

CyberSec First Responder - Threat Detection and Response (Exam CFR-310)

Course 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-310) certification examination. What you learn and practice in this course can be a significant part of your preparation.

Who Should Attend

This course is designed primarily for cybersecurity practitioners who perform job functions related to protecting information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This course focuses on the knowledge, ability, and skills necessary to provide for the defense of those information systems in a cybersecurity context, including protection, detection, analysis, investigation, and response processes. In addition, the course ensures that all members of an IT team—everyone from help desk staff to the Chief Information Officer—understand their role in these security processes.

Course Objectives

This is a 5-day class

Upcoming Dates

Date	Time	Where
10/05/2020	9:00AM - 5:00PM	Online LIVE
10/05/2020	9:00AM - 5:00PM	Online LIVE

[View All Course Dates & Register Today](#)

CyberSec First Responder - Threat Detection and Response (Exam CFR-310)

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

- 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.
- Implement a vulnerability management program.
- Evaluate the organization's security through penetration testing.
- 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 Outline

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

2 Analyzing the Threat Landscape

Topic A: Classify Threats and Threat Profiles

Topic B: Perform Ongoing Threat Research

3 Analyzing Reconnaissance Threats to Computing and Network Environments

Topic A: Implement Threat Modeling

Topic B: Assess the Impact of Reconnaissance

Topic C: Assess the Impact of Social Engineering

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

CyberSec First Responder - Threat Detection and Response (Exam CFR-310)

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

6 Managing Vulnerabilities in the Organization

Topic A: Implement a Vulnerability Management Plan
Topic B: Assess Common Vulnerabilities
Topic C: Conduct Vulnerability Scans

7 Implementing Penetration Testing to Evaluate Security

Topic A: Conduct Penetration Tests on Network Assets
Topic B: Follow Up on Penetration Testing

8 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

9 Analyzing Log Data

Topic A: Use Common Tools to Analyze Logs
Topic B: Use SIEM Tools for Analysis

10 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

11 Responding to Cybersecurity Incidents

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

12 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

13 Appendix A: Mapping Course Content to CyberSec First Responder™ (Exam CFR-310)

14 Appendix B: Regular Expressions

15 Appendix C: Security Resources

16 Appendix D: U.S. Department of Defense Operational Security Practices