CYBER HERO CERTIFICATION PRACTICE TEST (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cyberherocert.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 16

SAMPLE

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

SAMPLE

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

SAMPLE

Questions

SAMPLE

1. What is the primary goal of a security audit?

A. To assess the aesthetic of IT systems

B. To systematically evaluate security policies and practices

C. To implement new hardware solutions

D. To analyze software performance

2. What does "white-hat hacking" refer to?

A. Ethical hacking performed to improve security by identifying vulnerabilities

B. Illegal hacking for personal gain

C. A certification for cybersecurity professionals

D. A type of malware that exploits system vulnerabilities

3. In cybersecurity, what does the term "data breach" typically refer to?

A. Unencrypted data being accessed by unauthorized persons

B. Data stored on a cloud server

C. A physical loss of hardware

D. A software update failing

4. What occurs after the baseline is updated in Threatlocker?

A. Policies are deleted

B. It conducts its first learning based on found data

C. It automatically reinstalls all applications

D. It no longer monitors applications

5. What is "threat intelligence"?

A. Information that helps organizations understand potential cyber threats

B. A method of improving network speed

C. A type of firewall protection

D. A software used for data encryption

6. What happens when new computers are added with continuous deployment?

A. They will need manual software installation

B. They will automatically get ThreatLocker deployed

C. They will require configuration settings

D. They will be marked as incomplete installations

SAMPLE

7. During the automatic learning period, which folders will applications not be profiled unless matched to an application name?

A. Program Files and Windows Directory

B. Documents, Downloads, Desktop, Users, and Root of C:\

C. App Data and Temporary folders

D. Network shares and WinSxS folder

8. When elevating a policy, what is crucial to consider?

A. Allow interaction with all applications

B. Block interaction with all other applications, unless necessary

C. Set only a few applications to run

D. Keep applications unmonitored

9. Which of the following best describes the role of a SIEM system?

A. To provide antivirus protection

B. To aggregate and analyze security data

C. To facilitate network speed enhancements

D. To backup critical data regularly

10. Which element is an important part of employee training in security awareness?

A. Time management techniques

B. Effective communication practices

C. Awareness of evolving cyber threats

D. Knowledge of financial planning

SAMPLE

Answers

SAMPLE

1. B
2. A
3. A
4. B
5. A
6. B
7. B
8. B
9. B
10. C

SAMPLE

Explanations

SAMPLE

1. What is the primary goal of a security audit?

A. To assess the aesthetic of IT systems

B. To systematically evaluate security policies and practices

C. To implement new hardware solutions

D. To analyze software performance

The primary goal of a security audit is to systematically evaluate security policies and practices. This entails a comprehensive examination of an organization's security measures to ensure they are effective and comply with established standards and regulations. By focusing on security policies and practices, a security audit identifies vulnerabilities, assesses risks, and evaluates the overall security posture. This process is essential for ensuring that the organization's information assets are protected against threats and that adequate controls are in place to mitigate potential risks. A security audit provides insights into the effectiveness of existing policies and helps organizations to identify areas for improvement, ultimately strengthening their security framework. The other options do not align with the main objective of a security audit. Assessing the aesthetic of IT systems, implementing new hardware solutions, and analyzing software performance are important activities in their own right but do not focus specifically on evaluating the effectiveness and compliance of security measures within the organization.

2. What does "white-hat hacking" refer to?

A. Ethical hacking performed to improve security by identifying vulnerabilities

B. Illegal hacking for personal gain

C. A certification for cybersecurity professionals

D. A type of malware that exploits system vulnerabilities

White-hat hacking refers to ethical hacking conducted with the intent to improve an organization's overall security posture. White-hat hackers are cybersecurity professionals who use their skills and knowledge to find and fix vulnerabilities in systems, networks, and applications before malicious hackers can exploit them. This proactive approach helps organizations strengthen their defenses against potential cyberattacks. The practice of white-hat hacking is crucial in maintaining cybersecurity standards, as it provides insights into security weaknesses and enables businesses to implement the necessary measures to safeguard sensitive data. This form of hacking is performed in compliance with laws and regulations, and often involves obtaining permission from the organization being tested. Other options describe different aspects of cybersecurity, such as illegal hacking or malware, which are distinct from the ethical intent behind white-hat hacking. Thus, the focus on improving security through vulnerability identification solidifies A as the correct answer.

SAMPLE

3. In cybersecurity, what does the term "data breach" typically refer to?

A. Unencrypted data being accessed by unauthorized persons

B. Data stored on a cloud server

C. A physical loss of hardware

D. A software update failing

The term "data breach" typically refers to a situation where unencrypted data is accessed by unauthorized individuals. This definition highlights the fundamental aspect of a data breach, which involves a compromise of confidential information. When data is unencrypted, it is in a format that is not protected by encryption algorithms, making it easier for malicious actors to access and misuse sensitive information. The focus on unencrypted data underscores the importance of implementing strong encryption practices to safeguard information against unauthorized access. In a breach scenario, the consequences can include identity theft, financial loss, and reputational damage for organizations and individuals alike. Recognizing the significance of this aspect helps emphasize the need for robust cybersecurity measures to protect data integrity and confidentiality. Other options do not encapsulate the essence of what constitutes a data breach. For instance, data stored on a cloud server does not inherently imply a breach has occurred, nor does a physical loss of hardware or a software update failure signify unauthorized access to sensitive information. The core of a data breach is the unauthorized access to data, particularly when it is not adequately protected.

4. What occurs after the baseline is updated in Threatlocker?

A. Policies are deleted

B. It conducts its first learning based on found data

C. It automatically reinstalls all applications

D. It no longer monitors applications

When the baseline is updated in Threatlocker, the system conducts its first learning based on the data that it has gathered. This process is crucial as it allows the Threatlocker platform to recognize and categorize applications, setting a foundation for how those applications will be monitored and controlled in the future. Updating the baseline effectively means that Threatlocker can now better understand what is considered normal behavior for the applications that are allowed to run in your environment. It takes into account any changes in the application's activity or new applications since the last baseline was established. This learning phase helps to ensure that the security measures are adaptive and relevant to the current state of the systems being protected. The other options relate to false assumptions about the baseline update process. For instance, policies are not deleted, applications are not automatically reinstated, and monitoring of applications continues after the update, allowing for consistent oversight of application behavior.

SAMPLE

5. What is "threat intelligence"?

A. Information that helps organizations understand potential cyber threats

B. A method of improving network speed

C. A type of firewall protection

D. A software used for data encryption

Threat intelligence refers to the information that organizations gather and analyze to understand potential and existing cyber threats. This encompasses insights into hacker tactics, techniques, and procedures, as well as knowledge about vulnerabilities that could be exploited. By utilizing threat intelligence, organizations can enhance their defensive strategies, anticipate possible attacks, and respond effectively to security incidents. This proactive approach allows businesses to adapt their cybersecurity measures based on the evolving threat landscape. The other choices do not align with the definition of threat intelligence. Improving network speed pertains to performance optimization rather than security threats. Firewall protection relates specifically to establishing barriers against unauthorized access, while data encryption is focused on securing data through obfuscation. Thus, only the first option accurately describes what threat intelligence encompasses in the context of cybersecurity.

6. What happens when new computers are added with continuous deployment?

A. They will need manual software installation

B. They will automatically get ThreatLocker deployed

C. They will require configuration settings

D. They will be marked as incomplete installations

When new computers are added in an environment with continuous deployment, they typically receive automatic configuration and software deployments, which is a cornerstone of the continuous deployment process. This ensures that any new machines will be provisioned with the necessary security measures and software without requiring manual intervention. In this case, ThreatLocker, known for its application whitelisting and zero-trust security approach, would be deployed automatically to maintain a consistent security posture across all devices within the network. Automated deployments help streamline the process and ensure that new computers meet the organization's security and operational standards right from the start. Other responses hint at procedures that may occur in different deployment contexts. For example, manual software installation and requiring configuration settings may be necessary in more traditional or less automated environments. Marking installations as incomplete could occur if there are failed deployments, indicating an issue rather than a feature of continuous deployment. However, in a well-configured continuous deployment setup, ensuring that new machines automatically receive the necessary software, like ThreatLocker, aligns with the goals of rapid, reliable, and secure deployments.

SAMPLE

7. During the automatic learning period, which folders will applications not be profiled unless matched to an application name?

A. Program Files and Windows Directory

B. Documents, Downloads, Desktop, Users, and Root of C:\

C. App Data and Temporary folders

D. Network shares and WinSxS folder

The correct option identifies the folders that applications generally won't be profiled during the automatic learning period unless there is a specific match to an application name. The rationale behind this is rooted in the behavior of many operating systems, which treat certain user data directories, like Documents, Downloads, Desktop, Users, and the Root of C:\, differently from system-critical directories or application-specific directories. During the automatic learning phase, applications are focused on identifying configurations and behaviors primarily associated with system-level operations and applications rather than user-generated content or personal files. This means that folders often used for storing user files are typically excluded from automatic profiling unless those files are specifically linked to recognized applications. As a result, any executable or program-related data stored in these user folders may not be automatically tracked, requiring a defined match to an application name to include them in profiling activities. Understanding this is crucial for effective application management and ensuring that security measures are accurately applied to the right components within the operating environment.

8. When elevating a policy, what is crucial to consider?

A. Allow interaction with all applications

B. Block interaction with all other applications, unless necessary

C. Set only a few applications to run

D. Keep applications unmonitored

When elevating a policy, it is crucial to block interaction with all other applications unless necessary. This approach is essential for maintaining security and minimizing vulnerabilities. By restricting application interactions, you reduce the attack surface that could be exploited by malicious actors. This principle aligns with the concept of least privilege, which suggests that applications and users should only have the minimum access necessary to perform their functions. This significantly reduces the risk of unauthorized access and potential infiltration into the system, ensuring that even if one application is compromised, it cannot easily affect others or the overall security posture of the environment.

SAMPLE

9. Which of the following best describes the role of a SIEM system?

A. To provide antivirus protection

B. To aggregate and analyze security data

C. To facilitate network speed enhancements

D. To backup critical data regularly

A Security Information and Event Management (SIEM) system plays a crucial role in cybersecurity by aggregating and analyzing security data from various sources within an organization's IT infrastructure. This includes log data from servers, network devices, and security appliances, as well as event information from various applications. The primary function of a SIEM system is to provide real-time analysis of security alerts generated by applications and network hardware. By correlating different types of events and data points, a SIEM can identify potential security threats, detect anomalies, and assist in responding to incidents more effectively. In contrast, antivirus protection focuses specifically on detecting and mitigating malware; enhancing network speed pertains to improving the performance of data transmission; and backing up critical data regularly is aimed at data recovery and integrity rather than security analysis. Therefore, the role of a SIEM system is accurately described by its capacity to aggregate and analyze security data for improved monitoring and incident response.

10. Which element is an important part of employee training in security awareness?

A. Time management techniques

B. Effective communication practices

C. Awareness of evolving cyber threats

D. Knowledge of financial planning

Awareness of evolving cyber threats is indeed a crucial element of employee training in security awareness because it helps employees recognize and understand the various types of threats that can affect the organization. Cyber threats continuously evolve, with attackers developing more sophisticated methods to infiltrate systems and exploit vulnerabilities. By educating employees about the current landscape of cyber threats, organizations empower them to identify suspicious activities, safeguard sensitive information, and understand the implications of their actions in the digital environment. This awareness is vital for building a strong security culture within the organization, as employees are often the first line of defense against potential breaches. Without this knowledge, employees may inadvertently expose the organization to risks, making it essential for them to stay informed about the latest trends and tactics used by cybercriminals. While time management techniques, effective communication practices, and knowledge of financial planning are valuable skills for employees, they do not directly enhance the understanding needed to mitigate cyber threats, which places a significant emphasis on the importance of security awareness training.

SAMPLE

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://cyberherocert.examzify.com

We wish you the very best on your exam journey. You've got this!

SAMPLE