uCertify

Course Outline

Modern Security Operations Center

20 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: Preface

   Chapter 2: Introducing Security Operations and the SOC

   Chapter 3: Developing a Security Operations Center

   Chapter 4: SOC Services

   Chapter 5: People and Process

   Chapter 6: Centralizing Data

   Chapter 7: Reducing Risk and Exceeding Compliance

   Chapter 8: Threat Intelligence

   Chapter 9: Threat Hunting and Incident Response

   Chapter 10: Vulnerability Management

   Chapter 11: Data Orchestration

   Chapter 12: Future of the SOC

   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

The Modern Security Operations Center course helps you learn the essential skills and knowledge needed to protect organizations from cyber threats. This course is designed to provide students with a comprehensive understanding of modern SOC operations, including threat intelligence, incident response, and security monitoring. Throughout the course, you will learn about the latest tools and techniques used in SOCs to detect and respond to cyber threats. You will gain hands-on experience in threat hunting, incident response, and security monitoring, using industry-leading tools and technologies.

2. Pre-Assessment

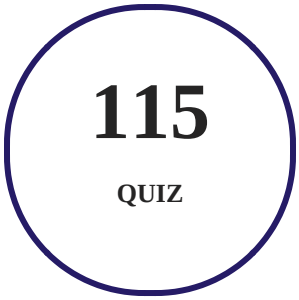
Pre-Assessment lets you identify the areas for improvement before you start your prep. It determines what students know about a topic before it is taught and identifies areas for improvement with question assessment before beginning the course.

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. 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.



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: Preface

- Vision
- Who Should Read This Course?
- How This Course Is Organized

- Course Structure

Chapter 2: Introducing Security Operations and the SOC

- Introducing the SOC
- Factors Leading to a Dysfunctional SOC
- Cyberthreats
- Investing in Security
- The Impact of a Breach
- Establishing a Baseline
- Fundamental Security Capabilities
- Standards, Guidelines, and Frameworks
- Industry Threat Models
- Vulnerabilities and Risk
- Business Challenges
- In-House vs. Outsourcing
- SOC Services
- SOC Maturity Models
- SOC Goals Assessment

- SOC Capabilities Assessment
- SOC Development Milestones
- Summary
- References

Chapter 3: Developing a Security Operations Center

- Mission Statement and Scope Statement
- Developing a SOC
- SOC Procedures
- Security Tools
- Planning a SOC
- Designing a SOC Facility
- Network Considerations
- Disaster Recovery
- Security Considerations
- Internal Security Tools
- Guidelines and Recommendations for Securing Your SOC Network
- SOC Tools

- Summary
- References

Chapter 4: SOC Services

- Fundamental SOC Services
- The Three Pillars of Foundational SOC Support Services
- SOC Service Areas
- SOC Service Job Goals
- Service Maturity: If You Build It, They Will Come
- SOC Service 1: Risk Management
- SOC Service 2: Vulnerability Management
- SOC Service 3: Compliance
- SOC Service 4: Incident Management
- SOC Service 5: Analysis
- SOC Service 6: Digital Forensics
- SOC Service 7: Situational and Security Awareness
- SOC Service 8: Research and Development
- Summary

- References

Chapter 5: People and Process

- Career vs. Job
- Developing Job Roles
- SOC Job Roles
- NICE Cybersecurity Workforce Framework
- Role Tiers
- SOC Services and Associated Job Roles
- Soft Skills
- Security Clearance Requirements
- Pre-Interviewing
- Interviewing
- Onboarding Employees
- Managing People
- Job Retention
- Training
- Certifications

- Evaluating Training Providers
- Company Culture
- Summary
- References

Chapter 6: Centralizing Data

- Data in the SOC
- Data-Focused Assessment
- Logs
- Security Information and Event Management
- Troubleshooting SIEM Logging
- APIs
- Big Data
- Machine Learning
- Summary
- References

Chapter 7: Reducing Risk and Exceeding Compliance

- Why Exceeding Compliance
- Policies
- Launching a New Policy
- Policy Enforcement
- Procedures
- Tabletop Exercise
- Standards, Guidelines, and Frameworks
- Audits
- Assessments
- Penetration Test
- Industry Compliance
- Summary
- References

Chapter 8: Threat Intelligence

- Threat Intelligence Overview
- Threat Intelligence Categories
- Threat Intelligence Context

- Evaluating Threat Intelligence
- Planning a Threat Intelligence Project
- Collecting and Processing Intelligence
- Actionable Intelligence
- Feedback
- Summary
- References

Chapter 9: Threat Hunting and Incident Response

- Security Incidents
- Incident Response Lifecycle
- Phase 1: Preparation
- Phase 2: Detection and Analysis
- Phase 3: Containment, Eradication, and Recovery
- Digital Forensics
- Phase 4: Post-Incident Activity
- Incident Response Guidelines
- Summary

- References

Chapter 10: Vulnerability Management

- Vulnerability Management
- Measuring Vulnerabilities
- Vulnerability Technology
- Vulnerability Management Service
- Vulnerability Response
- Vulnerability Management Process Summarized
- Summary
- References

Chapter 11: Data Orchestration

- Introduction to Data Orchestration
- Security Orchestration, Automation, and Response
- Endpoint Detection and Response
- Playbooks
- Automation
- DevOps Programming

- DevOps Tools
- Blueprinting with Osquery
- Network Programmability
- Cloud Programmability
- Summary
- References

Chapter 12: Future of the SOC

- All Eyes on SD-WAN and SASE
- MPLS Failure!
- IT Services Provided by the SOC
- Future of Training
- Full Automation with Machine Learning
- Future of Your SOC: Bringing It All Together
- Summary
- References

12. Practice Test

Here's what you get

100	100
PRE-ASSESSMENTS QUESTIONS	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.

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

Developing a Security Operations Center

- Using Windows Firewall
- Configuring a VPN
- Setting Up a Honeypot
- Capturing a Packet Using Wireshark
- Configuring NetFlow
- Implementing Intrusion Detection System

SOC Services

- Identifying Search Options in Metasploit
- Searching Exploits Using searchsploit
- Conducting Vulnerability Scanning Using Nessus
- Performing Vulnerability Scanning Using OpenVAS
- Using the SET Tool

Centralizing Data

- Viewing Windows Event Logs
- Viewing the Syslogs

Reducing Risk and Exceeding Compliance

- Using the Armitage Tool for Intrusion Detection

Threat Hunting and Incident Response

- Observing an MD5-Generated Hash Value

- Observing an SHA256-Generated Hash Value
- Analyzing Malicious Activity in Memory Using Volatility
- Analyzing Forensic Cases with Autopsy
- Completing the Chain of Custody

Vulnerability Management

- Using Nmap for Network Enumeration
- Consulting a Vulnerability Database
- Performing an Intense Scan in Zenmap

Data Orchestration

- Creating an Ansible Configuration File
- Creating Ansible Roles
- Using the Ansible Tool
- Using Osquery to Perform Enhanced Incident Response and Threat Hunting

Here's what you get

26	25	49
LIVE LABS	VIDEO TUTORIALS	MINUTES

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.