CyberSec First Responder – Advanced (CFR-A) Course

Course Duration: 40 Hrs. **Course Code: CFR-A-310**

Course Overview

The **CyberSec First Responder – Advanced (CFR-A)** course is designed for experienced cybersecurity professionals who are responsible for detecting, responding to, and managing advanced cyber threats. This course builds on foundational incident response knowledge and focuses on advanced threat analysis, incident handling, forensic investigation, and coordinated response strategies. Participants will gain hands-on understanding of managing complex security incidents while preparing for advanced-level cybersecurity response roles.

What You'll Learn?

By completing this course, you will be able to:

- Detect and analyze advanced cyber threats
- Perform advanced incident response and investigation
- Conduct digital forensics and evidence handling
- Respond to malware, ransomware, and APT attacks
- Coordinate response across technical, legal, and business teams
- Improve organizational cyber resilience
- Apply advanced incident response frameworks and best practices

Target Audience

This course is ideal for:

- Cybersecurity Analysts and Engineers

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

- Incident Response and SOC Professionals
- Security Operations Managers
- Digital Forensics and Threat Intelligence Analysts
- Experienced IT and Security Practitioners

Pre-Requisites

Participants should have:

- Prior experience in cybersecurity or incident response
- Understanding of networking, operating systems, and security concepts
- Familiarity with CyberSec First Responder (CFR) or equivalent knowledge

Course Content

Module 1: Advanced Incident Response Concepts

- Review of incident response lifecycle
- Advanced threat landscapes
- Incident classification and escalation

Module 2: Threat Detection and Analysis

- Advanced monitoring and alert analysis
- Threat intelligence integration
- Indicators of compromise (IOCs)

Module 3: Malware and Advanced Attack Techniques

- Ransomware and fileless malware

- Advanced persistent threats (APTs)
- Exploit and lateral movement analysis

Module 4: Digital Forensics and Investigation

- Evidence acquisition and preservation
- Memory, disk, and network forensics
- Forensic tools and methodologies

Module 5: Coordinated Incident Handling and Recovery

- Cross team collaboration during incidents
- Legal, regulatory, and compliance considerations
- Recovery, remediation, and resilience

Module 6: Advanced Response Exercises and Best Practices

- Incident response simulations
- Lessons learned and process improvement
- Best practices and course wrap-up