uCertify

Course Outline

Threat Hunting in the Cloud: Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks



27 Mar 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: Introduction to Threat Hunting

   Chapter 3: Modern Approach to Multi-Cloud Threat Hunting

   Chapter 4: Exploration of MITRE Key Attack Vectors

   Chapter 5: Microsoft Azure Cloud Threat Prevention Framework

   Chapter 6: Microsoft Cybersecurity Reference Architecture and Capability Map

   Chapter 7: AWS Cloud Threat Prevention Framework

   Chapter 8: AWS Reference Architecture

   Chapter 9: Threat Hunting in Other Cloud Providers

   Chapter 10: The Future of Threat Hunting

   Chapter 11: APPENDIX A: MITRE ATT&CK Tactics

   Chapter 12: APPENDIX B: Privilege Escalation

   Chapter 13: APPENDIX C: Credential Access

   Chapter 14: APPENDIX D: Lateral Movement

   Chapter 15: APPENDIX E: Command and Control

   Chapter 16: APPENDIX F: Data Exfiltration

   Chapter 17: APPENDIX G: MITRE Cloud Matrix

   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

Threat hunting is a critical focus area to increase the cybersecurity posture of any organization. The contents of the course are prepared to serve business decision-makers like board members, CXOs, and CISOs, as well as a technical audience. Business users will find the technology-agnostic cloud threat-hunting methodology framework valuable to manage their cybersecurity risks. This course addresses Microsoft Azure and AWS side by side. It contains assessment questions, interactive lessons with knowledge checks and quizzes, and hands-on labs to understand the threat-hunting framework in cybersecurity.

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.

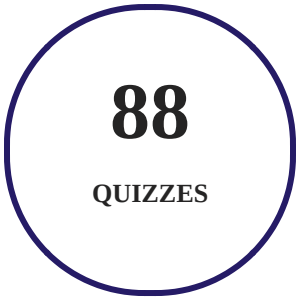
3. Exercises

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.



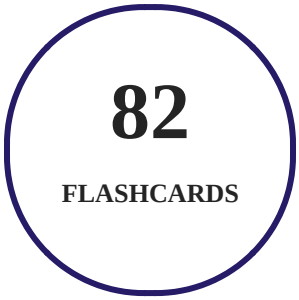
4. Quizzes

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

- What Does This Course Cover?
- Additional Resources

Chapter 2: Introduction to Threat Hunting

- The Rise of Cybercrime
- What Is Threat Hunting?
- The Key Cyberthreats and Threat Actors
- The Necessity of Threat Hunting
- Threat Modeling
- Threat-Hunting Maturity Model
- Human Elements of Threat Hunting
- Summary

Chapter 3: Modern Approach to Multi-Cloud Threat Hunting

- Multi-Cloud Threat Hunting
- Building Blocks for the Security Operations Center
- Cyberthreat Detection, Threat Modeling, and the Need for Proactive Threat Hunting Within SOC
- Cyber Resiliency and Organizational Culture
- Skillsets Required for Threat Hunting
- Threat-Hunting Process and Procedures

- Metrics for Assessing the Effectiveness of Threat Hunting
- Threat-Hunting Program Effectiveness
- Summary

Chapter 4: Exploration of MITRE Key Attack Vectors

- Understanding MITRE ATT&CK
- Threat Hunting Using Five Common Tactics
- Other Methodologies and Key Threat-Hunting Tools to Combat Attack Vectors
- Analysis Tools
- Summary

Chapter 5: Microsoft Azure Cloud Threat Prevention Framework

- Introduction to Microsoft Security
- Understanding the Shared Responsibility Model
- Microsoft Services for Cloud Security Posture Management and Logging/Monitoring
- Using Microsoft Secure and Protect Features
- Microsoft Detect Services
- Detecting “Privilege Escalation” TTPs
- Detecting Credential Access

- Detecting Lateral Movement
- Detecting Command and Control
- Detecting Data Exfiltration
- Microsoft Investigate, Response, and Recover Features
- Using Machine Learning and Artificial Intelligence in Threat Response
- Summary

Chapter 6: Microsoft Cybersecurity Reference Architecture and Capability Map

- Introduction
- Microsoft Security Architecture versus the NIST Cybersecurity Framework (CSF)
- Microsoft Security Architecture
- Using the Microsoft Reference Architecture
- Understanding the Security Operations Solutions
- Understanding the People Security Solutions
- Summary

Chapter 7: AWS Cloud Threat Prevention Framework

- Introduction to AWS Well-Architected Framework

- AWS Services for Monitoring, Logging, and Alerting
- AWS Protect Features
- AWS Detection Features
- How Do You Detect Privilege Escalation?
- How Do You Detect Credential Access?
- How Do You Detect Lateral Movement?
- How Do You Detect Command and Control?
- How Do You Detect Data Exfiltration?
- How Do You Handle Response and Recover?
- Summary
- References

Chapter 8: AWS Reference Architecture

- AWS Security Framework Overview
- AWS Reference Architecture
- Summary

Chapter 9: Threat Hunting in Other Cloud Providers

- The Google Cloud Platform

- The IBM Cloud
- Oracle Cloud Infrastructure Security
- The Alibaba Cloud
- Summary
- References

Chapter 10: The Future of Threat Hunting

- Artificial Intelligence and Machine Learning
- Advances in Quantum Computing
- Advances in IoT and Their Impact
- Operational Technology (OT)
- Blockchain
- Threat Hunting as a Service
- The Evolution of the Threat-Hunting Tool
- Potential Regulatory Guidance
- Summary
- References

Chapter 11: APPENDIX A: MITRE ATT&CK Tactics

Chapter 12: APPENDIX B: Privilege Escalation

Chapter 13: APPENDIX C: Credential Access

Chapter 14: APPENDIX D: Lateral Movement

Chapter 15: APPENDIX E: Command and Control

Chapter 16: APPENDIX F: Data Exfiltration

Chapter 17: APPENDIX G: MITRE Cloud Matrix

- Initial Access
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Data Exfiltration
- Impact

12. Practice Test

Here's what you get

50	50
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

Introduction to Threat Hunting

- Performing a Phishing Attack

Exploration of MITRE Key Attack Vectors

- Performing Local Privilege Escalation
- Enabling and Disabling GuardDuty
- Creating a CloudWatch Dashboard

Microsoft Azure Cloud Threat Prevention Framework

- Creating a Service Bus
- Deploying an Azure Firewall
- Creating an Azure Front Door

AWS Cloud Threat Prevention Framework

- Creating VPC Flow Logs
- Creating CloudTrail
- Examining Macie
- Creating a Rule in Amazon EventBridge
- Creating a Lambda Function
- Creating an Amazon SNS Topic

AWS Reference Architecture

- Creating a VPC

Threat Hunting in Other Cloud Providers

- Creating a VPC Network

Here's what you get

15	15	43
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.

GET IN TOUCH:

3187 Independence Drive
Livermore, CA 94551,
United States

+1-415-763-6300

support@ucertify.com

www.ucertify.com