uCertify

Cybersec First Responder (CFR-410)

Lesson

Practice test

Live-Lab

05 Sep 2023

8. 1 About This Course
   2 Assessing Cybersecurity Risk
   3 Analyzing the Threat Landscape
   4 Analyzing Reconnaissance Threats to Computing and Network Environments
   5 Analyzing Attacks on Computing and Network Environments
   6 Analyzing Post-Attack Techniques
   7 Assessing the Organization's Security Posture
   8 Collecting Cybersecurity Intelligence
   9 Analyzing Log Data
   10 Performing Active Asset and Network Analysis
   11 Responding to Cybersecurity Incidents
   12 Investigating Cybersecurity Incidents
   13 Appendix A: Regular Expressions

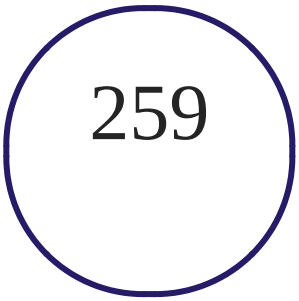
10.

1

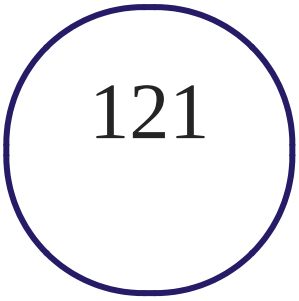
The course Cybersec First Responder (CFR-410) is designed to assist students in preparing for the CertNexus CyberSec First Responder (Exam CFR-410) certification examination. This course is designed primarily for cybersecurity practitioners preparing for or who currently perform job functions related 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.

2

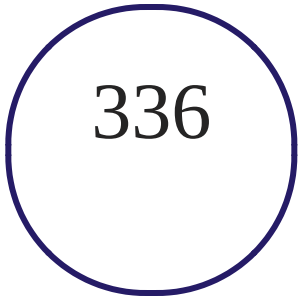
3



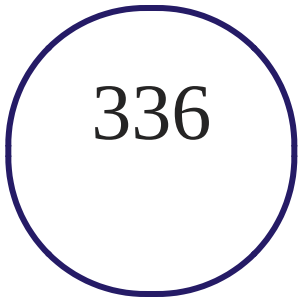
4



5



6



7

8

9

•

10

- **2014**
  1.
- **2015**
  5.
- **2016**
  5.
- **2017**
  3.
- **2018**
  3.
- **2019**
  3.
- **2020**
  3.

11

1: About This Course

- Course Description

2: 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

3: Analyzing the Threat Landscape

- Topic A: Classify Threats
- Topic B: Analyze Trends Affecting Security Posture

4: 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

5: 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

6: 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

7: 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

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 Indicators of Compromise

11: 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

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: Regular Expressions

- Topic A: Parse Log Files with Regular Expressions

12

50	1	100
PRE-ASSESSMENTS QUESTIONS	FULL LENGTH TESTS	POST-ASSESSMENTS QUESTIONS

13 Live Labs

-

Analyzing Reconnaissance Threats to Computing and Network Environments

- Exploiting a Website Using SQL Injection
- Conducting Vulnerability Scanning Using Nessus
- Performing Vulnerability Scanning Using OpenVAS
- Scanning the Local Network
- Getting TCP Settings
- Getting UDP Settings
- Displaying Metadata Information
- Using the tracert Command
- Getting Information about the Current Connection Statistics of UDP
- Getting Information about the Current Connection Statistics of TCP
- Getting Information about TCP Ports
- Getting Information about UDP Ports
- Finding the MAC Address of a System

Analyzing Attacks on Computing and Network Environments

- Using TCPdump
- Capturing Packets Using Wireshark
- Analyzing Traffic Captured from Site Survey Software (kismet)
- Exploiting LDAP-Based Authentication
- Using OWASP ZAP
- Using a Numeric IP Address to Locate a Web Server
- Using NetWitness Investigator
- Performing a Memory-Based Attack
- Using the hping Program
- Confirming the Spoofing Attack in Wireshark
- Performing Session Hijacking Using Burp Suite
- Getting Information about DNS

Analyzing Post-Attack Techniques

- Using the Event Viewer
- Using the dd Utility
- Using Global Regular Expressions Print (grep)
- Enabling the peek performance option

Assessing the Organization's Security Posture

- Obtaining IP Route Information from the IP Routing Table
- Using MBSA

Collecting Cybersecurity Intelligence

- Obtaining the IP version supported by a network adapter
- Obtaining Information about Different IP versions
- Obtaining Information about the Net Firewall Profile

Analyzing Log Data

- Analyzing Linux Logs for Security Intelligence

Performing Active Asset and Network Analysis

- Using FTK Imager
- Exploring Windows File Registry
- Using the Disk Defragmenter Microsoft Drive Optimizer
- Using a Hex Editor

Investigating Cybersecurity Incidents

- Converting a FAT32 Partition to NTFS Using Disk Management
- Converting an NTFS Partition to FAT32 Using Disk Management
- Converting the FAT32 Partition to NTFS Using cmd

42

LIVE LABS

14

support@ucertify.com