CyberSec First Responder

Course Duration: 5 Days.

Course overview

CyberSec First Responder (CFR), is a course designed for information assurance professionals who perform job functions related to the development, operation, management, and enforcement of security capabilities for systems and networks.

This course prepares students to take the CyberSec First Responder (Exam CFR-210) certification exam.

Upon Completion

Students will:

- Assess information security risk in computing and network environments.
- Analyze the cybersecurity threat landscape.
- Analyze reconnaissance threats to computing and network environments.
- Analyze attacks on computing and network environments.
- Analyze post-attack techniques on computing and network environments.
- Evaluate the organization's security posture within a risk management framework.
- Collect cybersecurity intelligence.
- Analyze data collected from security and event logs.
- Perform active analysis on assets and networks.
- Respond to cybersecurity incidents.
- Investigate cybersecurity incidents.

Who Should Attend

- Cybersecurity Practitioner
- Cybersecurity Specialist
- Security Operations Center Analyst
- Security Engineer
- IT Directors/IT Management of any kind
- IT Security Specialists of any kind
- Incident Responder
- Information Systems Analyst/Engineer/Manager
- Network Security Analyst/Engineer/Manager
- Network/Security Administrators of any kind
- IT Security Analyst
- Chief Information Officers

Course Content

Lesson 1: Assessing Information Security Risk Topic

- Identify the Importance of Risk Management Topic
- Assess Risk Topic
- Mitigate Risk Topic D: Integrate Documentation into Risk Management

Lesson 2: Analyzing the Threat Landscape Topic

- Classify Threats and Threat Profiles Topic
- Perform Ongoing Threat Research

Lesson 3: Analyzing Reconnaissance Threats to Computing and Network Environments Topic

- Implement Threat Modeling
- Assess the Impact of Reconnaissance Incidents
- Assess the Impact of Social Engineering

Lesson 4: Analyzing Attacks on Computing and Network Environments Topic

- Assess the Impact of System Hacking Attacks
- Assess the Impact of Web-Based Attacks
- Assess the Impact of Malware
- Assess the Impact of Hijacking and Impersonation Attacks
- Assess the Impact of DoS Incidents
- Assess the Impact of Threats to Mobile Security
- Assess the Impact of Threats to Cloud Security.

Lesson 5: Analyzing Post-Attack Techniques

- Assess Command and Control Techniques
- Assess Persistence Techniques
- Assess Lateral Movement and Pivoting Techniques
- Assess Data Exfiltration Techniques
- Assess Anti-Forensics Techniques

Lesson 6: Evaluating the Organization's Security Posture

- Conduct Vulnerability Assessments
- Conduct Penetration Tests on Network Assets
- Follow Up on Penetration Testing

Lesson 7: Collecting Cybersecurity Intelligence

- Deploy a Security Intelligence Collection and Analysis Platform
- Collect Data from Network-Based Intelligence Sources
- Collect Data from Host-Based Intelligence Sources

Lesson 8: Analyzing Log Data

- Use Common Tools to Analyze Logs
- Use SIEM Tools for Analysis
- Parse Log Files with Regular Expressions

Lesson 9: Performing Active Asset and Network Analysis

- Analyze Incidents with Windows-Based Tools
- Analyze Incidents with Linux-Based Tools
- Analyze Malware
- Analyze Indicators of Compromise.

Lesson 10: Responding to Cybersecurity Incidents

- Deploy an Incident Handling and Response Architecture
- Mitigate Incidents
- Prepare for Forensic Investigation as a CSIRT

Lesson 11: Investigating Cybersecurity Incidents

- Apply a Forensic Investigation Plan
- Securely Collect and Analyze Electronic Evidence
- Follow Up on the Results of an Investigation