

## CyberSec First Responder: Threat Detection and Response

**Length:** 5 Days

**Overview:** This course covers the duties of those who are responsible for monitoring and detecting security incidents in information systems and networks, and for executing a proper response to such incidents. Depending on the size of the organization, this individual may act alone or may be a member of a Cybersecurity incident response team (CSIRT). The course introduces tools and tactics to manage Cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyze Cybersecurity intelligence, and handle incidents as they occur. Ultimately, the course promotes a comprehensive approach to security aimed toward those on the front lines of defense.

This course is designed to assist students in preparing for the *CyberSec First Responder (Exam CFR-210)* certification examination. What you learn and practice in this course can be a significant part of your preparation.

**Course Objectives:** In this course, you will assess and respond to security threats and operate a systems and network security analysis platform.

You 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.

### COURSE CONTENT

#### 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

---