CyberSec First Responder Course

Course Duration: 40 Hrs. **Course Code: CFR-210**

Course Overview

The **CyberSec First Responder** course is designed to equip IT and security professionals with the essential skills needed to identify, respond to, and manage cybersecurity incidents effectively. This course focuses on real-world incident response scenarios, threat detection, containment, and recovery techniques. Participants will learn how to act as first responders during cyber incidents, minimizing damage and ensuring business continuity while preparing for industry-recognized cybersecurity response roles.

What You'll Learn?

By completing this course, you will be able to:

- Understand cybersecurity threats and attack vectors
- Detect and analyze security incidents
- Perform incident response and containment actions
- Conduct basic digital forensics and evidence handling
- Implement recovery and post-incident activities
- Communicate effectively during security incidents
- Apply best practices for cyber incident response

Target Audience

This course is ideal for:

- Security Analysts and SOC Analysts
- Network and System Administrators

- IT Support and Operations Professionals
- Incident Response Team Members
- Professionals beginning a career in cybersecurity

Pre-Requisites

Participants should have:

- Basic understanding of networking and operating systems
- Familiarity with IT infrastructure concepts
- Interest in cybersecurity operations
- Prior security knowledge is helpful but not mandatory

Course Content

Module 1: Introduction to Cybersecurity and Incident Response

- Cybersecurity fundamentals
- Types of cyber threats and attacks
- Role of a cyber first responder

Module 2: Threat Detection and Analysis

- Identifying indicators of compromise (IOCs)
- Log analysis and monitoring
- Basic threat intelligence concepts

Module 3: Incident Response Process

- Incident response lifecycle
- Containment, eradication, and recovery
- Incident prioritization and escalation

Module 4: Digital Forensics Basics

- Evidence collection and preservation
- Forensic tools and techniques
- Legal and compliance considerations

Module 5: Recovery and Post-Incident Activities

- System restoration and validation
- Lessons learned and root cause analysis
- Improving security posture

Module 6: Communication, Documentation, and Best Practices

- Incident reporting and documentation
- Stakeholder communication during incidents
- Industry best practices and career guidance