€TRAINING

Certified Network Defender CND

Certified Network Defender CND

Introduction:

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

This training program is designed to provide comprehensive knowledge and skills required for network security and defense. It equips participants with the tools and expertise needed to effectively safeguard their organization's network environment.

Program Objectives:

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

- Understand key network security principles and concepts.
- Implement effective network monitoring and defense strategies.
- Analyze network traffic to detect and respond to security incidents.
- Manage and mitigate network security threats and vulnerabilities.
- Develop and execute incident response and recovery plans.
- Prepare for the certification exam.

Targeted Audience:

- Network security professionals.
- IT administrators and engineers.
- Security analysts and engineers.
- IT managers and decision-makers.

Program Outline:

Unit 1:

Network Security Fundamentals:

- Understanding network security principles and objectives.
- Overview of network security technologies and tools.

- Types of network attacks and threats.
- Network security policies and best practices.
- Introduction to network defense mechanisms.

Unit 2:

Network Monitoring and Analysis:

- Techniques for network traffic analysis and monitoring.
- Tools and methods for detecting network anomalies.
- Setting up and configuring network monitoring systems.
- Analyzing logs and reports to identify security incidents.
- Exercises for network traffic analysis.

Unit 3:

Network Defense Strategies:

- Implementing firewalls, VPNs, and intrusion prevention systems.
- Approaches for Configuring and managing network security devices.
- Defense-in-depth strategies and layered security approaches.
- Protecting against common network vulnerabilities.
- Deploying and managing network defenses.

Unit 4:

Incident Response and Management:

- Developing an incident response plan and procedures.
- Identifying and classifying security incidents.
- Techniques for managing and mitigating security breaches.
- Steps for Conducting forensic analysis and evidence collection.
- Simulated incident response scenarios and exercises.

Unit 5:

Advanced Network Security Topics:

- Understanding and implementing network segmentation and isolation.
- Managing network security for cloud and virtual environments.
- Advanced threat detection and response techniques.
- Risk assessment and vulnerability management.
- Future trends in network security and emerging threats.
- Prepare for the certification exam.

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