uCertify

Course Outline

Cisco CyberOps Associate CBROPS (200-201)

18 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: Cybersecurity Fundamentals

   Chapter 3: Introduction to Cloud Computing and Cloud Security

   Chapter 4: Access Control Models

   Chapter 5: Types of Attacks and Vulnerabilities

   Chapter 6: Fundamentals of Cryptography and Public Key Infrastructure (PKI)

   Chapter 7: Introduction to Virtual Private Networks (VPNs)

   Chapter 8: Introduction to Security Operations Management

   Chapter 9: Fundamentals of Intrusion Analysis

   Chapter 10: Introduction to Digital Forensics

   Chapter 11: Network Infrastructure Device Telemetry and Analysis

   Chapter 12: Endpoint Telemetry and Analysis

   Chapter 13: Challenges in the Security Operations Center (SOC)

   Chapter 14: The Art of Data and Event Analysis

   Chapter 15: Classifying Intrusion Events into Categories

   Chapter 16: Introduction to Threat Hunting

   Videos and How To
9. Practice Test

1. Course Objective

Prepare yourself for a career in cybersecurity and become a certified Cisco CyberOps Associate with the comprehensive Cisco CyberOps Associate CBROPS (200-201) course. Designed to equip you with the necessary skills and knowledge, this course covers cybersecurity principles through interactive lessons, quizzes, test preps, and hands-on labs. With a focus on preventing, detecting, analyzing, and responding to cybersecurity incidents, this course will prepare you for the exam and pave the way for associate-level job roles in security operations centers (SOCs).

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. Quiz

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

- The Cisco CyberOps Associate Certification
- The Exam Objectives (Domains)
- Steps to Pass the 200-201 CBROPS Exam
- Signing Up for the Exam
- Facts About the Exam
- About the Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

Chapter 2: Cybersecurity Fundamentals

- Introduction to Cybersecurity
- Threats, Vulnerabilities, and Exploits
- Network Security Systems
- Intrusion Detection Systems and Intrusion Prevention Systems
- Advanced Malware Protection
- Web Security Appliance
- Email Security Appliance
- Cisco Security Management Appliance
- Cisco Identity Services Engine
- Security Cloud-Based Solutions
- Cisco NetFlow
- Data Loss Prevention
- The Principles of the Defense-in-Depth Strategy
- Confidentiality, Integrity, and Availability: The CIA Triad
- Risk and Risk Analysis
- Personally Identifiable Information and Protected Health Information
- Principle of Least Privilege and Separation of Duties

- Security Operations Centers
- Playbooks, Runbooks, and Runbook Automation
- Digital Forensics
- Review All Key Topics
- Review Questions

Chapter 3: Introduction to Cloud Computing and Cloud Security

- Cloud Computing and the Cloud Service Models
- Cloud Security Responsibility Models
- DevOps, Continuous Integration (CI), Continuous Delivery (CD), and DevSecOps
- Understanding the Different Cloud Security Threats
- Review All Key Topics
- Review Questions

Chapter 4: Access Control Models

- Information Security Principles
- Subject and Object Definition
- Access Control Fundamentals
- Access Control Process

- Information Security Roles and Responsibilities
- Access Control Types
- Access Control Models
- Access Control Mechanisms
- Identity and Access Control Implementation
- Review All Key Topics
- Review Questions

Chapter 5: Types of Attacks and Vulnerabilities

- Types of Attacks
- Types of Vulnerabilities
- Review All Key Topics
- Review Questions

Chapter 6: Fundamentals of Cryptography and Public Key Infrastructure (PKI)

- Cryptography
- Block and Stream Ciphers
- Symmetric and Asymmetric Algorithms

- Hashes
- Digital Signatures
- Next-Generation Encryption Protocols
- IPsec and SSL/TLS
- Fundamentals of PKI
- Root and Identity Certificates
- Revoking Digital Certificates
- Using Digital Certificates
- Review All Key Topics
- Review Questions

Chapter 7: Introduction to Virtual Private Networks (VPNs)

- What Are VPNs?
- Site-to-Site vs. Remote-Access VPNs
- An Overview of IPsec
- SSL VPNs
- Review All Key Topics
- Review Questions

Chapter 8: Introduction to Security Operations Management

- Introduction to Identity and Access Management
- Security Events and Log Management
- Asset Management
- Introduction to Enterprise Mobility Management
- Configuration and Change Management
- Vulnerability Management
- Patch Management
- Review All Key Topics
- Review Questions

Chapter 9: Fundamentals of Intrusion Analysis

- Introduction to Incident Response
- The Incident Response Plan
- The Incident Response Process
- Information Sharing and Coordination
- Incident Response Team Structure
- Common Artifact Elements and Sources of Security Events

- Understanding Regular Expressions
- Protocols, Protocol Headers, and Intrusion Analysis
- How to Map Security Event Types to Source Technologies
- Review All Key Topics
- Review Questions

Chapter 10: Introduction to Digital Forensics

- Introduction to Digital Forensics
- The Role of Attribution in a Cybersecurity Investigation
- The Use of Digital Evidence
- Evidentiary Chain of Custody
- Reverse Engineering
- Fundamentals of Microsoft Windows Forensics
- Fundamentals of Linux Forensics
- Review All Key Topics
- Review Questions

Chapter 11: Network Infrastructure Device Telemetry and Analysis

- Network Infrastructure Logs
- Traditional Firewall Logs
- NetFlow Analysis
- Network Packet Capture
- Network Profiling
- Review All Key Topics
- Review Questions

Chapter 12: Endpoint Telemetry and Analysis

- Understanding Host Telemetry
- Host Profiling
- Analyzing Windows Endpoints
- Linux and macOS Analysis
- Endpoint Security Technologies
- Review All Key Topics
- Review Questions

Chapter 13: Challenges in the Security Operations Center (SOC)

- Security Monitoring Challenges in the SOC

- Additional Evasion and Obfuscation Techniques
- Review All Key Topics
- Review Questions

Chapter 14: The Art of Data and Event Analysis

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

Chapter 15: Classifying Intrusion Events into Categories

- Diamond Model of Intrusion
- Cyber Kill Chain Model
- The Kill Chain vs. MITRE’s ATT&CK
- Review All Key Topics

- Review Questions

Chapter 16: Introduction to Threat Hunting

- What Is Threat Hunting?
- The Threat-Hunting Process
- Threat Hunting and MITRE’s ATT&CK
- Threat-Hunting Case Study
- Threat Hunting, Honeypots, Honeynets, and Active Defense
- Review All Key Topics
- Review Questions

11. Practice Test

Here's what you get

90	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

Cybersecurity Fundamentals

- Exploiting Command Injection Vulnerabilities

- Using Rainbow Tables
- Consulting a Vulnerability Database
- Configuring Dynamic NAT
- Creating and Applying a Numbered Standard ACL
- Creating and Applying a Numbered Extended ACL

Introduction to Cloud Computing and Cloud Security

- Simulating a DoS Attack

Access Control Models

- Installing Antivirus Software
- Enabling AAA Services and Working with Method Lists
- Implementing Port Security

Types of Attacks and Vulnerabilities

- Understanding Local Privilege Escalation
- Applying a DNS Capture Filter
- Configuring a BPDU Guard on a Switch Port
- Using Maltego
- Using Shodan to Find Webcams
- Using Nikto
- Using Social Engineering Techniques to Plan an Attack
- Simulating the DDoS Attack
- Performing ARP Spoofing
- Cracking a Linux Password Using John the Ripper
- Performing Active Reconnaissance
- Performing a Memory-Based Attack
- Performing a MITM Attack
- Defending Against a Buffer Overflow Attack
- Attacking a Website Using XSS Injection
- Conducting Cross-Site Request Forgery Attacks

Fundamentals of Cryptography and Public Key Infrastructure (PKI)

- Using PGP
- Generating a Symmetric Key
- Generating an Asymmetric Key
- Applying Symmetric Key Encryption
- Observing an MD5-Generated Hash Value
- Observing an SHA-Generated Hash Value
- Examining PKI Certificates

Introduction to Virtual Private Networks (VPNs)

- Implementing IPsec VPNs through CLI
- Configuring an SSL Cisco AnyConnect Secure Mobility Client VPN
- Configuring Clientless SSL VPNs on ASA

Introduction to Security Operations Management

- Viewing Event Logs

Fundamentals of Intrusion Analysis

- Using the Armitage Tool for Intrusion Detection
- Performing Intrusion Detection Using Zeek
- Capturing a Packet Using Tshark
- Capturing Network Packets Using tcpdump

Introduction to Digital Forensics

- Using Reverse Engineering
- Changing the Startup Type of Service
- Viewing the Windows File Registry
- Managing NTFS Permissions
- Using Linux Commands

Network Infrastructure Device Telemetry and Analysis

- Configuring a Router to Use NTP Services

- Simulating an Eavesdropping Attack Using Wireshark
- Configuring NetFlow and NetFlow Data Export

Endpoint Telemetry and Analysis

- Showing Logging in to a System
- Identifying Listening Ports on the Network
- Using Windows Event Viewer
- Changing File Permissions
- Using a Symlink

Introduction to Threat Hunting

- Examining MITRE ATT&CK
- Setting Up a Honeypot

Here's what you get

55	56	02:06
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.