CBRCOR Exam: Performing CyberOps Using Cisco core Security Technologies v1.2

Course Duration: 40 Hours **Course Code: CBRCOR v1.2**

1. Course Overview

The **CBRCOR: Performing CyberOps Using Cisco Core Security Technologies v1.2** course is designed to equip cybersecurity professionals with advanced skills in security concepts, network intrusion analysis, endpoint threat detection, and cybersecurity operations. This training provides in-depth knowledge of how to leverage Cisco's core security technologies to protect and defend organizational IT infrastructure against evolving threats.

2. What You'll Learn?

By the end of this course, you will be able to:

- Understand and implement core cybersecurity concepts and techniques.
- Analyze network traffic and identify potential security threats.
- Configure and monitor Cisco security technologies for threat detection and response.
- Detect, investigate, and respond to endpoint-based threats.
- Apply techniques for incident handling and digital forensics.
- Strengthen the organization's security posture using Cisco's advanced tools and solutions.

3. Target Audience

This course is ideal for:

- Security Operations Center (SOC) analysts.
- Network security engineers.
- Cybersecurity analysts.
- Security administrators and consultants.
- Professionals preparing for the **Cisco CyberOps Professional Certification**.

4. Pre-Requisites

Before taking this course, participants should have:

- A solid understanding of networking fundamentals.
- Familiarity with Cisco security concepts and basic configuration.
- Knowledge equivalent to the **Cisco CCNA** level.
- Experience working with security operations, incident response, or network defense is recommended.

5. Course Content

Module 1: Cybersecurity Fundamentals

- Core security concepts
- Common threats and attack vectors
- Security operations processes

Module 2: Network Intrusion Analysis

- Traffic analysis methodologies
- Identifying anomalies and malicious patterns

- Intrusion detection and prevention

Module 3: Endpoint Threat Detection and Response

- Endpoint protection techniques
- Identifying malware and advanced persistent threats (APTs)
- Forensics and incident investigation

Module 4: Security Monitoring with Cisco Technologies

- Using Cisco Security Solutions (Firepower, Umbrella, SecureX, etc.)
- Configuring and monitoring threat detection tools
- Security event correlation and analysis

Module 5: Incident Handling and Response

- Incident response methodologies
- Containment, eradication, and recovery processes
- Best practices in incident management

Module 6: Advanced CyberOps Techniques

- Automating SOC workflows
- Using playbooks for response
- Advanced threat hunting and digital forensics