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

Course Overview

This is a 5-day class

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.

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

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

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)