uCertify

Course Outline

Cybersec First Responder (CFR-410)

04 May 2024

1. Course Objective
2. Pre-Assessment
3. Exercises, Quizzes, Flashcards & Glossary

   Number of Questions
4. Expert Instructor-Led Training
5. ADA Compliant & JAWS Compatible Platform
6. State of the Art Educator Tools
7. Award Winning Learning Platform (LMS)
8. Chapter & Lessons

   Syllabus

   Chapter 1: About This Course

   Chapter 2: Assessing Cybersecurity Risk

   Chapter 3: Analyzing the Threat Landscape

   Chapter 4: Analyzing Reconnaissance Threats to Computing and Network Environments

   Chapter 5: Analyzing Attacks on Computing and Network Environments

   Chapter 6: Analyzing Post-Attack Techniques

   Chapter 7: Assessing the Organization's Security Posture

   Chapter 8: Collecting Cybersecurity Intelligence

   Chapter 9: Analyzing Log Data

   Chapter 10: Performing Active Asset and Network Analysis

   Chapter 11: Responding to Cybersecurity Incidents

   Chapter 12: Investigating Cybersecurity Incidents

   Chapter 13: Appendix A: Regular Expressions

   Videos and How To
9. Practice Test

   Here's what you get

   Features
10. Live labs

Lab Tasks

Here's what you get

11. Post-Assessment

1. Course Objective

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. Pre-Assessment

Pre-Assessment lets you identify the areas for improvement before you start your prep. It determines what students know about a topic before it is taught and identifies areas for improvement with question assessment before beginning the course.

3. Exercises

There is no limit to the number of times learners can attempt these. Exercises come with detailed remediation, which ensures that learners are confident on the topic before proceeding.

4. Quizzes

Quizzes test your knowledge on the topics of the exam when you go through the course material. There is no limit to the number of times you can attempt it.

5. flashcards

Flashcards are effective memory-aiding tools that help you learn complex topics easily. The flashcard will help you in memorizing definitions, terminologies, key concepts, and more. There is no limit to the number of times learners can attempt these. Flashcards help master the key concepts.

6. Glossary of terms

uCertify provides detailed explanations of concepts relevant to the course through Glossary. It contains a list of frequently used terminologies along with its detailed explanation. Glossary defines the key terms.

7. Expert Instructor-Led Training

uCertify uses the content from the finest publishers and only the IT industry's finest instructors. They have a minimum of 15 years real-world experience and are subject matter experts in their fields. Unlike a live class, you can study at your own pace. This creates a personal learning experience and gives you all the benefit of hands-on training with the flexibility of doing it around your schedule 24/7.

8. ADA Compliant & JAWS Compatible Platform

uCertify course and labs are ADA (Americans with Disability Act) compliant. It is now more accessible to students with features such as:

- Change the font, size, and color of the content of the course
- Text-to-speech, reads the text into spoken words
- Interactive videos, how-tos videos come with transcripts and voice-over
- Interactive transcripts, each word is clickable. Students can clip a specific part of the video by clicking on a word or a portion of the text.

JAWS (Job Access with Speech) is a computer screen reader program for Microsoft Windows that reads the screen either with a text-to-speech output or by a Refreshable Braille display. Student can easily navigate uCertify course using JAWS shortcut keys.

9. State of the Art Educator Tools

uCertify knows the importance of instructors and provide tools to help them do their job effectively. Instructors are able to clone and customize course. Do ability grouping. Create sections. Design grade scale and grade formula. Create and schedule assessments. Educators can also move a student from self-paced to mentor-guided to instructor-led mode in three clicks.

10. Award Winning Learning Platform (LMS)

uCertify has developed an award winning, highly interactive yet simple to use platform. The SIIA CODiE Awards is the only peer-reviewed program to showcase business and education technology's finest products and services. Since 1986, thousands of products, services and solutions have been

recognized for achieving excellence. uCertify has won CODiE awards consecutively for last 7 years:

- **2014**
    1. Best Postsecondary Learning Solution

- **2015**
    1. Best Education Solution
    2. Best Virtual Learning Solution
    3. Best Student Assessment Solution
    4. Best Postsecondary Learning Solution
    5. Best Career and Workforce Readiness Solution
    6. Best Instructional Solution in Other Curriculum Areas
    7. Best Corporate Learning/Workforce Development Solution

- **2016**
    1. Best Virtual Learning Solution
    2. Best Education Cloud-based Solution
    3. Best College and Career Readiness Solution
    4. Best Corporate / Workforce Learning Solution
    5. Best Postsecondary Learning Content Solution
    6. Best Postsecondary LMS or Learning Platform
    7. Best Learning Relationship Management Solution

- **2017**
    1. Best Overall Education Solution
    2. Best Student Assessment Solution
    3. Best Corporate/Workforce Learning Solution
    4. Best Higher Education LMS or Learning Platform

- **2018**
    1. Best Higher Education LMS or Learning Platform

2. Best Instructional Solution in Other Curriculum Areas
3. Best Learning Relationship Management Solution

- **2019**
  1. Best Virtual Learning Solution
  2. Best Content Authoring Development or Curation Solution
  3. Best Higher Education Learning Management Solution (LMS)

- **2020**
  1. Best College and Career Readiness Solution
  2. Best Cross-Curricular Solution
  3. Best Virtual Learning Solution

11. Chapter & Lessons

uCertify brings these textbooks to life. It is full of interactive activities that keeps the learner engaged. uCertify brings all available learning resources for a topic in one place so that the learner can efficiently learn without going to multiple places. Challenge questions are also embedded in the chapters so learners can attempt those while they are learning about that particular topic. This helps them grasp the concepts better because they can go over it again right away which improves learning.

Learners can do Flashcards, Exercises, Quizzes and Labs related to each chapter. At the end of every lesson, uCertify courses guide the learners on the path they should follow.

Syllabus

Chapter 1: About This Course

- Course Description

Chapter 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

Chapter 3: Analyzing the Threat Landscape

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

Chapter 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

Chapter 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

Chapter 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

Chapter 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

Chapter 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

Chapter 9: Analyzing Log Data

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

Chapter 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

Chapter 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

Chapter 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

Chapter 13: Appendix A: Regular Expressions

- Topic A: Parse Log Files with Regular Expressions

12. Practice Test

Here's what you get

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

Features

Each question comes with detailed remediation explaining not only why an answer option is correct but also why it is incorrect.

Unlimited Practice

Each test can be taken unlimited number of times until the learner feels they are prepared. Learner can review the test and read detailed remediation. Detailed test history is also available.

Each test set comes with learn, test and review modes. In learn mode, learners will attempt a question and will get immediate feedback and complete remediation as they move on to the next question. In

test mode, learners can take a timed test simulating the actual exam conditions. In review mode, learners can read through one item at a time without attempting it.

13. Live Labs

The benefits of live-labs are:

- Exam based practical tasks
- Real equipment, absolutely no simulations
- Access to the latest industry technologies
- Available anytime, anywhere on any device
- Break and Reset functionality
- No hardware costs

Lab Tasks

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

Here's what you get

42	42	01:04
LIVE LABS	VIDEO TUTORIALS	HOURS

14. Post-Assessment

After completion of the uCertify course Post-Assessments are given to students and often used in conjunction with a Pre-Assessment to measure their achievement and the effectiveness of the exam.

GET IN TOUCH: