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

Course Summary

Description

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.

In addition, this course can help students who are looking to fulfill DoD directive 8570.01 for information assurance (IA) training. This program is designed for personnel performing IA functions, establishing IA policies, and implementing security measures and procedures for the Department of Defense and affiliated information systems and networks.

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.

Audience

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.

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

Course Summary (cont.)

Topics

- Assessing Information Security Risk
- Analyzing the Threat Landscape
- Analyzing Reconnaissance Threats to Computing and Network Environments
- Analyzing Attacks on Computing and Network Environments
- Analyzing Post-Attack Techniques
- Evaluating the Organization’s Security Posture
- Collecting Cybersecurity Intelligence
- Analyzing Log Data
- Performing Active Asset and Network Analysis
- Responding to Cybersecurity Incidents
- Investigating Cybersecurity Incidents
- 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

Prerequisites

To ensure your success in this course, you should have the following requirements:

- At least two years (recommended) of experience in computer network security technology or a related field.
- The ability to recognize information security vulnerabilities and threats in the context of risk management.
- Competency with some of the common operating systems for typical computing environments.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in computing environments. Safeguards include, but are not limited to, basic authentication and authorization, resource permissions, and anti-malware mechanisms.
- Familiarity with some of the common concepts for network environments, such as routing and switching.
- Foundational knowledge of major TCP/IP networking protocols, including, but not limited to, TCP, IP, UDP, DNS, HTTP, ARP, ICMP, and DHCP.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in network environments. Safeguards include, but are not limited to, firewalls, intrusion prevention systems, and virtual private networks (VPNs).

You can obtain this level of skills and knowledge by taking the following Logical Operations courses or by passing the relevant exams:

- *CompTIA® A+®: A Comprehensive Approach (Exams 220-901 and 220-902)*
- *CompTIA® Network+® (Exam N10-006)*
- *CompTIA® Security+® (Exam SY0-401)*

Duration

Five days

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

Course Outline

I. *Assessing Information Security Risk*
   A. Identify the Importance of Risk Management
   B. Assess Risk
   C. Mitigate Risk
   D. Integrate Documentation into Risk Management

II. *Analyzing the Threat Landscape*
   A. Classify Threats and Threat Profiles
   B. Perform Ongoing Threat Research
   C.

III. *Analyzing Reconnaissance Threats to Computing and Network Environments*
   A. Implement Threat Modeling
   B. Assess the Impact of Reconnaissance Incidents
   C. Assess the Impact of Social Engineering

IV. *Analyzing Attacks on Computing and Network Environments*
   A. Assess the Impact of System Hacking Attacks
   B. Assess the Impact of Web-Based Attacks
   C. Assess the Impact of Malware
   D. Assess the Impact of Hijacking and Impersonation Attacks
   E. Assess the Impact of DoS Incidents
   F. Assess the Impact of Threats to Mobile Security
   G. Assess the Impact of Threats to Cloud Security

V. *Analyzing Post-Attack Techniques*
   A. Assess Command and Control Techniques
   B. Assess Persistence Techniques
   C. Assess Lateral Movement and Pivoting Techniques
   D. Assess Data Exfiltration Techniques
   E. Assess Anti-Forensics Techniques

VI. *Evaluating the Organization's Security Posture*
   A. Conduct Vulnerability Assessments
   B. Conduct Penetration Tests on Network Assets
   C. Follow Up on Penetration Testing

VII. *Collecting Cybersecurity Intelligence*
   A. Deploy a Security Intelligence Collection and Analysis Platform
   B. Collect Data from Network-Based Intelligence Sources
   C. Collect Data from Host-Based Intelligence Sources

VIII. *Analyzing Log Data*
   A. Use Common Tools to Analyze Logs
   B. Use SIEM Tools for Analysis
   C. Parse Log Files with Regular Expressions

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

Course Outline (cont.)

IX. *Performing Active Asset and Network Analysis*

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

X. *Responding to Cybersecurity Incidents*

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

XI. *Investigating Cybersecurity Incidents*

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

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

XIII. Appendix B: List of Security Resources

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