies. By the end of the training, you'll be adept at applying your knowledge to create secure networks and proactively defend against cyber-attacks.

Obtainable Skills

- Intrusion Detection Systems Management
- Risk Assessment and Management
- Network Security Policy Development
- Defensive Firewall Configuration
- Threat Intelligence Analysis
- Incident Response Strategies
- Security Control Implementation
- C|ND Certification Exam Preparation
- Vulnerability Assessment Techniques

Course Insights

Audience Profile

The C|ND Training Course is tailor-made for IT professionals, network administrators, and security enthusiasts eager to deepen their understanding of network defense mechanisms. It is ideal for individuals possessing intermediate experience in networking who wish to transition into security-focused roles or enhance their existing expertise. This course is particularly beneficial for cybersecurity practitioners looking to obtain a well-respected credential and tackle complex network security challenges in industries such as finance, healthcare, and government.

Course Outcomes

By the end of this course, participants will:

1. Develop and implement comprehensive network security strategies to protect organizational assets.
2. Conduct detailed network traffic analysis to identify and mitigate potential threats.
3. Implement robust firewalls and intrusion detection systems to enhance network security posture.
4. Formulate and enforce security policies to ensure compliance and manage risk effectively.
5. Demonstrate preparedness to pass the Certified Network Defender (C|ND) certification exam.

Module by Module Learning *Outline*

6 Modules

Module 1: Introduction to Network Defense

Learning Objectives:

- Understand the foundational principles of network security and defense.
- Learn the importance of securing network infrastructure and assets.

Topics Covered

Basics of Network Security:

- Key concepts in network defense.
- Overview of network threats and vulnerabilities.

Network Defense Tools and Techniques:

- Exploring defensive technologies and solutions.
- Importance of layered security strategies.

Module 2: Managing Network Security Policies

Learning Objectives:

- Develop and implement effective network security policies.
- Understand the role of policies in mitigating network risks.

Topics Covered

Security Policy Framework:

- Components of a strong network security policy.
- Steps to create and enforce security policies.

Risk Management and Compliance:

- Techniques for risk assessment and management.
- Importance of compliance with industry standards.

Module 3: Network Traffic Analysis and Intrusion Detection

Learning Objectives:

- Conduct network traffic analysis to identify anomalies and threats.
- Utilize intrusion detection systems to enhance network security.

Topics Covered

Network Traffic Monitoring:

- Tools and techniques for traffic analysis.
- Identifying unusual patterns and potential intrusions.

Intrusion Detection Systems (IDS):

- Types and functions of IDS.
- Implementing and managing intrusion detection solutions.

Module 4: Implementing Firewalls and Security Controls

Learning Objectives:

- Configure defensive firewalls to protect network infrastructure.
- Apply security controls effectively to minimize security risks.

Topics Covered

Firewall Configuration and Management:

- Setting up and maintaining various types of firewalls.
- Best practices for firewall rules and policies.

Security Control Implementation:

- Types of security controls and their uses.
- Techniques for deploying effective security measures.

Module 5: Threat Intelligence and Incident Response

Learning Objectives:

- Utilize threat intelligence to identify potential network threats.
- Develop and implement incident response strategies.

Topics Covered

Understanding Threat Intelligence:

- Processes for gathering and analyzing threat data.
- Role of threat intelligence in proactive defense.

Incident Response Planning:

- Crafting effective incident response plans.
- Steps to take during a network security incident.

Module 6: Preparing for the C|ND Certification Exam

Learning Objectives:

- Understand the structure and requirements of the C|ND exam.
- Review key topics and skills necessary for certification.

Topics Covered

Exam Preparation Techniques:

- Study strategies and resources for exam success.
- Practice exams and simulations.

Review of Core C|ND Topics:

- Recap of key concepts covered in modules.
- Final tips and advice for exam readiness.