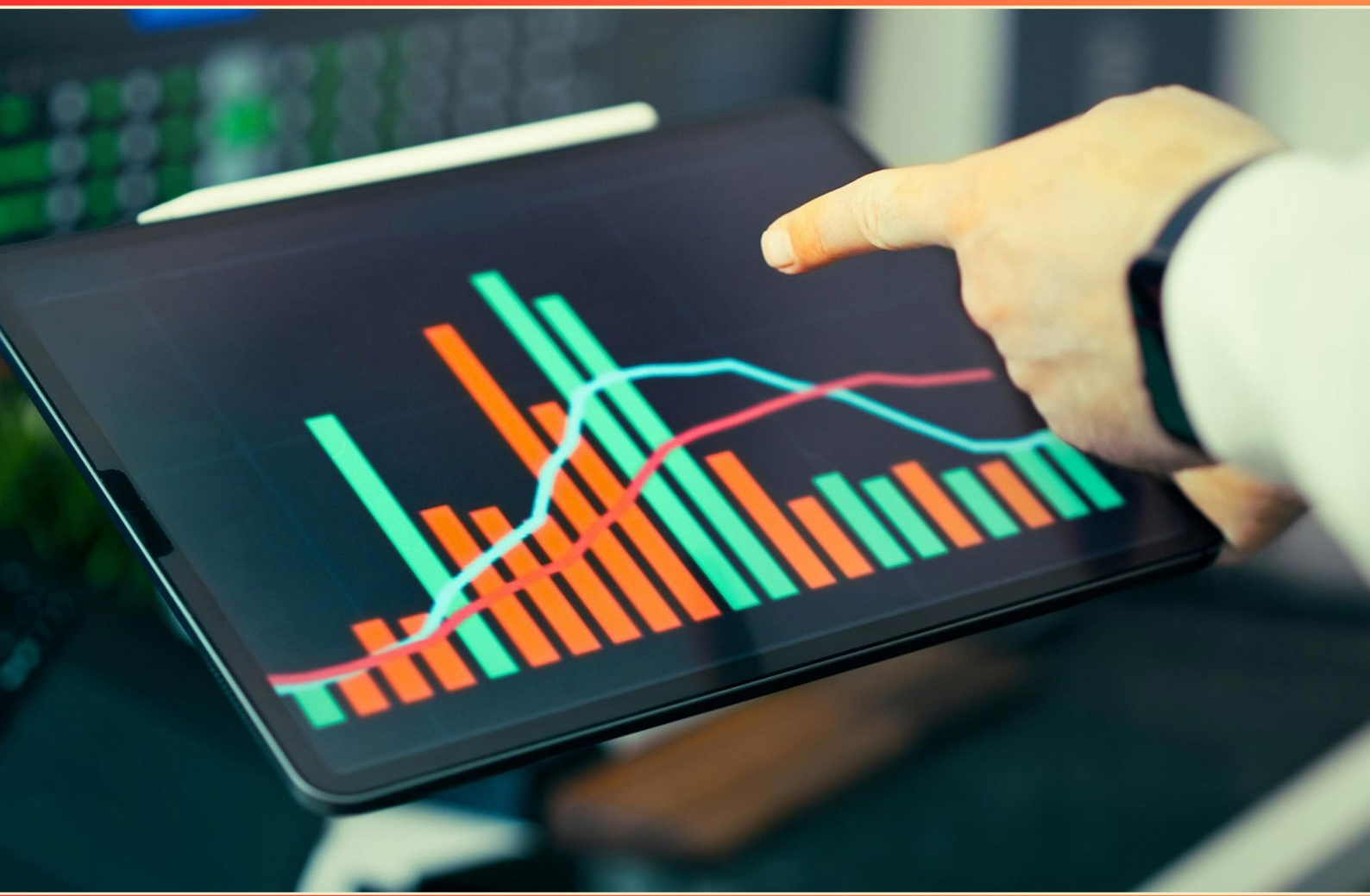
GIAC CLOUD SECURITY AUTOMATION PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://giaccloudsecurityautomation.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 main purpose of logging in cloud security?

A. To improve user experience

B. To maintain a record of system changes

C. To enhance network performance

D. To ensure exclusive access to sensitive data

2. Which mode in terraform WAF policy is primarily concerned with blocking traffic?

A. Alert

B. Warning

C. Monitoring

D. Prevention

3. What outcomes should security controls aim to achieve in cloud computing?

A. Maximize revenue for the provider

B. Minimize user inconvenience

C. Ensure compliance and mitigate risks

D. Enhance the aesthetic of user interfaces

4. What aspect of cloud security do CIS benchmarks typically address?

A. Network traffic analysis

B. Configuration and hardening of systems

C. User training and awareness

D. Application performance optimization

5. What type of attack does a Security Orchestration, Automation, and Response (SOAR) tool specifically target?

A. Denial of Service Attacks

B. Phishing Attacks

C. Malware Infections

D. Rapid response to security incidents through automated workflows

SAMPLE

6. What does logging with IAM permissions NOT control?

A. Access rights to view logs

B. Turning logging functions on or off

C. Audit trail for access

D. Encryption standards for logs

7. Which of the following is NOT a function of AWS Lambda resource policies?

A. Granting permissions to services

B. Managing function execution times

C. Enabling cross-account resource access

D. Allowing external applications to invoke functions

8. What are security controls in the context of cloud computing?

A. Policies that restrict user access

B. Mechanisms or practices that mitigate risks

C. Standards for cloud service pricing

D. Protocols for data transfer

9. What is the mode associated with a terraform WAF policy that has a score of 5?

A. Prevention

B. Warning

C. Block

D. Monitoring

10. What is a cloud security incident?

A. An event that improves system performance

B. An event that compromises the confidentiality, integrity, or availability of cloud data or services

C. An occurrence that only affects virtual machines

D. A routine check of system security settings

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the main purpose of logging in cloud security?

A. To improve user experience

B. To maintain a record of system changes

C. To enhance network performance

D. To ensure exclusive access to sensitive data

The main purpose of logging in cloud security is to maintain a record of system changes. Logging serves as a critical function for security, providing an audit trail of activities and events that occur within a system. This includes tracking modifications to systems, applications, and configurations, which can help detect unauthorized changes or actions that may indicate a security incident. By recording comprehensive logs, organizations can analyze security events, identify vulnerabilities, and respond to incidents more effectively. The data captured through logs can also assist in compliance with regulatory requirements and internal policies by providing evidence of actions taken within the environment. While improving user experience, enhancing network performance, and ensuring exclusive access to sensitive data are all important aspects of cloud operations, they do not encapsulate the primary role of logging in cloud security, which is fundamentally about accountability, traceability, and security incident management.

2. Which mode in terraform WAF policy is primarily concerned with blocking traffic?

A. Alert

B. Warning

C. Monitoring

D. Prevention

The mode in a Terraform Web Application Firewall (WAF) policy that is primarily focused on blocking traffic is the prevention mode. When a WAF is configured in prevention mode, it actively filters and blocks potentially harmful requests before they reach the web application. This is a critical feature in protecting applications from various types of attacks, such as SQL injection, cross-site scripting (XSS), and other malicious activities. In this mode, the WAF doesn't just alert or log suspicious activity; it takes action by denying the traffic that meets certain attack criteria defined in its ruleset. This proactive approach is essential for maintaining the security posture of web applications, especially in environments where sensitive data is handled or where compliance with security regulations is necessary. Overall, prevention mode serves as a defensive layer, reducing the risk of exploitations and ensuring that applications can operate securely. The other modes, while useful for monitoring and warning purposes, do not actively block traffic, which is the primary function of prevention mode.

SAMPLE

3. What outcomes should security controls aim to achieve in cloud computing?

A. Maximize revenue for the provider

B. Minimize user inconvenience

C. Ensure compliance and mitigate risks

D. Enhance the aesthetic of user interfaces

Security controls in cloud computing are critical to affirming the integrity and confidentiality of data, as well as ensuring that any existing regulatory requirements are met. The primary objective of security controls should focus on ensuring compliance with relevant standards and frameworks, while also effectively mitigating risks associated with data breaches, unauthorized access, and other security threats. By incorporating comprehensive security controls, organizations not only protect their own assets but also maintain trust with their customers and stakeholders. Compliance with regulations such as GDPR, HIPAA, or PCI DSS is essential for organizations operating in various industries, as non-compliance can lead to severe financial penalties and reputational damage. While user convenience is important, and fostering revenue for the provider may benefit certain aspects of the service, these aspects are secondary to the overarching need for robust risk management and regulatory compliance in the cloud environment. Aesthetics, though they can enhance user experience, do not contribute to the security stance of the cloud services being utilized. Therefore, the focus must be on ensuring compliance and mitigating risks as the primary outcomes that security controls should aim to achieve.

4. What aspect of cloud security do CIS benchmarks typically address?

A. Network traffic analysis

B. Configuration and hardening of systems

C. User training and awareness

D. Application performance optimization

CIS benchmarks primarily focus on the configuration and hardening of systems, which is essential in maintaining cloud security. These benchmarks provide a set of best practices and guidelines for securing various systems and technologies. By following these recommendations, organizations can minimize vulnerabilities and reduce the risk of security breaches. This includes specifying secure configuration settings, default password changes, and system-specific hardening techniques for various environments such as cloud services, operating systems, and applications. In contrast, the other options do not align with the core purpose of CIS benchmarks. Network traffic analysis relates to monitoring and handling data flows rather than system configuration. User training and awareness emphasize the human factor in security but are outside the scope of technical benchmarks. Application performance optimization focuses on improving application efficiency rather than security hardening practices. Thus, the option that correctly identifies the primary area that CIS benchmarks address is indeed the configuration and hardening of systems.

SAMPLE

5. What type of attack does a Security Orchestration, Automation, and Response (SOAR) tool specifically target?

A. Denial of Service Attacks

B. Phishing Attacks

C. Malware Infections

D. Rapid response to security incidents through automated workflows

A Security Orchestration, Automation, and Response (SOAR) tool is designed specifically to enhance an organization's ability to respond swiftly and effectively to security incidents through automated workflows. SOAR platforms streamline the incident response process by integrating various security tools and enabling security teams to automate repetitive tasks. This automation allows teams to react quickly to threats, reducing the time it takes to contain and remediate incidents, which is crucial in minimizing potential damage. With the capability to orchestrate responses across different security technologies, SOAR tools facilitate real-time data analysis and decision-making during security events. The focus on rapid incident response is what fundamentally distinguishes SOAR from other tools that may target specific types of attacks, such as denial of service, phishing, or malware infections. Instead of addressing these attacks in isolation, SOAR provides a holistic approach that enhances overall security posture by enabling proactive and automated responses to a wide variety of incidents.

6. What does logging with IAM permissions NOT control?

A. Access rights to view logs

B. Turning logging functions on or off

C. Audit trail for access

D. Encryption standards for logs

When considering what logging with IAM (Identity and Access Management) permissions does not control, it is important to understand the specific aspects of logging and IAM. Choosing the option that indicates it does not control turning logging functions on or off is appropriate because IAM permissions are primarily designed to manage access to resources, including who can view logs and who can access the log data itself. IAM roles and policies determine which users or services can get information about or manipulate log data but do not configure logging features such as enabling or disabling the logging itself. The actual operation of turning logging capabilities on or off is generally handled separately, often through specific service configurations in the cloud platform. Access rights to view logs, the audit trail for access, and encryption standards for logs are all directly influenced by IAM policies. They determine who can see what log data, ensure there is a record of access, and specify how log data is secured. Thus, IAM plays a critical role in managing these areas, while turning logging functions on or off is typically beyond its scope.

SAMPLE

7. Which of the following is NOT a function of AWS Lambda resource policies?

A. Granting permissions to services

B. Managing function execution times

C. Enabling cross-account resource access

D. Allowing external applications to invoke functions

AWS Lambda resource policies focus on the security and access control of Lambda functions, which includes granting the necessary permissions and access rights for various services, users, or applications to interact with those functions. Granting permissions to services enables Lambda functions to be invoked by other AWS services or third-party applications, while enabling cross-account resource access allows different AWS accounts to invoke functions securely. Allowing external applications to invoke functions is a crucial aspect of Lambda resource policies, as it determines which external sources can trigger the functions, ensuring that only authorized entities can invoke them. However, managing function execution times is not a function of AWS Lambda resource policies. Execution times are governed by the configuration settings of the Lambda function itself, where developers can specify timeouts and resource allocation. This aspect focuses more on the operational parameters of executing the function rather than access control, which is central to the purpose of resource policies. Therefore, managing function execution times does not fall under the scope of AWS Lambda resource policies.

8. What are security controls in the context of cloud computing?

A. Policies that restrict user access

B. Mechanisms or practices that mitigate risks

C. Standards for cloud service pricing

D. Protocols for data transfer

In the context of cloud computing, security controls refer to the mechanisms or practices that are put in place to mitigate risks associated with data and system vulnerabilities. These controls are essential as they help to ensure the confidentiality, integrity, and availability of data stored and processed in cloud environments. They can include a wide range of measures, such as encryption, access controls, monitoring, and incident response strategies. By implementing effective security controls, organizations can manage risks more effectively and safeguard their cloud resources against threats such as unauthorized access, data breaches, and service disruptions. While other options touch on related concepts, they do not accurately capture the definition of security controls. Policies that restrict user access relate more specifically to governance and user management rather than the broader scope of security controls. Standards for cloud service pricing focus on the financial aspects of cloud services, which do not pertain to security. Protocols for data transfer, although important for secure data transmission, represent only a subset of security controls rather than the full spectrum of practices dedicated to risk mitigation. Thus, the correct answer emphasizes the overarching role of security controls in comprehensive risk management strategies within cloud computing.

SAMPLE

9. What is the mode associated with a terraform WAF policy that has a score of 5?

A. Prevention

B. Warning

C. Block

D. Monitoring

The mode associated with a Terraform Web Application Firewall (WAF) policy that has a score of 5 is categorized as "Prevention." In the context of WAF policies, scores are typically assigned to indicate the severity of threats or the level of action the WAF should take in response to certain behaviors or requests. A score of 5 indicates a higher level of concern, where immediate action is necessary to protect the application. This means that when a threat reaches this score, the WAF enters a preventive mode, actively blocking malicious traffic that meets certain criteria. In this proactive stance, the WAF not only alerts administrators but also takes steps to prevent potential breaches or attacks from affecting the web application. Understanding the significance of the score system is crucial because it helps organizations prioritize their security measures and allocate resources effectively. In this case, a prevention mode ensures that significant threats are dealt with assertively, helping to maintain the integrity and availability of web applications.

10. What is a cloud security incident?

A. An event that improves system performance

B. An event that compromises the confidentiality, integrity, or availability of cloud data or services

C. An occurrence that only affects virtual machines

D. A routine check of system security settings

A cloud security incident is defined as an event that compromises the confidentiality, integrity, or availability of cloud data or services. This definition encapsulates the key aspects of what constitutes a security incident in a cloud environment. In cloud computing, where data and services are often highly interconnected and accessible over the internet, any situation that leads to unauthorized access, alteration of data, disruption in service, or loss of data can be considered a serious security incident. This may include unauthorized data breaches, service outages due to DDoS attacks, or misconfigurations that expose sensitive information. Recognizing incidents that threaten these three core principles—confidentiality, integrity, and availability—is essential for maintaining a secure cloud environment. Other choices do not accurately capture the essence of a cloud security incident. Events that improve system performance or routine checks of security settings do not relate to a security breach or compromise. An occurrence that only affects virtual machines may not encompass the broader implications of incidents that can affect all aspects of cloud data and services. Thus, the definition that centers around compromising essential security properties is the most accurate.

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://giaccloudsecurityautomation.examzify.com

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

SAMPLE