€TRAINING

Logical Operations CyberSec First Responder CFR

Logical Operations CyberSec First Responder CFR

Introduction:

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

The CyberSec First Responder CFR certification is a recognized credential in the cybersecurity field. It is accredited under the ISO/IEC 17024:2012 standard and validates an individual's ability to identify, assess, respond to, and protect against security threats. This training program focuses on developing expertise in cybersecurity incident handling, forensic analysis, risk assessment, and threat intelligence.

Program Objectives:

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

- Identify and analyze security threats and vulnerabilities.
- Evaluate network defense tools and methodologies.
- Use digital forensics and cyber threat intelligence frameworks.
- Explore security incident handling and response procedures.
- Prepare for the CFR certification exam.

Targeted Audience:

- Cybersecurity analysts and threat intelligence professionals.
- Incident response and security operations center SOC team members.
- Network security engineers and system administrators.
- Risk management and compliance professionals.
- IT professionals preparing for the CFR certification.

Program Outline:

Unit 1:

Cybersecurity Threats and Vulnerability Assessment:

- Overview of cyber threats and attack vectors.

- The process of identifying vulnerabilities in networks, applications, and systems.
- Threat intelligence sources and information gathering techniques.
- Risk assessment methodologies and security policies.
- Evaluating the impact of emerging threats on IT environments.

Unit 2:

Network Defense and Security Operations:

- Network security fundamentals and defense-in-depth strategies.
- Firewalls, intrusion detection, and intrusion prevention systems IDS/IPS.
- SIEM tools and security monitoring measures.
- Secure access controls and authentication mechanisms.
- Incident detection techniques through network traffic and log analysis.

Unit 3:

Digital Forensics and Incident Handling:

- Principles of digital forensics in cybersecurity investigations.
- Methods of collecting and preserving digital evidence.
- Malware analysis and forensic examination techniques.
- Incident handling procedures and security event analysis techniques.
- Legal and regulatory considerations in cybersecurity forensics.

Unit 4:

Incident Response and Risk Mitigation:

- Frameworks for developing structured incident response plans.
- Cybersecurity frameworks and compliance requirements.
- Business continuity and disaster recovery strategies.
- Incident containment and mitigation methodologies.
- The role of security awareness and ongoing risk assessment.

Unit 5:

CFR Certification Exam Preparation:

- Review of CFR exam structure and key domains.
- Reviewing key topics and areas of emphasis in the exam syllabus.
- Sample exam questions and their potential answers.
- Resources and study materials for exam preparation.

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