virtual instructor-led training

CyberSec First Responder (CFR)

churchillsquareconsulting.virtualinstructorledtraining.com/courses/cybersec-first-responder-cfr/

Introduction:

This course covers network defense and incident response methods, tactics, and procedures that are in alignment with industry frameworks such as NIST 800-61r2 (Computer Security Incident Handling Guide), US-CERT's National Cyber Incident Response Plan (NCIRP), and Presidential Policy Directive (PPD)-41 on Cyber Incident Coordination, NIST 800.171r2 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations). It is ideal for candidates who have been tasked with the responsibility of monitoring and detecting security incidents in information systems and networks, and for executing standardized responses to such incidents. The course introduces tools, tactics, and procedures to manage cybersecurity risks, defend cybersecurity assets, identify various types of common threats, evaluate the organization's security, collect and analyze cybersecurity intelligence, and remediate and report incidents as they occur. This course provides a comprehensive methodology for individuals responsible for defending the cybersecurity of their organization.

This course is designed to assist students in preparing for the CertNexus CyberSec First Responder (Exam CFR-410) certification examination. What you learn and practice in this course can be a significant part of your preparation.

Purchase of this course includes the associated exam voucher.

Objectives:

In this course, you will assess and respond to security threats and operate a systems and network security analysis platform.
Assess cybersecurity risks to the organization.
Analyze the threat landscape.
Analyze various reconnaissance threats to computing and network environments.
Analyze various attacks on computing and network environments.
Analyze various post-attack techniques.
Assess the organization's security posture through auditing, vulnerability management, and penetration testing.
Collect cybersecurity intelligence from various network-based and host-based sources

Analyze log data to reveal evidence of threats and incidents.
Perform active asset and network analysis to detect incidents.
Respond to cybersecurity incidents using containment, mitigation, and recovery tactics.
Investigate cybersecurity incidents using forensic analysis techniques

Course Outline:

1 – Assessing Cybersecurity 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: Analyze Trends Affecting Security Posture

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

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 – Assessing the Organization’s Security Posture

- Topic A: Implement Cybersecurity Auditing
- Topic B: Implement a Vulnerability Management Plan
- Topic C: Assess Vulnerabilities

- Topic D: Conduct Penetration Testing

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

8 – Analyzing Log Data

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

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 Indicators of Compromise

10 – Responding to Cybersecurity Incidents

- Topic A: Deploy an Incident Handling and Response Architecture
- Topic B: Mitigate Incidents
- Topic C: Hand Over Incident Information to a Forensic Investigation

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

Enroll in this course

£3,495.00

Select a start date for your 5 Days course

- 2023-02-13 09:00:00_2023-02-17 17:00:00

- 2023-05-22 09:00:00_2023-05-26 17:00:00