JASON DION SECURITY+ COURSE PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://dionsecurityplus.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 does grayware refer to?

A. Malicious software that encrypts files

B. Software that is neither benign nor malicious

C. A tool for remote access by attackers

D. Software that gathers information without consent

2. What is the primary purpose of the CIA triad in cybersecurity?

A. To ensure confidentiality, integrity, and availability of information

B. To provide network segmentation and firewalls

C. To implement antivirus software

D. To secure physical locations

3. What is the purpose of data encryption?

A. To speed up data transmission

B. To prevent unauthorized access to information

C. To facilitate data recovery

D. To enhance the visual presentation of data

4. Which term refers to the practice of using multiple servers to handle increased loads?

A. Server partitioning

B. Load balancing

C. Server mirroring

D. Traffic shaping

5. In which layer of the OSI model does encryption primarily occur?

A. Network layer

B. Transport layer

C. Application layer

D. Presentation layer

6. What primary function do Network Attached Storage (NAS) devices serve?

A. They perform data analysis for databases

B. They connect directly to a network for data storage

C. They transmit data securely over the internet

D. They provide power backup to computers

SAMPLE

7. Which concept involves restricting access to information based on the principle of least privilege?

A. Role-Based Access Control

B. Mandatory Access Control

C. Discretionary Access Control

D. Network Access Control

8. Which of the following is a common security framework used in information security?

A. ISO 27001

B. HIPAA

C. PCI-DSS

D. All of the above

9. How can organizations reinforce security policies with employees?

A. By limiting their access to information

B. By providing regular training and updates

C. By increasing workloads

D. By avoiding communication about security

10. What is the first step in the Five Steps to Authentication?

A. Something you do

B. Something you know

C. Something you are

D. Something you have

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What does grayware refer to?

A. Malicious software that encrypts files

B. Software that is neither benign nor malicious

C. A tool for remote access by attackers

D. Software that gathers information without consent

Grayware refers to software that exists in the gray area between benign and malicious applications. It does not fall neatly into categories of either safe software or outright malware. Instead, grayware includes programs that may exhibit undesirable behavior but are not harmful or malicious in nature, such as adware or potentially unwanted programs (PUPs). These applications can slow down systems, display unwanted ads, or lead to a poor user experience without being overtly threatening like traditional malware. This definition helps clarify grayware's role in cybersecurity, as it often requires careful consideration and management, as it may not be outright harmful but can still pose risks to user privacy and system performance. Understanding this distinction is crucial for cybersecurity professionals when assessing applications and their potential effects on systems.

2. What is the primary purpose of the CIA triad in cybersecurity?

A. To ensure confidentiality, integrity, and availability of information

B. To provide network segmentation and firewalls

C. To implement antivirus software

D. To secure physical locations

The primary purpose of the CIA triad in cybersecurity is to ensure the confidentiality, integrity, and availability of information. Each component of the triad addresses a fundamental aspect of information security. Confidentiality ensures that sensitive information is accessed only by authorized individuals, preventing unauthorized exposure or data breaches. Integrity maintains the accuracy and reliability of data, ensuring that it cannot be altered or tampered with by unauthorized users. Availability ensures that information and resources are accessible to authorized users when needed, minimizing downtime and disruptions to services. While other choices address security measures, they do not encompass the foundational principles of information security that the CIA triad represents. Network segmentation and firewalls enhance security but do not fundamentally relate to the management of information itself like the triad does. Antivirus software is a tool used to protect systems from malware but does not cover the broader aspects included in the CIA triad. Securing physical locations is important for overall security but is not specifically tied to the management of information in the context of the CIA triad.

3. What is the purpose of data encryption?

A. To speed up data transmission

B. To prevent unauthorized access to information

C. To facilitate data recovery

D. To enhance the visual presentation of data

The purpose of data encryption primarily revolves around securing information by transforming it into a format that is unreadable to anyone who does not possess the correct decryption key. This process protects sensitive data from unauthorized access, ensuring that even if data is intercepted or accessed by malicious entities, it remains confidential and infeasible for them to understand or utilize. By encrypting data, organizations can maintain confidentiality regarding sensitive information, such as personal identification data, financial details, or proprietary business information. This level of security is essential in countless scenarios, including online transactions, communications, and data storage, where the risk of unauthorized access is significant. While other options touch on important aspects of data handling—such as data recovery or improved transmission speeds—these do not address the central aim of encryption, which is to safeguard information from being accessed or discerned without proper authorization.

SAMPLE

4. Which term refers to the practice of using multiple servers to handle increased loads?

A. Server partitioning

B. Load balancing

C. Server mirroring

D. Traffic shaping

Load balancing is the correct term that refers to the practice of distributing incoming network traffic across multiple servers to ensure that no single server becomes overwhelmed with too much load. This technique enhances the availability and reliability of applications by optimizing resource use, maximizing throughput, minimizing response time, and avoiding overload of any single server. By spreading the workload evenly, load balancing helps maintain performance levels even during peak usage times. In contrast, server partitioning involves dividing a server's resources into smaller, isolated units, which is not primarily focused on distributing traffic but rather on resource allocation within a single server. Server mirroring entails creating a duplicate of a server to offer redundancy and ensure data availability but does not directly address the distribution of incoming traffic. Traffic shaping involves controlling the flow of data to ensure that bandwidth is used efficiently but does not inherently involve the use of multiple servers for managing load. Thus, load balancing is specifically tailored to manage increased workloads across multiple servers effectively.

5. In which layer of the OSI model does encryption primarily occur?

A. Network layer

B. Transport layer

C. Application layer

D. Presentation layer

Encryption primarily occurs in the presentation layer of the OSI model. This layer is responsible for translating data between the application layer and the lower layers, including formatting, encryption, and compression. When data is prepared for transmission or stored, encryption can be applied to secure it, ensuring that sensitive information is protected from unauthorized access during transmission. The presentation layer also deals with data representation, which includes converting data formats and handling character encoding. Since it sits above the session layer and below the application layer, it acts as an intermediary that can implement encryption mechanisms to secure user data before it is processed by applications or sent over the network. While encryption can also be utilized at other layers, like the transport layer (such as TLS/SSL for secure communications), the core function of data encryption itself aligns with the roles and responsibilities of the presentation layer as it directly handles the formatting and security of data being sent or received by applications. This is why the presentation layer is recognized as the primary layer for encryption in the context of the OSI model.

SAMPLE

6. What primary function do Network Attached Storage (NAS) devices serve?

A. They perform data analysis for databases

B. They connect directly to a network for data storage

C. They transmit data securely over the internet

D. They provide power backup to computers

Network Attached Storage (NAS) devices primarily serve the function of connecting directly to a network for data storage. This allows multiple users and devices across the network to access files and data stored on the NAS efficiently. NAS systems provide a centralized location for storing data, which simplifies file sharing, backup, and access management in both home and business environments. Additionally, because they are networked, NAS devices often come equipped with their own operating systems and software to manage storage, user permissions, and sometimes even perform tasks such as media streaming. By offering such features, NAS plays an important role in enhancing data accessibility and collaboration, making it a vital component of modern networked environments.

7. Which concept involves restricting access to information based on the principle of least privilege?

A. Role-Based Access Control

B. Mandatory Access Control

C. Discretionary Access Control

D. Network Access Control

The principle of least privilege is a security concept that dictates that individuals should only have access to the information and resources that are necessary for them to perform their job functions. This minimizes the risk of unauthorized access or potential data breaches. Role-Based Access Control (RBAC) is directly aligned with this principle because it assigns permissions to users based on their role within the organization. By establishing roles—such as administrator, manager, or employee—RBAC ensures that users have only the permissions necessary for their role. For example, an employee in a financial department may have access to sensitive financial data, while someone in human resources may not have that same level of access, thereby adhering to the least privilege principle. The other concepts, while they may involve access control, do not specifically implement the least privilege principle to the same degree as RBAC does. Mandatory Access Control assigns access based on predetermined policies, which may not consider individual job roles. Discretionary Access Control allows users to determine who can access their resources, potentially leading to excessive permissions. Network Access Control focuses on managing device access to a network rather than how users access specific information. Thus, Role-Based Access Control is the most accurate answer in relation to the principle of least privilege.

SAMPLE

8. Which of the following is a common security framework used in information security?

A. ISO 27001

B. HIPAA

C. PCI-DSS

D. All of the above

The correct choice is that all of these frameworks are indeed commonly referenced in the context of information security, but it is important to understand their individual roles and how they fit within the larger framework of security compliance. ISO 27001 is an international standard for information security management systems (ISMS) and provides a systematic approach to managing sensitive company information to keep it secure. It is a flexible framework applicable to organizations of any size and in any industry, focused on establishing, implementing, maintaining, and continually improving a risk management process. HIPAA, the Health Insurance Portability and Accountability Act, is specifically designed for the healthcare sector in the United States, establishing requirements for protecting sensitive patient information. It lays out standards for the privacy and security of health information, making it critical for healthcare organizations to comply with to safeguard patient data. PCI-DSS, the Payment Card Industry Data Security Standard, is applicable to organizations that handle credit cards and other payment information. This framework helps to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment, emphasizing the protection of cardholder data to prevent fraud and data breaches. Each of these frameworks serves a unique purpose and audience, but they are all widely used in the field of information

9. How can organizations reinforce security policies with employees?

A. By limiting their access to information

B. By providing regular training and updates

C. By increasing workloads

D. By avoiding communication about security

Providing regular training and updates is a fundamental approach for organizations to reinforce security policies among employees. This method ensures that personnel are not only aware of existing policies but also understand the rationale behind them, the importance of compliance, and any updates or changes. Regular training sessions help build a culture of security awareness and encourage proactive behavior toward safeguarding sensitive information. Through ongoing education, employees can stay informed about the latest threats, vulnerabilities, and best practices in cybersecurity. This equips them to recognize potential security risks and respond appropriately. By embedding this knowledge into the workplace, organizations can foster an environment where security is prioritized, ultimately leading to a stronger overall security posture. Other options, while they may seem relevant in specific contexts, do not effectively reinforce security policies in the same way. Limiting access to information can result in frustration or resistance if employees do not understand why those limits are in place. Increasing workloads may lead to burnout and reduced attention to security measures, while avoiding communication about security creates a lack of awareness, making employees less vigilant. Regular training and communication are vital for ensuring that everyone is aligned with security objectives.

SAMPLE

10. What is the first step in the Five Steps to Authentication?

A. Something you do

B. Something you know

C. Something you are

D. Something you have

The first step in the Five Steps to Authentication is "Something you know." This foundational concept revolves around the use of knowledge-based factors for verifying identity, such as passwords or personal identification numbers (PINs). Authentication's essence is about ensuring that a user is who they claim to be, and using information that the user knows allows systems to establish a baseline of trust. This method is prevalent in online services where users create accounts protected by passwords as a primary security measure. Once this initial knowledge-based step is established, other factors can come into play, such as biometric methods (something you are), physical tokens (something you have), or behavioral patterns (something you do) to enhance security further. However, starting with "something you know" sets the stage for initiating secure access procedures and establishing user identity.

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://dionsecurityplus.examzify.com

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

SAMPLE