uCertify

Course Outline

CompTIA CySA+ (CS0-002)

08 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: The Importance of Threat Data and Intelligence

   Chapter 3: Utilizing Threat Intelligence to Support Organizational Security

   Chapter 4: Vulnerability Management Activities

   Chapter 5: Analyzing Assessment Output

   Chapter 6: Threats and Vulnerabilities Associated with Specialized Technology

   Chapter 7: Threats and Vulnerabilities Associated with Operating in the Cloud

   Chapter 8: Implementing Controls to Mitigate Attacks and Software Vulnerabilities

   Chapter 9: Security Solutions for Infrastructure Management

   Chapter 10: Software Assurance Best Practices

   Chapter 11: Hardware Assurance Best Practices

   Chapter 12: Analyzing Data as Part of Security Monitoring Activities

   Chapter 13: Implementing Configuration Changes to Existing Controls to Improve Security

   Chapter 14: The Importance of Proactive Threat Hunting

   Chapter 15: Automation Concepts and Technologies

   Chapter 16: The Incident Response Process

   Chapter 17: Applying the Appropriate Incident Response Procedure

   Chapter 18: Analyzing Potential Indicators of Compromise

Chapter 19: Utilizing Basic Digital Forensics Techniques

Chapter 20: The Importance of Data Privacy and Protection

Chapter 21: Applying Security Concepts in Support of Organizational Risk Mitigation

Chapter 22: The Importance of Frameworks, Policies, Procedures, and Controls

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

Get certified for the CySA+ CS0-002 exam with the CompTIA Cybersecurity Analyst (CySA+) course and lab. The lab provides a hands-on learning experience in a safe, online environment. The CySA+ study guide covers the CS0-002 exam objectives and provides an understanding of the topics such as firewalls and anti-virus software. The CySA+ practice test will provide you an analytics-based approach within the IT security industry that is increasingly important for organizations.

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: Introduction

- Goals and Methods
- Who Should Read This Course?
- Strategies for Exam Preparation
- How the Course Is Organized
- What’s New?

Chapter 2: The Importance of Threat Data and Intelligence

- Intelligence Sources

- Indicator Management
- Threat Classification
- Threat Actors
- Intelligence Cycle
- Commodity Malware
- Information Sharing and Analysis Communities
- Review All Key Topics
- Review Questions

Chapter 3: Utilizing Threat Intelligence to Support Organizational Security

- Attack Frameworks
- Threat Research
- Threat Modeling Methodologies
- Threat Intelligence Sharing with Supported Functions
- Review All Key Topics
- Review Questions

Chapter 4: Vulnerability Management Activities

- Vulnerability Identification
- Validation
- Remediation/Mitigation
- Scanning Parameters and Criteria
- Inhibitors to Remediation
- Review All Key Topics
- Review Questions

Chapter 5: Analyzing Assessment Output

- Web Application Scanner
- Infrastructure Vulnerability Scanner
- Software Assessment Tools and Techniques
- Enumeration
- Wireless Assessment Tools
- Cloud Infrastructure Assessment Tools
- Review All Key Topics
- Review Questions

Chapter 6: Threats and Vulnerabilities Associated with Specialized Technology

- Mobile
- Internet of Things (IoT)
- Embedded Systems
- Real-Time Operating System (RTOS)
- System-on-Chip (SoC)
- Field Programmable Gate Array (FPGA)
- Physical Access Control
- Building Automation Systems
- Vehicles and Drones
- Workflow and Process Automation Systems
- Incident Command System (ICS)
- Supervisory Control and Data Acquisition (SCADA)
- Review All Key Topics
- Review Questions

Chapter 7: Threats and Vulnerabilities Associated with Operating in the Cloud

- Cloud Deployment Models
- Cloud Service Models

- Function as a Service (FaaS)/Serverless Architecture
- Infrastructure as Code (IaC)
- Insecure Application Programming Interface (API)
- Improper Key Management
- Unprotected Storage
- Logging and Monitoring
- Review All Key Topics
- Review Questions

Chapter 8: Implementing Controls to Mitigate Attacks and Software Vulnerabilities

- Attack Types
- Vulnerabilities
- Review All Key Topics
- Review Questions

Chapter 9: Security Solutions for Infrastructure Management

- Cloud vs. On-premises
- Asset Management

- Segmentation
- Network Architecture
- Change Management
- Virtualization
- Containerization
- Identity and Access Management
- Cloud Access Security Broker (CASB)
- Honeypot
- Monitoring and Logging
- Encryption
- Certificate Management
- Active Defense
- Review All Key Topics
- Review Questions

Chapter 10: Software Assurance Best Practices

- Platforms
- Software Development Life Cycle (SDLC) Integration

- DevSecOps
- Software Assessment Methods
- Secure Coding Best Practices
- Static Analysis Tools
- Dynamic Analysis Tools
- Formal Methods for Verification of Critical Software
- Service-Oriented Architecture
- Review All Key Topics
- Review Questions

Chapter 11: Hardware Assurance Best Practices

- Hardware Root of Trust
- eFuse
- Unified Extensible Firmware Interface (UEFI)
- Trusted Foundry
- Secure Processing
- Anti-Tamper
- Self-Encrypting Drives

- Trusted Firmware Updates
- Measured Boot and Attestation
- Bus Encryption
- Review All Key Topics
- Review Questions

Chapter 12: Analyzing Data as Part of Security Monitoring Activities

- Heuristics
- Trend Analysis
- Endpoint
- Network
- Log Review
- Impact Analysis
- Security Information and Event Management (SIEM) Review
- Query Writing
- E-mail Analysis
- Review All Key Topics
- Review Questions

Chapter 13: Implementing Configuration Changes to Existing Controls to Improve Security

- Permissions
- Whitelisting and Blacklisting
- Firewall
- Intrusion Prevention System (IPS) Rules
- Data Loss Prevention (DLP)
- Endpoint Detection and Response (EDR)
- Network Access Control (NAC)
- Sinkholing
- Malware Signatures
- Sandboxing
- Port Security
- Review All Key Topics
- Review Questions

Chapter 14: The Importance of Proactive Threat Hunting

- Establishing a Hypothesis

- Profiling Threat Actors and Activities
- Threat Hunting Tactics
- Reducing the Attack Surface Area
- Bundling Critical Assets
- Attack Vectors
- Integrated Intelligence
- Improving Detection Capabilities
- Review All Key Topics
- Review Questions

Chapter 15: Automation Concepts and Technologies

- Workflow Orchestration
- Scripting
- Application Programming Interface (API) Integration
- Automated Malware Signature Creation
- Data Enrichment
- Threat Feed Combination
- Machine Learning

- Use of Automation Protocols and Standards
- Continuous Integration
- Continuous Deployment/Delivery
- Review All Key Topics
- Review Questions

Chapter 16: The Incident Response Process

- Communication Plan
- Response Coordination with Relevant Entities
- Factors Contributing to Data Criticality
- Review All Key Topics
- Review Questions

Chapter 17: Applying the Appropriate Incident Response Procedure

- Preparation
- Detection and Analysis
- Containment
- Eradication and Recovery
- Post-Incident Activities

- Review All Key Topics
- Review Questions

Chapter 18: Analyzing Potential Indicators of Compromise

- Network-Related Indicators of Compromise
- Host-Related Indicators of Compromise
- Application-Related Indicators of Compromise
- Review All Key Topics
- Review Questions

Chapter 19: Utilizing Basic Digital Forensics Techniques

- Network
- Endpoint
- Mobile
- Cloud
- Virtualization
- Legal Hold
- Procedures

- Hashing
- Carving
- Data Acquisition
- Review All Key Topics
- Review Questions

Chapter 20: The Importance of Data Privacy and Protection

- Privacy vs. Security
- Non-technical Controls
- Technical Controls
- Review All Key Topics
- Review Questions

Chapter 21: Applying Security Concepts in Support of Organizational Risk Mitigation

- Business Impact Analysis
- Risk Identification Process
- Risk Calculation
- Communication of Risk Factors
- Risk Prioritization

- Systems Assessment
- Documented Compensating Controls
- Training and Exercises
- Supply Chain Assessment
- Review All Key Topics
- Review Questions

Chapter 22: The Importance of Frameworks, Policies, Procedures, and Controls

- Frameworks
- Policies and Procedures
- Category
- Control Type
- Audits and Assessments
- Review All Key Topics
- Review Questions

11. Practice Test

Here's what you get

84	2	90
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

Vulnerability Management Activities

- Conducting Vulnerability Scanning Using Nessus

Analyzing Assessment Output

- Using Nikto
- Using OWASP ZAP
- Inspecting the Vulnerability in the Echo Server's Source Code
- Performing Reconnaissance on a Network
- Using the hping Program
- Identifying Search Options in Metasploit

Implementing Controls to Mitigate Attacks and Software Vulnerabilities

- Scanning the Rootkit
- Configuring DHCP Snooping
- Performing a MITM Attack
- Exploiting a Website Using SQL Injection
- Performing Session Hijacking Using Burp Suite
- Detecting Rootkits
- Performing ARP Spoofing

Security Solutions for Infrastructure Management

- Configuring Remote Access with VPN
- Configuring the SSL Port Setting
- Attacking a Website Using XSS Injection

- Setting up a Honeypot on Kali Linux
- Using the MD5 Hash Algorithm
- Encrypting and Decrypting a File Using AES Crypt

Analyzing Data as Part of Security Monitoring Activities

- Performing a Memory-Based Attack
- Using Apktool to Decode and Analyze the apk file
- Simulating the DDoS Attack
- Simulating a DoS Attack
- Scanning the Website using URLVoid
- Configuring Snort
- Making Syslog Entries Readable
- Examining Audited Events
- Installing Splunk on the Server

Implementing Configuration Changes to Existing Controls to Improve Security

- Using the iptables Command to Create a Personal Firewall in Linux

The Importance of Proactive Threat Hunting

- Working with the Task Manager

Applying the Appropriate Incident Response Procedure

- Configuring a Perimeter Firewall

Analyzing Potential Indicators of Compromise

- Performing the Initial Scan

Utilizing Basic Digital Forensics Techniques

- Confirming the Spoofing Attack in Wireshark
- Capturing a Packet Using Wireshark
- Downloading and Installing Wireshark

The Importance of Frameworks, Policies, Procedures, and Controls

- Reviewing and Modifying the Policy Items

Here's what you get

37	37	01:55
LIVE LABS	VIDEO TUTORIALS	HOURS

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