Course Ou

CCNA Cyber Ops SECO



26 Mar 2024

Contents

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: Threat Analysis

   Chapter 3: Forensics

   Chapter 4: Fundamentals of Intrusion Analysis

   Chapter 5: NetFlow for Cybersecurity

   Chapter 6: Introduction to Incident Response and the Incident Handling Process

   Chapter 7: Incident Response Teams

   Chapter 8: Compliance Frameworks

   Chapter 9: Network and Host Profiling

   Chapter 10: The Art of Data and Event Analysis

   Chapter 11: Intrusion Event Categories

   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

Prepare for the Cisco 210-255 SECOPS certification exam with the CCNA Cyber Ops SECOPS (210-255) course and lab. Lab simulates real-world, hardware, software, and command-line interface environments and can be mapped to any text-book, course, or training. Interactive chapters comprehensively cover CCNA Cyber Ops certification exam objectives and provide knowledge in areas such as endpoint threat analysis, computer forensics, network intrusion analysis, incident response, data and event analysis, incident handling, and so on.

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.

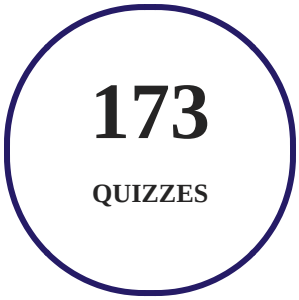
3. Exercises

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.



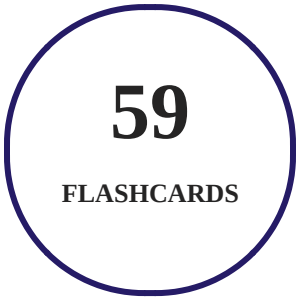
4. Quizzes

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: Introduction

- About the 210-255 CCNA Cyber Ops SECOPS Exam
- About the CCNA Cyber Ops SECOPS #210-255 Official Cert Guide

Chapter 2: Threat Analysis

- What Is the CIA Triad: Confidentiality, Integrity, and Availability?
- Threat Modeling
- Defining and Analyzing the Attack Vector
- Understanding the Attack Complexity
- Privileges and User Interaction
- The Attack Scope
- Review All Key Topics

Chapter 3: Forensics

- Introduction to Cybersecurity Forensics
- The Role of Attribution in a Cybersecurity Investigation
- The Use of Digital Evidence
- Fundamentals of Microsoft Windows Forensics
- Fundamentals of Linux Forensics
- Review All Key Topics

Chapter 4: Fundamentals of Intrusion Analysis

- Common Artifact Elements and Sources of Security Events
- Understanding Regular Expressions
- Protocols, Protocol Headers, and Intrusion Analysis
- Using Packet Captures for Intrusion Analysis
- Review All Key Topics

Chapter 5: NetFlow for Cybersecurity

- Introduction to NetFlow
- NetFlow Versions
- IPFIX
- NetFlow for Cybersecurity and Incident Response
- NetFlow Analysis Tools
- Review All Key Topics

Chapter 6: Introduction to Incident Response and the Incident Handling Process

- Introduction to Incident Response
- The Incident Response Plan
- The Incident Response Process
- Information Sharing and Coordination

- Incident Response Team Structure
- The Vocabulary for Event Recording and Incident Sharing (VERIS)
- Review All Key Topics

Chapter 7: Incident Response Teams

- Computer Security Incident Response Teams (CSIRTs)
- Product Security Incident Response Teams (PSIRTs)
- National CSIRTs and Computer Emergency Response Teams (CERTs)
- Coordination Centers
- Incident Response Providers and Managed Security Service Providers (MSSPs)
- Review All Key Topics

Chapter 8: Compliance Frameworks

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley (SOX)
- Summary
- References

- Review All Key Topics

Chapter 9: Network and Host Profiling

- Network Profiling
- Host Profiling
- Summary
- References
- Review All Key Topics

Chapter 10: The Art of Data and Event Analysis

- Normalizing Data
- Using the 5-Tuple Correlation to Respond to Security Incidents
- Retrospective Analysis and Identifying Malicious Files
- Mapping Threat Intelligence with DNS and Other Artifacts
- Deterministic Versus Probabilistic Analysis
- Review All Key Topics

Chapter 11: Intrusion Event Categories

- Diamond Model of Intrusion

- Cyber Kill Chain Model
- Summary
- References
- Review All Key Topics

Videos and How To

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

62	04:55
VIDEOS	HOURS

12. Practice Test

Here's what you get

60	2	60
PRE-ASSESSMENTS QUESTIONS	FULL LENGTH TESTS	POST-ASSESSMENTS QUESTIONS

Features

uCertify provides video training courses that contain videos and test set questions based on the exam. These courses are interactive and engaging and the learners can view the content at their own pace, in their own time, and on any device. Learners can easily track the engagement levels so they immediately know which course components are easy to understand and which are more difficult. Test set in the courses closely follow the exam objectives and are designed to simulate real exam conditions.

Each pre and post assessment comes with interactive questions which help users in better understanding of the subject matter.

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

Threat Analysis

- Scanning the Rootkit
- Performing the Initial Scan
- Understanding attack complexity

Forensics

- Understanding cybersecurity investigations
- Understanding disk imaging
- Understanding Windows file system
- Understanding file system structure
- Understanding Linux Boot Process

Fundamentals of Intrusion Analysis

- Understanding fundamentals of intrusion analysis
- Understanding security threat intelligence
- Understanding evasion techniques
- Understanding header protocol
- 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

- Confirming the Spoofing Attack in Wireshark
- Observing Traffic Patterns Using Wireshark
- Analyzing Protocols with Wireshark

NetFlow for Cybersecurity

- Understanding NetFlow cache
- Understanding NetFlow for cybersecurity
- Examining the DDOS_Attack.pcap File
- Exporting your Windows logs
- Making Syslog Entries Readable
- Identifying a suspicious account on the System User Groups
- Enabling logging for audited objects
- Examining the Audited Events

Introduction to Incident Response and the Incident Handling Process

- Understanding response plan
- Understanding VERIS schema

Incident Response Teams

- Establishing a CSIRT
- Consulting a Vulnerability Database

Compliance Frameworks

- Uploading the Trojan horse simulator to VirusTotal
- Uploading the Trojan horse simulator to Malware
- Assessing the impact of malware

Network and Host Profiling

- Understanding network profiling

The Art of Data and Event Analysis

- Understanding SIEM
- Using 5-Tuple correlation
- Understanding threat intelligence
- Understanding event analysis

Intrusion Event Categories

- Performing Reconnaissance on a Network
- Understanding Kill Chain Model

Here's what you get

41

LIVE LABS

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:

3187 Independence Drive
Livermore, CA 94551,
United States

+1-415-763-6300

support@ucertify.com

www.ucertify.com