€TRAINING

Certified Network Defender CND

18 - 22 August 2025
Kuala Lumpur (Malaysia)

Certified Network Defender CND

REF: Y2669 DATE: 18 - 22 August 2025 Venue: Kuala Lumpur (Malaysia) - Fee: 5850 Euro

Introduction:

This program is designed to prepare participants for the certification exam only.

Cybersecurity is a critical field in today's interconnected world, where organizations face constant threats to their networks and data. The Certified Network Defender CND program equips participants with advanced skills to protect, detect, and respond to network security threats effectively. This training program provides a comprehensive understanding of network defense strategies, risk mitigation, and practical tools to secure organizational networks.

Program Objectives:

By the end of this program, participants will be able to:

- Explore the fundamentals of network security and defense mechanisms.
- Identify and mitigate network vulnerabilities and threats.
- Implement advanced security measures to protect network infrastructure.
- Conduct regular monitoring, analysis, and threat detection.
- Prepare effectively for the Certified Network Defender CND certification exam.

Targeted Audience:

- Network administrators and engineers.
- IT professionals responsible for cybersecurity.
- Security analysts and incident response teams.
- System administrators and infrastructure managers.
- Professionals preparing for the Certified Network Defender CND certification.

Program Outline:

Unit 1:

Fundamentals of Network Security:

- Overview of network defense principles and frameworks.

- Common network threats and vulnerabilities.
- Importance of network monitoring and threat detection.
- Overview of firewalls, VPNs, and intrusion detection systems.

Unit 2:

Identifying and Mitigating Network Threats:

- How to conduct network vulnerability assessments.
- Tools for recognizing advanced persistent threats and malware.
- Implementing security patches and updates effectively.
- Strategies for defending against denial-of-service DoS attacks.
- Tools for real-time network threat analysis.

Unit 3:

Securing Network Infrastructure:

- Configuring secure network architecture.
- Protecting wireless networks from unauthorized access.
- Implementing encryption and secure communication protocols.
- Managing user access and permissions securely.
- Safeguarding critical systems and endpoints.

Unit 4:

Incident Response and Recovery:

- Methods of developing and implementing incident response plans.
- Analyzing and mitigating security incidents effectively.
- How to conduct forensic investigations on compromised systems.
- Ensuring business continuity through recovery strategies.
- Reporting and documenting incidents for future prevention.

Unit 5:

Certification Exam Preparation:

- Overview of the CND certification exam structure and topics.
- Key areas of focus: network defense, incident response, and threat mitigation.
- Reviewing key topics and concepts covered in the exam.
- Sample exam questions and their potential answers.
- Resources and materials for further study.

Note: This program is designed to prepare participants for the certification exam only.