uCertify

Course Outline

CompTIA Cybersecurity Analyst (CySA+)

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: Introduction

   Chapter 2: Defending Against Cybersecurity Threats

   Chapter 3: Reconnaissance and Intelligence Gathering

   Chapter 4: Designing a Vulnerability Management Program

   Chapter 5: Analyzing Vulnerability Scans

   Chapter 6: Building an Incident Response Program

   Chapter 7: Analyzing Symptoms for Incident Response

   Chapter 8: Performing Forensic Analysis

   Chapter 9: Recovery and Post-Incident Response

   Chapter 10: Policy and Compliance

   Chapter 11: Defense-in-Depth Security Architectures

   Chapter 12: Identity and Access Management Security

   Chapter 13: Software Development Security

   Chapter 14: Cybersecurity Toolkit

   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 an updated version of this course, please check out the latest **CompTIA Cybersecurity Analyst (CySA+)** course!

Kick start your prep for the CySA+ 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 provides complete coverage of the CS0-001 exam objectives and includes topics such as policy and compliance; forensic analysis, vulnerability scans, identity and access management security; and many more. This CySA+ training is for IT security analysts, vulnerability analysts, or threat intelligence analysts.

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

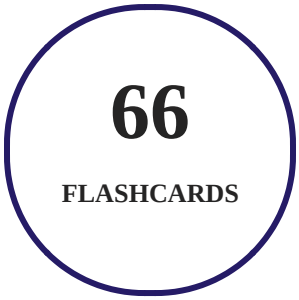
Quizzes test your knowledge on the topics of the exam when you go through the course material. There is no limit to the number of times you can attempt it.

380

QUIZZES

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: Introduction

- What Does This Book Cover?
- Setting Up a Kali and Metasploitable Learning Environment
- Setting Up Your Environment
- Objectives Map for CompTIA Cybersecurity Analyst (CySA+) Exam CS0-001

Chapter 2: Defending Against Cybersecurity Threats

- Cybersecurity Objectives
- Evaluating Security Risks

- Building a Secure Network
- Secure Endpoint Management
- Penetration Testing
- Reverse Engineering
- Summary
- Exam Essentials
- Lab Exercises

Chapter 3: Reconnaissance and Intelligence Gathering

- Footprinting
- Passive Footprinting
- Gathering Organizational Intelligence
- Detecting, Preventing, and Responding to Reconnaissance
- Summary
- Exam Essentials
- Lab Exercises

Chapter 4: Designing a Vulnerability Management Program

- Identifying Vulnerability Management Requirements
- Configuring and Executing Vulnerability Scans
- Developing a Remediation Workflow
- Overcoming Barriers to Vulnerability Scanning
- Summary
- Exam Essentials
- Lab Exercises

Chapter 5: Analyzing Vulnerability Scans

- Reviewing and Interpreting Scan Reports
- Validating Scan Results
- Common Vulnerabilities
- Summary
- Exam Essentials
- Lab Exercises

Chapter 6: Building an Incident Response Program

- Security Incidents
- Phases of Incident Response

- Building the Foundation for Incident Response
- Creating an Incident Response Team
- Coordination and Information Sharing
- Classifying Incidents
- Summary
- Exam Essentials
- Lab Exercises

Chapter 7: Analyzing Symptoms for Incident Response

- Analyzing Network Events
- Handling Network Probes and Attacks
- Investigating Host Issues
- Investigating Service and Application Issues
- Summary
- Exam Essentials
- Lab Exercises

Chapter 8: Performing Forensic Analysis

- Building a Forensics Capability
- Understanding Forensic Software
- Conducting a Forensic Investigation
- Forensic Investigation: An Example
- Summary
- Exam Essentials
- Lab Exercises

Chapter 9: Recovery and Post-Incident Response

- Containing the Damage
- Incident Eradication and Recovery
- Wrapping Up the Response
- Summary
- Exam Essentials
- Lab Exercises

Chapter 10: Policy and Compliance

- Understanding Policy Documents
- Complying with Laws and Regulations

- Adopting a Standard Framework
- Implementing Policy-Based Controls
- Security Control Verification and Quality Control
- Summary
- Exam Essentials
- Lab Exercises

Chapter 11: Defense-in-Depth Security Architectures

- Understanding Defense in Depth
- Implementing Defense in Depth
- Analyzing Security Architecture
- Summary
- Exam Essentials
- Lab Exercises

Chapter 12: Identity and Access Management Security

- Understanding Identity
- Threats to Identity and Access

- Identity as a Security Layer
- Understanding Federated Identity and Single Sign-On
- Summary
- Exam Essentials
- Lab Exercises

Chapter 13: Software Development Security

- Understanding the Software Development Life Cycle
- Designing and Coding for Security
- Software Security Testing
- Summary
- Exam Essentials
- Lab Exercises

Chapter 14: Cybersecurity Toolkit

- Host Security Tools
- Monitoring and Analysis Tools
- Scanning and Testing Tools

- Network Security Tools
- Web Application Security Tools
- Forensics Tools
- Summary

Videos and How To

uCertify course includes videos to help understand concepts. It also includes How Tos that help learners in accomplishing certain tasks.

48	13:09
VIDEOS	HOURS

11. Practice Test

Here's what you get

85	4	85
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

Reconnaissance and Intelligence Gathering

- Performing Reconnaissance on a Network
- Identifying Search Options in Metasploit
- Performing the Initial Scan
- Initiating an SSH Session from your Windows 10 Client to your Windows Server

Designing a Vulnerability Management Program

- Conducting Vulnerability Scans

Analyzing Vulnerability Scans

- Consulting a Vulnerability Database

Analyzing Symptoms for Incident Response

- Examining the DDOS_Attack.pcap File
- Retrieving a Real-Time List of Running Processes
- Examining the Audited Events

Policy and Compliance

- 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

Software Development Security

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

Cybersecurity Toolkit

- Using the Process Explorer to View Specific Details About Running Processes on the System
- Making Syslog Entries Readable
- Installing Splunk on the Server
- Scanning the Rootkit
- Working with Wireshark's Interface
- Analyzing the Capture File to Find the Attack(s)
- Generating Network Traffic and Using Filters
- Confirming the Spoofing Attack in Wireshark
- Starting a Live Packet Capture

Here's what you get

23	23	02
LIVE LABS	VIDEO TUTORIALS	MINUTES

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.