uCertify

Course Outline

Digital Forensics and Incident Response

05 Jul 2024

www.uCertify.com

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: Understanding Incident Response

   Chapter 3: Managing Cyber Incidents

   Chapter 4: Fundamentals of Digital Forensics

   Chapter 5: Investigation Methodology

   Chapter 6: Collecting Network Evidence

   Chapter 7: Acquiring Host-Based Evidence

   Chapter 8: Remote Evidence Collection

   Chapter 9: Forensic Imaging

   Chapter 10: Analyzing Network Evidence

   Chapter 11: Analyzing System Memory

   Chapter 12: Analyzing System Storage

   Chapter 13: Analyzing Log Files

   Chapter 14: Writing the Incident Report

   Chapter 15: Ransomware Preparation and Response

   Chapter 16: Ransomware Investigations

   Chapter 17: Malware Analysis for Incident Response

   Chapter 18: Leveraging Threat Intelligence

- Chapter 19: Threat Hunting
- Chapter 20: Appendix

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

Explore the complexities of digital forensics, mastering the techniques of investigating cyber incidents, scrutinizing digital evidence, and effectively responding to cybersecurity threats. From grasping the essentials of cybercrime investigations to navigating advanced forensic analysis and incident response strategies, this course provides a comprehensive skill set. Dive into practical learning with the latest tools, analyze real-life examples, and develop the skills needed to strengthen digital environments.

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.

148

EXERCISES

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.

60

QUIZ

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.

94

FLASHCARDS

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.

94

GLOSSARY OF 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

- Who this course is for

- What this course covers

- To get the most out of this course

Chapter 2: Understanding Incident Response

- The IR process
- The IR framework
- The IR plan
- The IR playbook/handbook
- Testing the IR framework
- Summary
- Further reading

Chapter 3: Managing Cyber Incidents

- Engaging the incident response team
- SOAR
- Incorporating crisis communications
- Incorporating containment strategies
- Getting back to normal – eradication, recovery, and post-incident activity
- Summary
- Further reading

Chapter 4: Fundamentals of Digital Forensics

- An overview of forensic science
- Locard’s exchange principle
- Legal issues in digital forensics
- Forensic procedures in incident response
- Summary
- Further reading

Chapter 5: Investigation Methodology

- An intrusion analysis case study: The Cuckoo’s Egg
- Types of incident investigation analysis
- Functional digital forensic investigation methodology
- The cyber kill chain
- The diamond model of intrusion analysis
- Summary

Chapter 6: Collecting Network Evidence

- An overview of network evidence

- Firewalls and proxy logs
- NetFlow
- Packet capture
- Wireshark
- Evidence collection
- Summary
- Further reading

Chapter 7: Acquiring Host-Based Evidence

- Preparation
- Order of volatility
- Evidence acquisition
- Acquiring volatile memory
- Acquiring non-volatile evidence
- Summary
- Further reading

Chapter 8: Remote Evidence Collection

- Enterprise incident response challenges

- Endpoint detection and response
- Velociraptor overview and deployment
- Velociraptor scenarios
- Summary

Chapter 9: Forensic Imaging

- Understanding forensic imaging
- Tools for imaging
- Preparing a staging drive
- Using write blockers
- Imaging techniques
- Summary
- Further reading

Chapter 10: Analyzing Network Evidence

- Network evidence overview
- Analyzing firewall and proxy logs
- Analyzing NetFlow

- Analyzing packet captures
- Summary
- Further reading

Chapter 11: Analyzing System Memory

- Memory analysis overview
- Memory analysis methodology
- Memory analysis tools
- Memory analysis with Strings
- Summary
- Further reading

Chapter 12: Analyzing System Storage

- Forensic platforms
- Autopsy
- Master File Table analysis
- Prefetch analysis
- Registry analysis
- Summary

- Further reading

Chapter 13: Analyzing Log Files

- Logs and log management
- Working with SIEMs
- Windows Logs
- Analyzing Windows Event Logs
- Summary
- Further reading

Chapter 14: Writing the Incident Report

- Documentation overview
- Executive summary
- Incident investigation report
- Forensic report
- Preparing the incident and forensic report
- Summary
- Further reading

Chapter 15: Ransomware Preparation and Response

- History of ransomware
- Conti ransomware case study
- Proper ransomware preparation
- Eradication and recovery
- Summary
- Further reading

Chapter 16: Ransomware Investigations

- Ransomware initial access and execution
- Discovering credential access and theft
- Investigating post-exploitation frameworks
- Command and Control
- Investigating lateral movement techniques
- Summary
- Further reading

Chapter 17: Malware Analysis for Incident Response

- Malware analysis overview
- Setting up a malware sandbox
- Static analysis
- Dynamic analysis
- ClamAV
- YARA
- Summary
- Further reading

Chapter 18: Leveraging Threat Intelligence

- Threat intelligence overview
- Sourcing threat intelligence
- The MITRE ATT&CK framework
- Working with IOCs and IOAs
- Threat intelligence and incident response
- Summary
- Further reading

Chapter 19: Threat Hunting

- Threat hunting overview
- Crafting a hypothesis
- Planning a hunt
- Digital forensic techniques for threat hunting
- EDR for threat hunting
- Summary
- Further reading

Chapter 20: Appendix

12. Practice Test

Here's what you get

55	55
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

Fundamentals of Digital Forensics

- Completing the Chain of Custody

Investigation Methodology

- Performing Reconnaissance on a Network

Collecting Network Evidence

- Installing a DHCP Server
- Performing a Proxy Server Operation
- Creating a Firewall Rule
- Capturing Packet Using RawCap
- Using tcpdump to Capture Packets

Acquiring Host-Based Evidence

- Using WinPmem for Memory Acquisition
- Using FTK Imager
- Using FTK Imager for Obtaining Protected Files

Remote Evidence Collection

- Using the Velociraptor Server

Forensic Imaging

- Preparing a Staging Drive
- Using EnCase Imager

Analyzing Network Evidence

- Working with NetworkMiner
- Capturing a Packet Using Wireshark

Analyzing System Memory

- Analyzing Malicious Activity in Memory Using Volatility
- Working with Strings in Linux

Analyzing System Storage

- Analyzing Forensic Case with Autopsy
- Viewing the Windows File Registry

Analyzing Log Files

- Creating an Event Log View
- Examining Windows Event Logs Using DeepBlueCLI

Ransomware Preparation and Response

- Understanding LPE

Ransomware Investigations

- Using Social Engineering Techniques to Plan an Attack
- Passing the Hash Using Mimikatz

Malware Analysis for Incident Response

- Analyzing Malware Using VirusTotal
- Using Process Explorer
- Handling Potential Malware Using ClamAV

Leveraging Threat Intelligence

- Examining MITRE ATT&CK
- Using Maltego to Gather Information

Here's what you get

29

LIVE LABS

29

VIDEO TUTORIALS

49

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