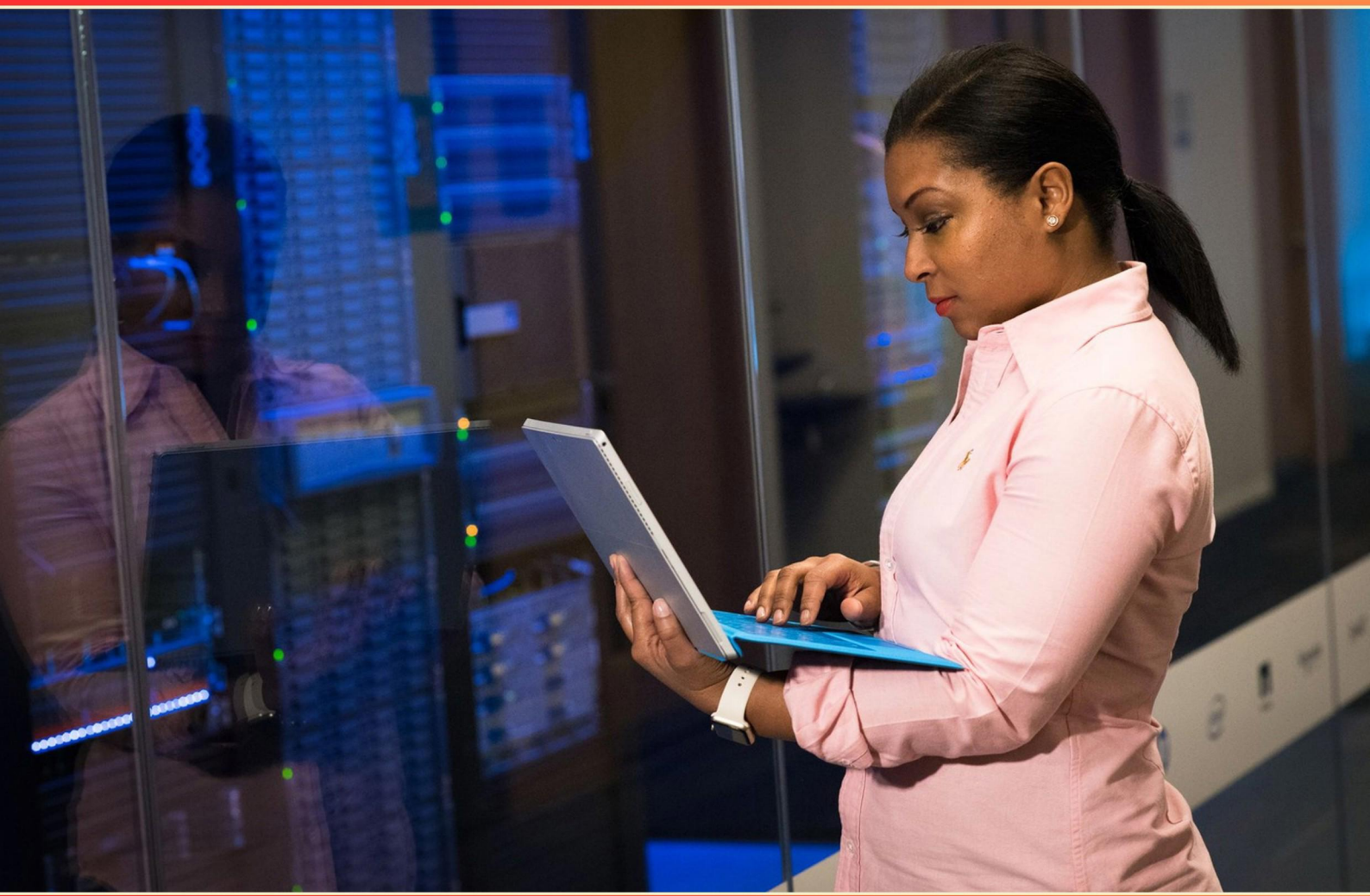
EC-COUNCIL CERTIFIED INCIDENT HANDLER (ECIH) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://eccouncilecih.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 type of DoS attack occurs when an attacker exploits weaknesses in programming source code?**

   A. Protocol

   B. Volumetric

   C. Permanent

   D. Application layer

2. **Which technique tricks individuals into revealing sensitive information during reconnaissance attacks?**

   A. Ping Sweeping

   B. Port Scanning

   C. DNS Footprinting

   D. Social Engineering

3. **When addressing email incidents, what is the primary focus of the recovery step?**

   A. Changing passwords

   B. Detecting the breach

   C. Preparation for future attacks

   D. Eradicating malware

4. **What capability do Security Incident and Event Management (SIEM) solutions provide in the context of insider threat prevention?**

   A. Ensure ongoing confidentiality, integrity, and availability of systems

   B. Make optimal use of digital evidence with minimal investigation costs

   C. Draw patterns for informed decision-making against cyberattacks

   D. Build custom queries and generate alerts for threat detection

5. **Which of the following best describes a characteristic of distributed storage in cloud computing?**

   A. Single point of failure

   B. Data is stored in multiple locations

   C. Requires physical storage hardware

   D. Unrestricted access to all users

SAMPLE

6. What action can an incident responder take to monitor the integrity of critical files?

A. Create cryptographic checksums of critical files.

B. Use isolated test networks.

C. Create checksums and use monitoring tools.

D. None of these choices apply.

7. Which type of phishing specifically targets high profile individuals such as CEOs and politicians?

A. Whaling

B. Spear Phishing

C. Puddle Phishing

D. Pharming

8. Which cloud deployment model is specifically designed for a limited set of organizations with shared interests?

A. Public cloud

B. Hybrid cloud

C. Community cloud

D. Private cloud

9. What is a major benefit of using Infrastructure-as-a-Service (IaaS)?

A. Cost efficiency

B. Global accessibility

C. On-premise control

D. High security

10. Which of the following is NOT considered a type of computer security incident?

A. Unauthorized access

B. Malicious code attack

C. All of these choices are correct

D. Fraud and theft

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What type of DoS attack occurs when an attacker exploits weaknesses in programming source code?

A. Protocol

B. Volumetric

C. Permanent

D. Application layer

The correct choice is the application layer. This type of Denial of Service (DoS) attack specifically targets the application layer of the OSI model, which is where applications and services interact with users and other systems. By exploiting vulnerabilities in programming source code—such as flaws in how the application processes requests or manages resources—an attacker can cause the application to crash or become unresponsive to legitimate users. For example, if an application has a buffer overflow vulnerability, an attacker might send specially crafted input that causes the application to exceed its memory limits. This not only disrupts the service for legitimate users but can also lead to unauthorized access if the vulnerability is severe enough. Understanding this distinction is crucial for incident handlers, as it guides the strategies they must employ to defend against specific attacks based on their targets. The other types of attacks mentioned don't specifically focus on exploiting programming weaknesses in applications. Protocol attacks target the network protocols themselves, volumetric attacks overwhelm system resources with excessive traffic, and permanent attacks imply more complex scenarios that typically involve irreversible damage rather than just leveraging weaknesses in code.

2. Which technique tricks individuals into revealing sensitive information during reconnaissance attacks?

A. Ping Sweeping

B. Port Scanning

C. DNS Footprinting

D. Social Engineering

The technique that effectively tricks individuals into revealing sensitive information during reconnaissance attacks is social engineering. This method relies on psychological manipulation rather than technical hacking skills. Attackers exploit human trust and curiosity to gain sensitive information, often posing as trusted figures or creating scenarios that compel the target to disclose details. For instance, an attacker might impersonate an IT support technician, asking employees for their usernames and passwords under the pretext of performing system updates. This direct interaction with a potential victim can yield critical data that might not be accessible through more technical means. While techniques like ping sweeping, port scanning, and DNS footprinting gather system information and map network resources, they do not involve interaction with individuals. Such methods focus on finding out which devices are active or identifying open ports, but they lack the human element that characterizes social engineering attacks. Therefore, social engineering stands out as the technique that specifically manipulates people into divulging sensitive information.

SAMPLE

3. When addressing email incidents, what is the primary focus of the recovery step?

A. Changing passwords

B. Detecting the breach

C. Preparation for future attacks

D. Eradicating malware

The primary focus of the recovery step in addressing email incidents is to restore normal operations while ensuring that the organization is secure and ready to continue functioning effectively. In this context, changing passwords is critical because it directly addresses potential unauthorized access to accounts that may have been compromised during the incident. By changing passwords, you are taking proactive steps to secure email accounts that may have been exposed and to prevent further unauthorized access, thereby helping to contain the incident and move towards recovery. The other considerations, while important in the overall incident response process, do not specifically align with the immediate recovery efforts. Detecting the breach is an essential part of the response phase, and preparation for future attacks falls under the lessons learned and mitigation stages post-incident. Eradicating malware is also critical but typically occurs in the containment or remediation phase, prior to the recovery step. After ensuring the system is clean, the recovery step primarily focuses on restoring access and operations securely, which makes changing passwords the vital action in that phase.

4. What capability do Security Incident and Event Management (SIEM) solutions provide in the context of insider threat prevention?

A. Ensure ongoing confidentiality, integrity, and availability of systems

B. Make optimal use of digital evidence with minimal investigation costs

C. Draw patterns for informed decision-making against cyberattacks

D. Build custom queries and generate alerts for threat detection

In the context of insider threat prevention, the correct capability provided by Security Incident and Event Management (SIEM) solutions is the ability to draw patterns for informed decision-making against cyberattacks. This is essential because insiders can often exhibit behaviors that deviate from normal patterns. By analyzing logs and events collected from various sources, SIEM solutions can identify anomalous activities that may indicate malicious insider behavior. The capability to draw patterns allows organizations to establish a baseline of normal user behavior, which can then be compared against current activities. If a user suddenly begins accessing sensitive information they typically do not engage with, or if their login times change significantly, these deviations can trigger alerts. This proactive threat detection is key to mitigating risks before they escalate into data breaches or other harmful incidents. While ensuring ongoing confidentiality, integrity, and availability of systems is important, it does not specifically focus on the behavior of individuals within the organization, which is critical in managing insider threats. Similarly, optimizing the use of digital evidence and minimizing investigation costs is relevant but does not directly address the detection and prevention of insider threats. Building custom queries and generating alerts do play a role in SIEM functionality but are more specific tools rather than the broader capability to identify patterns for decision-making against potential insider threats

SAMPLE

5. Which of the following best describes a characteristic of distributed storage in cloud computing?

A. Single point of failure

B. Data is stored in multiple locations

C. Requires physical storage hardware

D. Unrestricted access to all users

The characteristic of distributed storage in cloud computing that is best described by the selected answer is that data is stored in multiple locations. Distributed storage systems leverage the idea of storing data across various geographical locations, which enhances data availability, redundancy, and resilience. This means that even if one storage node goes down, the data can still be accessed from other nodes, thereby preventing data loss and downtime. This approach contrasts sharply with having a single point of failure, which would make the storage system less reliable. A requirement for physical storage hardware is also not a defining feature of cloud-based distributed storage, as these services often abstract away physical hardware management from the user. Lastly, unrestricted access to all users does not accurately represent distributed storage; in fact, strict access controls are often enforced to protect sensitive data and ensure that only authorized users can access certain information.

6. What action can an incident responder take to monitor the integrity of critical files?

A. Create cryptographic checksums of critical files.

B. Use isolated test networks.

C. Create checksums and use monitoring tools.

D. None of these choices apply.

Creating checksums is a widely recognized method for monitoring the integrity of critical files. Checksums are unique values generated from the contents of a file; any change in the file will result in a different checksum. By generating cryptographic checksums for critical files, incident responders can establish a baseline of file integrity. The use of monitoring tools in conjunction with these checksums enhances the incident responder's ability to detect any unauthorized changes or corruption. Monitoring tools can continuously check the integrity of files against the established checksums, alerting responders to any discrepancies. This method is effective because it combines the robustness of cryptographic techniques with real-time monitoring, ensuring that any alterations—whether they be malicious or accidental—are identified quickly. While using isolated test networks may provide a safeguard for testing environments and creating cryptographic checksums alone is beneficial, the combination of checksums with monitoring tools directly addresses the need for ongoing integrity oversight in operational environments.

SAMPLE

7. Which type of phishing specifically targets high profile individuals such as CEOs and politicians?

A. Whaling

B. Spear Phishing

C. Puddle Phishing

D. Pharming

Whaling is a specific type of phishing that focuses on high-profile targets, such as CEOs, politicians, and other significant figures within an organization. The term "whaling" derives from the idea of targeting large, important individuals, similar to how whalers sought large whales. This method involves crafting highly personalized attacks that exploit the authority and access these individuals have, often utilizing information that is readily available or that can be gathered through various means to make the communication appear legitimate and trustworthy. Such phishing attempts often involve direct emails or communications that have a high likelihood of eliciting a response due to the authority of the sender, and they typically aim to deceive the victim into revealing sensitive information or performing actions that compromise security, such as transferring funds. In contrast, other types of phishing, like spear phishing, target specific individuals but do not necessarily focus exclusively on those in high-profile positions. Puddle phishing and pharming refer to different methods of manipulating or redirecting users, but they do not specifically denote a targeted approach aimed at high-ranking or well-known individuals.

8. Which cloud deployment model is specifically designed for a limited set of organizations with shared interests?

A. Public cloud

B. Hybrid cloud

C. Community cloud

D. Private cloud

The community cloud is specifically designed for a limited set of organizations that share common interests, objectives, and requirements. This model allows multiple organizations to collaborate and utilize shared computing resources while ensuring that their specific needs are met. Organizations within a community cloud typically have similar security policies, compliance requirements, or other regulatory concerns that make it more beneficial for them to share a cloud infrastructure. Community clouds foster collaboration and resource sharing among organizations, which can lead to increased efficiency and reduced costs. This dedicated approach allows the participating organizations to address their unique requirements while still benefiting from the advantages of cloud computing, such as scalability and flexibility. The public cloud, on the other hand, is available to any organization or individual, thus lacking the focused community aspect. Hybrid clouds combine elements of both public and private clouds, making them suitable for broader use cases rather than a specific set of organizations. Private clouds are intended for single organizations, providing exclusive access for that particular entity rather than sharing among multiple organizations.

SAMPLE

9. What is a major benefit of using Infrastructure-as-a-Service (IaaS)?

A. Cost efficiency

B. Global accessibility

C. On-premise control

D. High security

The major benefit of using Infrastructure-as-a-Service (IaaS) is global accessibility. IaaS provides a flexible and easily accessible platform that allows users to access computing resources over the internet from anywhere in the world, as long as they have an internet connection. This characteristic enables organizations to deploy applications and services in multiple regions without the need for substantial capital investment in physical hardware and infrastructure. While cost efficiency is indeed a benefit of IaaS, the significance of global accessibility outstrips it, as it empowers businesses to quickly scale operations across different geographical locations without being tied to a specific data center. IaaS also facilitates disaster recovery and business continuity plans due to its ability to maintain resources in various locations simultaneously. On-premise control is contrary to the very nature of IaaS, as this model emphasizes using cloud resources instead of managing physical infrastructure on-site. High security can vary among providers and configurations but is not inherently a guaranteed benefit of IaaS. Therefore, the capability to access infrastructure globally is pivotal, making global accessibility the most relevant advantage of IaaS.

10. Which of the following is NOT considered a type of computer security incident?

A. Unauthorized access

B. Malicious code attack

C. All of these choices are correct

D. Fraud and theft

The assertion that "All of these choices are correct" refers to the idea that every listed option constitutes a type of computer security incident. However, this is not accurate, as the question specifically seeks the option that is NOT considered a type of computer security incident. Unauthorized access is typically a breach of security protocols, where an individual gains access to systems or data they are not permitted to access. Malicious code attacks involve harmful software that infiltrates systems intending to damage or steal data, clearly fitting the definition of a computer security incident. Similarly, fraud and theft encompass unauthorized actions that often result in loss or compromise of information and resources. Since all the other options represent valid types of incidents that affect computer security, it follows that the answer stating that "All of these choices are correct" does not accurately identify a singular incident that would be considered irrelevant to computer security. The phrasing implies that none of the listed incidents fit the criteria of a security incident, which is not the case for these examples. Thus, identifying "C" as an answer overlooks the fact that the other options indeed represent recognized categories of security incidents.

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://eccouncilecih.examzify.com

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

SAMPLE