(CFR) CyberSec First Responder: Threat Detection and Response (Exam CFR-210) (CFR)

Modality: Virtual Classroom

Duration: 5 Days

SATV Value:

CLC:

NATU:

SUBSCRIPTION: No

About this Course:

This intermediate-level training program is designed to help professionals learn the art of identifying cybersecurity threats and responding effectively. The course provides a comprehensive walkthrough of the Cybersecurity Threat Detection & Response System for Security Professionals and Cybersecurity Incident Response Team Members. This course covers the key concepts of Cybersecurity Risks Management, Threat Detection, Cybersecurity Intelligence Collection, Information System Security Assessment & Evaluation, and Response Preparation.

This course trains & prepares candidates for success in the CyberSec First Responder (CFR-210) Certification Exam. In addition to this, professionals involved in Information Assurance, Security Policy Development, and Security Strategies Implementation can greatly benefit from the teachings of this course.

Course Objectives:

The core objective of this course is to help professionals develop a better understanding and sound knowledge of the following key concepts:

- Information Security Risk Evaluation and Response in Networking Ecosystem
- Reconnaissance Attack Identification in Network & Computing Environments
- Assessing the Effectiveness of Risk Management Framework (RMF)
- Cybersecurity Intelligence Collection & Security & Event Log Data Assessment
- Assets & Network Evaluation Techniques for Risk Management
- Cybersecurity Threat & Vulnerabilities Landscape & Incidents Scrutiny
- Effective Incident Management & Threats Mitigation Measures

Audience:

- Cybersecurity Practitioners & Network Security Professionals
- Help Desk Managers & Chief Information Officers
- Professionals liable for Information System Security & Network Protection
- Candidates striving to learn Cybersecurity Threat Management & Detection

Prerequisites:

Professionals planning to enroll in the (CFR) CyberSec First Responder: Threat Detection and Response (Exam CFR-210) (CFR) course must comply with the following prerequisites:

- Fundamental Knowledge of Network Security, Firewalls, VPN, & Intrusion Prevention
- Familiarity with Computing Environments, Operating Systems, & Risk Management
- Minimum 2 years' Experience in Network Security Technology
- Know-how of TCP/IP Networking Protocols such as TCP, DNS, HTTP, IP, & DHCP
- CompTIA® A+®: A Comprehensive Approach is Highly Recommended
- CompTIA® Network+® (Exam N10-006) is Highly Recommended
- CompTIA® Security+® (Exam SY0-401) is Highly Recommended

Course Outline:

Lesson 1: Assessing Information Security Risk

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

Lesson 2: Analyzing the Threat Landscape

- Topic A: Classify Threats and Threat Profiles
- Topic B: Perform Ongoing Threat Research

Lesson 3: Analyzing Reconnaissance Threats to Computing and Network Environments

- Topic A: Implement Threat Modeling
- Topic B: Assess the Impact of Reconnaissance Incidents
- Topic C: Assess the Impact of Social Engineering

Lesson 4: Analyzing Attacks on Computing and Network Environments

- Topic A: Assess the Impact of System Hacking Attacks
- Topic B: Assess the Impact of Web-Based Attacks
- Topic C: Assess the Impact of Malware
- Topic D: Assess the Impact of Hijacking and Impersonation Attacks
- Topic E: Assess the Impact of DoS Incidents
- Topic F: Assess the Impact of Threats to Mobile Security
- Topic G: Assess the Impact of Threats to Cloud Security

Lesson 5: Analyzing Post-Attack Techniques

- Topic A: Assess Command and Control Techniques
- Topic B: Assess Persistence Techniques
- Topic C: Assess Lateral Movement and Pivoting Techniques

- Topic D: Assess Data Exfiltration Techniques
- Topic E: Assess Anti-Forensics Techniques

Lesson 6: Evaluating the Organization?s Security Posture

- Topic A: Conduct Vulnerability Assessments
- Topic B: Conduct Penetration Tests on Network Assets
- Topic C: Follow Up on Penetration Testing

Lesson 7: Collecting Cybersecurity Intelligence

- Topic A: Deploy a Security Intelligence Collection and Analysis Platform
- Topic B: Collect Data from Network-Based Intelligence Sources
- Topic C: Collect Data from Host-Based Intelligence Sources

Lesson 8: Analyzing Log Data

- Topic A: Use Common Tools to Analyze Logs
- Topic B: Use SIEM Tools for Analysis
- Topic C: Parse Log Files with Regular Expressions

Lesson 9: Performing Active Asset and Network Analysis

- Topic A: Analyze Incidents with Windows-Based Tools
- Topic B: Analyze Incidents with Linux-Based Tools
- Topic C: Analyze Malware
- Topic D: Analyze Indicators of Compromise

Lesson 10: Responding to Cybersecurity Incidents

- Topic A: Deploy an Incident Handling and Response Architecture
- Topic B: Mitigate Incidents
- Topic C: Prepare for Forensic Investigation as a CSIRT

Lesson 11: Investigating Cybersecurity Incidents

- Topic A: Apply a Forensic Investigation Plan
- Topic B: Securely Collect and Analyze Electronic Evidence
- Topic C: Follow Up on the Results of an Investigation

Appendix A: Mapping Course Content to CyberSec First Responder (Exam CFR-210)

Appendix B: List of Security Resources

Appendix C: U.S. Department of Defense Operational Security Practices