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 15

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 does the acronym "VPN" stand for?

A. Virtual Public Network

B. Virtual Private Network

C. Vulnerable Point Neutralizer

D. Variable Protocol Node

2. What does ThreatLocker use to profile drivers?

A. The name of the driver

B. The version number of the driver

C. The hash of the file

D. The size of the driver file

3. What happens when you click the Remove Unused Policy button?

A. All policies are immediately deleted

B. You can select a date to remove unused policies

C. You receive a summary of all policies

D. Unused policies are archived for later review

4. By default, what channel is an organization on when new versions of TL are released?

A. Beta update channel

B. Test update channel

C. Regular update channel

D. Premium update channel

5. When deploying through command prompt with the stub installer, what are valid switches that can be used?

A. group name, company, and key

B. user name, project name, and key

C. account name, department, and key

D. group name, identifier, and key

SAMPLE

6. What does a digital signature ensure regarding a document?

A. It reduces file size

B. It simplifies document sharing

C. It prevents unauthorized alterations

D. It enhances color quality

7. What is the maximum allowed time for user login inactivity?

A. One hour

B. Three hours

C. Two hours

D. Five hours

8. Can a specific port number be assigned to a tag in a policy?

A. Yes, tags can specify port numbers

B. No, tags cannot specify port numbers

C. Port numbers are included as part of the tag name

D. Only certain protocols allow port specification

9. What does the threatlocker agent do at the kernel level?

A. It installs necessary updates

B. It enhances network performance

C. It stops various threats and malware

D. It manages user permissions

10. What does the acronym "SSL" stand for?

A. Standard Secure Layer

B. Secure Sockets Layer

C. Safety Security Logs

D. Simple Sign-On Layer

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What does the acronym "VPN" stand for?

A. Virtual Public Network

B. Virtual Private Network

C. Vulnerable Point Neutralizer

D. Variable Protocol Node

The acronym "VPN" stands for Virtual Private Network. This terminology is fundamental in cybersecurity and networking as it describes a technology that creates a secure connection over a less secure network, such as the internet. A VPN allows users to send their data securely by establishing an encrypted tunnel between their devices and the VPN server. This way, sensitive information remains private and protected from potential intruders. Using a VPN is particularly important for maintaining privacy while using public Wi-Fi networks, as it helps to protect against unauthorized access to personal data. The technology is also used to circumvent geographical restrictions and maintain anonymity online, adding another layer of security for users. The other options do not accurately reflect the established definition of VPN within cyber security and networking contexts. While they may sound plausible, they do not correspond to the widely accepted terminology used in the industry.

2. What does ThreatLocker use to profile drivers?

A. The name of the driver

B. The version number of the driver

C. The hash of the file

D. The size of the driver file

ThreatLocker uses the hash of the file to profile drivers because file hashing is a reliable method of ensuring file integrity and authenticity. A hash function generates a unique string of characters (the hash) based on the contents of the file. This means even a slight change in the file will result in a completely different hash value. By using hashes, ThreatLocker can accurately identify and manage drivers, distinguishing between safe and potentially harmful software. This approach provides a strong defense against malicious modifications or tampering, as it is based on an unalterable representation of the file's data. In comparison, factors such as the name or version number of the driver may not be unique or could be easily spoofed, while the size of the driver file does not sufficiently account for the content's integrity. Thus, relying on the hash of the file ensures a more robust and secure method for profiling drivers.

3. What happens when you click the Remove Unused Policy button?

A. All policies are immediately deleted

B. You can select a date to remove unused policies

C. You receive a summary of all policies

D. Unused policies are archived for later review

When you click the Remove Unused Policy button, the correct outcome is that you have the option to select a date to remove unused policies. This function allows administrators to manage their policies effectively by ensuring that only those that are actively in use are retained. By setting a specific date, it gives the user control over the timeline of policy management, which can help in maintaining a clean and organized policy framework. This process facilitates an efficient cleanup of policies that are no longer needed without the risk of accidentally deleting those that might still serve a purpose. In contrast, the other options suggest more drastic or less controlled outcomes, such as the immediate deletion of all policies, or merely receiving a summary of policies without taking action. Archiving unused policies for later review implies a preservation rather than removal, which does not align with the intent of the button. Effective policy management requires careful consideration of what is active versus obsolete, and the ability to set a date for removal helps to balance that need.

SAMPLE

4. By default, what channel is an organization on when new versions of TL are released?

A. Beta update channel

B. Test update channel

C. Regular update channel

D. Premium update channel

When a new version of technology or software is released, organizations typically default to the regular update channel. This channel provides a stable and tested version of the software that is deemed suitable for most users and environments, ensuring that organizations have access to the latest features and security updates without the additional risks associated with less stable versions. The regular update channel is designed for wide deployment, offering a good balance of new functionality and reliability. It allows organizations to ensure that they are not exposed to the potential bugs and issues that can arise during beta or test phases of software releases, which are intended mainly for feedback and bug identification rather than widespread use. This approach helps maintain operational stability and security across the organization while still keeping software up-to-date, reflecting the best practices in software lifecycle management.

5. When deploying through command prompt with the stub installer, what are valid switches that can be used?

A. group name, company, and key

B. user name, project name, and key

C. account name, department, and key

D. group name, identifier, and key

The correct answer is based on understanding the purpose and functionality of the command line interface when using a stub installer for deployment. In this context, the valid switches that can be used during deployment specifically include the group name, company, and key. The group name is essential as it categorizes the deployment under a specific group, allowing for organized management of resources and installations. The company switch helps associate the deployment with the relevant organization, which can be crucial for licensing and support purposes. Lastly, the key switch typically refers to a license key or a unique identifier that authorizes the installation, ensuring that only legitimate users can execute the deployment. The other options include combinations of terms that do not match the expected functionality of a stub installer in a deployment scenario or include terms that are not standard within this context. Understanding the specific terminology and their implication in the deployment process is key to identifying the correct choice.

6. What does a digital signature ensure regarding a document?

A. It reduces file size

B. It simplifies document sharing

C. It prevents unauthorized alterations

D. It enhances color quality

A digital signature serves a critical role in ensuring the integrity and authenticity of a document. By creating a unique digital fingerprint of the document using cryptographic techniques, a digital signature guarantees that any alterations made to the document after it has been signed can be detected. This means that if someone attempts to change the content of a digitally signed document, the signature will no longer be valid, alerting the recipient to potential tampering. The main purpose of a digital signature is to provide assurance that the document has not been altered since it was signed, thereby preventing unauthorized modifications. This is particularly important in legal, financial, and other sensitive communications where the accuracy and authenticity of information are paramount.

SAMPLE

7. What is the maximum allowed time for user login inactivity?

A. One hour

B. Three hours

C. Two hours

D. Five hours

The correct answer reflects common security best practices regarding user session management. Limiting the maximum allowed time for user login inactivity to two hours is a widely accepted guideline designed to mitigate potential security risks. Keeping a session active for too long without user interaction increases the likelihood of unauthorized access, especially in public or shared environments. By setting a two-hour inactivity timeout, organizations can effectively reduce the window of opportunity for malicious actors to exploit idle sessions. This time frame balances user convenience with security needs, ensuring that users have enough time to return to their sessions while still maintaining an added layer of protection against unauthorized access. Organizations may choose different timeouts based on their specific security requirements, but two hours is a standard measure that aligns with many regulatory and compliance guidelines.

8. Can a specific port number be assigned to a tag in a policy?

A. Yes, tags can specify port numbers

B. No, tags cannot specify port numbers

C. Port numbers are included as part of the tag name

D. Only certain protocols allow port specification

In the context of cybersecurity policies, tags are generally used for categorizing or labeling resources, such as network traffic, devices, or security rules. Tags are intended to convey metadata and help with organization, classification, and identification purposes. The reason why the assertion that tags cannot specify port numbers is accurate stems from the fundamental function of tags in policy settings. Tags are typically abstract identifiers that allow users to group items based on attributes; however, they do not carry specific technical parameters like port numbers. Instead, ports are usually addressed in a different part of the policy configuration where actual network behavior is defined, such as in access control lists (ACLs) or firewall rules. This distinction clarifies that while network policies will often involve port numbers for actual communication protocols, tags themselves remain a high-level organizational tool without granular specifications such as port assignments. Thus, the correct interpretation of the role of tags in policy does not extend to the direct assignment of port numbers.

SAMPLE

9. What does the threatlocker agent do at the kernel level?

A. It installs necessary updates

B. It enhances network performance

C. It stops various threats and malware

D. It manages user permissions

The correct choice focuses on the primary function of the ThreatLocker agent at the kernel level, which is to stop various threats and malware. At this level, the agent operates with high privileges, allowing it to monitor and control system activities more effectively than applications with less privilege. This capability is critical for identifying and blocking malicious behavior before it can impact the system's integrity or data security. Kernel-level operations provide a robust layer of defense, as the agent can detect malicious processes, lock down unauthorized changes, and ensure that threat actors cannot exploit vulnerabilities within the operating system. This proactive stance is essential in a security architecture, as it creates barriers against potential exploits that are often present in software running in user mode. The other options relate to functions that are outside the scope of what a ThreatLocker agent does at the kernel level. While updating software and managing permissions are important for overall security management, they do not define the specific role attributed to the ThreatLocker agent in stopping threats and malware directly. Enhancing network performance, too, is important in cybersecurity but does not align with the primary focus of the ThreatLocker agent's functionalities at the kernel level.

10. What does the acronym "SSL" stand for?

A. Standard Secure Layer

B. Secure Sockets Layer

C. Safety Security Logs

D. Simple Sign-On Layer

The acronym "SSL" stands for Secure Sockets Layer. This is a standard security technology used to establish an encrypted link between a server and a client, typically a web server and a browser. SSL ensures that all data transmitted between these two entities remains private and secure. When SSL is implemented, it provides authentication for the server and allows secure transmission of data, which helps protect sensitive information such as credit card numbers, login credentials, and personal data from being intercepted during transmission. Understanding the significance of SSL is vital in the context of cybersecurity because it plays a crucial role in safeguarding communications over the internet. As technology evolved, SSL has largely been succeeded by Transport Layer Security (TLS), but the term SSL is still widely used to refer to both protocols in general discussions about internet security.

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