uCertify

Course Outline

CompTIA Cybersecurity Analyst (CySA+)



23 Mar 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: Assessing Information Security Risk

   Chapter 2: Analyzing the Threat Landscape

   Chapter 3: Analyzing Reconnaissance Threats to Computing and Network Environments

   Chapter 4: Analyzing Attacks on Computing and Network Environments

   Chapter 5: Analyzing Post-Attack Techniques

   Chapter 6: Managing Vulnerabilities in the Organization

   Chapter 7: Implementing Penetration Testing to Evaluate Security

   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: Addressing Security Architecture Issues

   Chapter 14: Appendix A: Mapping Course Content to CyberSec First Responder (Exam CFR-210)

   Chapter 15: Appendix B: Mapping Course Content to CompTIA® CyberSecurity Analyst+ (Exam CS0-001)

   Chapter 16: Appendix C: Security Resources

   Chapter 17: Appendix D: U.S. Department of Defense Operational Security

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

We have a course on the latest CySA+ exam, please check out the latest **CompTIA Cybersecurity Analyst (CySA+)** course!

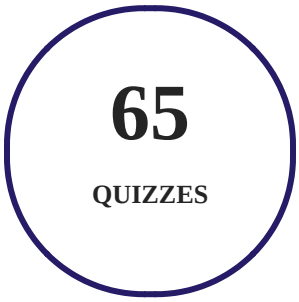
Gain the skills required to pass the CompTIA CySA certification exam with the CompTIA Cybersecurity Analyst (CySA+) course and lab. The lab simulates real-world, hardware, software, and command-line interface environments and can be mapped to any text-book, course or training. The CySA+ study guide focuses on all the objectives of the CS0-001 exam and is designed for IT security analysts, vulnerability analysts, or threat intelligence analysts to configure and use threat detection tools, and perform data analysis.

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. 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.



4. 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.



5. 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.



6. 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.

7. 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.

8. 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.

9. 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

10. 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: 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
- Summary

Chapter 2: Analyzing the Threat Landscape

- TOPIC A: Classify Threats and Threat Profiles

- TOPIC B: Perform Ongoing Threat Research
- Summary

Chapter 3: Analyzing Reconnaissance Threats to Computing and Network Environments

- TOPIC A: Implement Threat Modeling
- TOPIC B: Assess the Impact of Reconnaissance Incidents
- TOPIC C: Assess the Impact of Social Engineering
- Summary

Chapter 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
- Summary

Chapter 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
- Summary

Chapter 6: Managing Vulnerabilities in the Organization

- TOPIC A: Implement a Vulnerability Management Plan
- TOPIC B: Assess Common Vulnerabilities
- TOPIC C: Conduct Vulnerability Scans
- Summary

Chapter 7: Implementing Penetration Testing to Evaluate Security

- TOPIC A: Conduct Penetration Tests on Network Assets
- TOPIC B: Follow Up on Penetration Testing
- Summary

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
- Summary

Chapter 9: Analyzing Log Data

- TOPIC A: Use Common Tools to Analyze Logs
- TOPIC B: Use SIEM Tools for Analysis
- TOPIC C: Parse Log Files with Regular Expressions
- Summary

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 Malware
- TOPIC D: Analyze Indicators of Compromise
- Summary

Chapter 11: Responding to Cybersecurity Incidents

- TOPIC A: Deploy an Incident Handling and Response Architecture
- TOPIC B: Mitigate Incidents
- TOPIC C: Prepare for Forensic Investigation as a CSIRT
- Summary

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
- Summary

Chapter 13: Addressing Security Architecture Issues

- TOPIC A: Remediate Identity and Access Management Issues
- TOPIC B: Implement Security During the SDLC
- Summary

Chapter 14: Appendix A: Mapping Course Content to CyberSec First Responder (Exam CFR-210)

Chapter 15: Appendix B: Mapping Course Content to CompTIA® CyberSecurity Analyst+ (Exam CS0-001)

Chapter 16: Appendix C: Security Resources

- TOPIC A: List of Security Resources

Chapter 17: Appendix D: U.S. Department of Defense Operational Security

- TOPIC A: Summary of U.S. Department of Defense Operational Security Practices

11. Practice Test

Here's what you get

36	2	75
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.

12. 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

Assessing Information Security Risk

- Adding Revision to the Revision History
- Viewing and Downloading the Policy Templates
- Opening the Policy Template and Setting the Company Name
- Reviewing and Modifying the Policy Items

Analyzing the Threat Landscape

- Identifying the most significant emerging technologies of 2016

- Consulting a Vulnerability Database
- Finding information security blogs

Analyzing Reconnaissance Threats to Computing and Network Environments

- Performing Reconnaissance on a Network
- Downloading and Installing Wireshark and WinPcap
- Working with Wireshark's Interface
- Analyzing the Capture File to Find the Attack(s)
- Generating Network Traffic and Using Filters
- Examining the traffic between client and server
- Assessing the impact of malware

Analyzing Attacks on Computing and Network Environments

- Confirming the Spoofing Attack in Wireshark
- Identifying security apps available for Android
- Examining the DDOS_Attack.pcap File

Analyzing Post-Attack Techniques

- Scanning the Rootkit

Managing Vulnerabilities in the Organization

- Conducting Vulnerability Scans

Implementing Penetration Testing to Evaluate Security

- Identifying Search Options in Metasploit
- Performing the Initial Scan

Collecting Cybersecurity Intelligence

- Collecting network-based security intelligence
- Exporting your Windows logs

Analyzing Log Data

- Making Syslog Entries Readable
- Installing Splunk on the Server

Performing Active Asset and Network Analysis

- Manipulating Kali Linux VM's network interfaces
- Retrieving a Real-Time List of Running Processes
- Starting a Live Packet Capture
- Examining the ipconfig options and creating the activity log
- Initiating an SSH Session from your Windows 10 Client to your Windows Server
- Using the Process Explorer to View Specific Details About Running Processes on the System
- Acquiring the Trojan horse simulator
- Accessing remotely the DT_Watch folder to generate audit logs
- Uploading the Trojan horse simulator to VirusTotal
- Uploading the Trojan horse simulator to Malware
- Identifying a suspicious account on the System User Groups
- Enabling auditing of the DT_Watch folder
- Examining the Audited Events
- Enabling logging for audited objects

Addressing Security Architecture Issues

- Inspecting the Vulnerability in the echo Server's Source Code

Here's what you get

40

LIVE LABS

13. 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:

3187 Independence Drive
Livermore, CA 94551,
United States

+1-415-763-6300

support@ucertify.com

www.ucertify.com