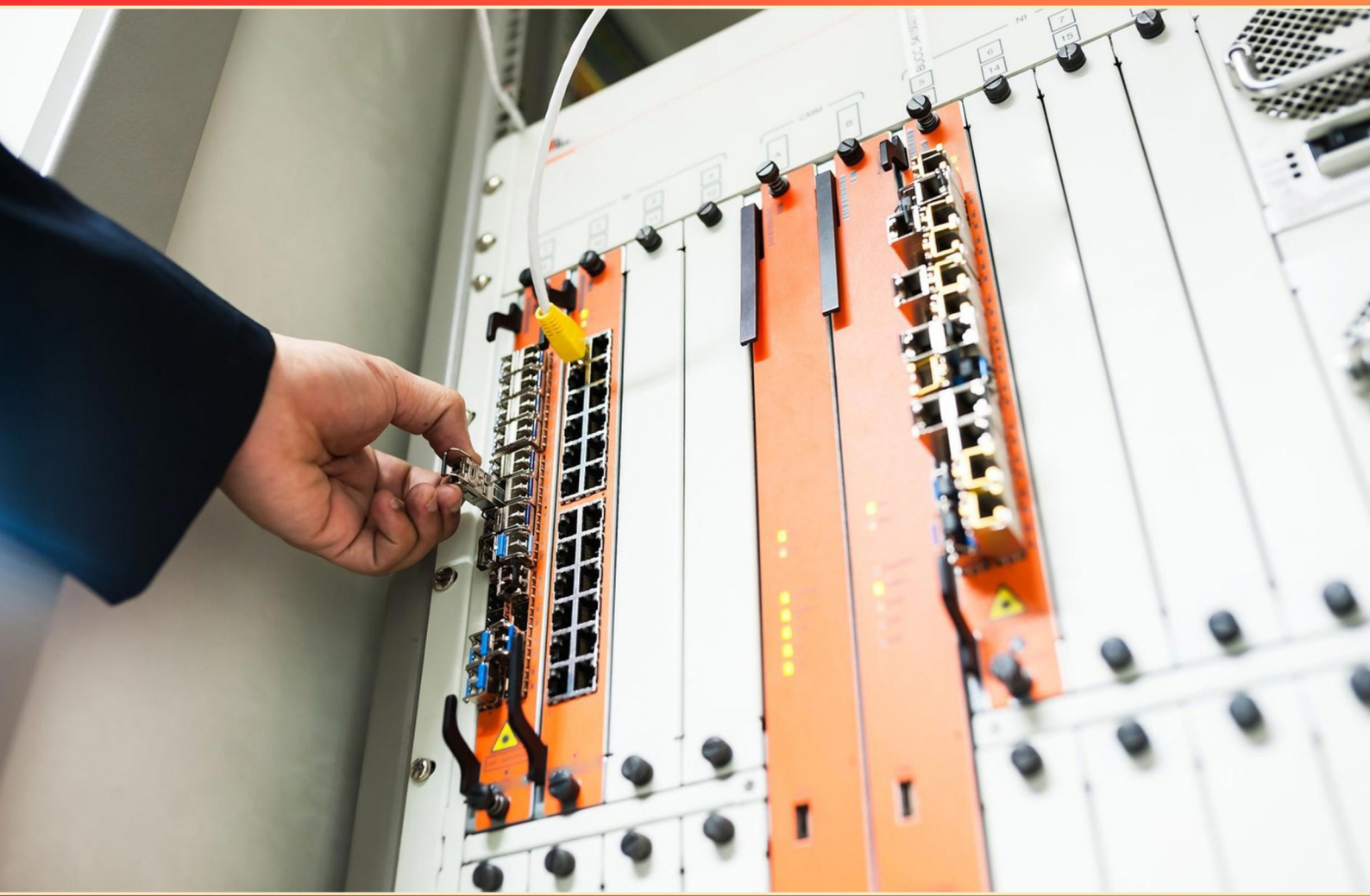
CERTIFIED INCIDENT HANDLER (CIH) PRACTICE ECAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://certifiedincidenthandler.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 web application security threat did Jack identify during his investigation?**

   A. Injection attack

   B. Software and data integrity failure

   C. Denial of service

   D. Phishing

2. **What threat-hunting step involves mitigating the immediate threat and taking corrective actions?**

   A. Response/resolution

   B. Hypothesis

   C. Collect and process the data

   D. Investigation

3. **Identify the practice that will not aid incident responders in mitigating attacks stemming from vulnerable and outdated components.**

   A. Retain unnecessary components, functions, dependencies, and files

   B. Regularly update all components and libraries

   C. Conduct vulnerability assessments regularly

   D. Remove unused services and functions

4. **Which of the following is an auditing and recovery tool for SQL server databases that allows incident handlers to recover the affected SQL database from a database backup?**

   A. ApexSQL Log

   B. SQL Server Management Studio

   C. SharePoint Recovery Tool

   D. Oracle SQL Developer

5. **Which tool is designed to protect websites from SQL injection and other malicious attacks?**

   A. dotDefender

   B. Burp Suite

   C. Nessus

   D. OWASP ZAP

SAMPLE

6. Which practice should an incident responder avoid during the containment of email security incidents?

A. Isolate affected email accounts

B. Allow automatic email forwarding to remote domains

C. Change employee email passwords

D. Notify relevant stakeholders

7. Which type of coding error can lead to attacks that exploit memory vulnerabilities?

A. Buffer Overflows

B. SQL Injection

C. Cross-Site Scripting

D. Data Leakage

8. What tool is used to detect insider threats before they cause damage?

A. DataRobot

B. Vectra Cognito

C. Wireshark

D. Nuix Adaptive Security

9. What is the name of the SIEM tool that assists in detecting real-time network threats?

A. loggly

B. ArcSight Enterprise Security Manager

C. Graylog

D. FortiSIEM

10. Which of the following types of email attacks was identified when unsolicited email links requested personal information from company employees?

A. Spamming

B. Phishing

C. Spimming

D. Malware

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What type of web application security threat did Jack identify during his investigation?

A. Injection attack

B. Software and data integrity failure

C. Denial of service

D. Phishing

The choice indicating software and data integrity failure accurately reflects a critical web application security threat. This type of threat occurs when the data or software within an application is manipulated or compromised, leading to unauthorized changes that can affect the integrity, accuracy, or reliability of the information. In many scenarios, this can happen through various methods such as tampering with code or exploiting vulnerabilities to alter data. For instance, if an attacker gains access to modify backend databases or configuration files, it can disrupt application functionality or lead to misleading information being presented to users. Consequently, ensuring integrity in software and data is essential for maintaining trust and security in web applications. Other types of threats, while serious, don't encompass the specific nuances of this integrity failure. Injection attacks involve inserting malicious code into an application, while denial of service focuses on making a service unavailable to users. Phishing typically involves deception to steal sensitive information, which does not directly align with the integrity failure context that Jack identified in his investigation.

2. What threat-hunting step involves mitigating the immediate threat and taking corrective actions?

A. Response/resolution

B. Hypothesis

C. Collect and process the data

D. Investigation

The response/resolution step in threat hunting is focused on addressing and mitigating the immediate threat that has been identified. This phase is crucial because it involves taking the necessary actions to contain and eliminate the threat, thereby reducing its potential impact on the organization. It encompasses not only remediation efforts to stop the threat but also corrective actions to prevent recurrence. In addition to identifying and resolving the incident, this step may include informing relevant stakeholders, implementing changes to security policies or controls, and updating systems to ensure they are fortified against similar threats in the future. This proactive approach not only addresses the current issue but also enhances the overall security posture of the organization. While hypothesis formulation helps in defining what to look for during the hunt, and collecting and processing data are foundational tasks that precede the identification of threats, the investigation phase centers around understanding the nature and scope of the threat. Response/resolution is distinct as it explicitly focuses on action taken after a threat has been detected.

SAMPLE

3. Identify the practice that will not aid incident responders in mitigating attacks stemming from vulnerable and outdated components.

A. Retain unnecessary components, functions, dependencies, and files

B. Regularly update all components and libraries

C. Conduct vulnerability assessments regularly

D. Remove unused services and functions

Retaining unnecessary components, functions, dependencies, and files can significantly contribute to the risk profile of an organization. Outdated and vulnerable components are often targets for attackers, and keeping them increases the attack surface. Incident responders benefit from a streamlined and secure environment, which involves identifying and eliminating anything that is no longer needed. Regular updates, vulnerability assessments, and the removal of unused services and functions all contribute to a proactive security posture. These practices ensure that known vulnerabilities are addressed, risks are assessed frequently, and only necessary services are running, reducing the potential points of exploitation. In contrast, the practice of retaining outdated components explicitly contradicts the principles of vulnerability management and incident response, thereby not aiding in mitigating attacks effectively.

4. Which of the following is an auditing and recovery tool for SQL server databases that allows incident handlers to recover the affected SQL database from a database backup?

A. ApexSQL Log

B. SQL Server Management Studio

C. SharePoint Recovery Tool

D. Oracle SQL Developer

ApexSQL Log is indeed an auditing and recovery tool specifically designed for SQL Server databases. It allows incident handlers to perform detailed auditing of changes made to the database, and more importantly, it enables them to recover data from transaction logs. This makes it a valuable asset when dealing with incidents where data may have been deleted or modified unintentionally or maliciously. The tool provides a way to analyze the transaction log to see what changes occurred, and it offers functionality to roll back these changes or recover the affected data from the database backup. This capability is crucial for maintaining data integrity and ensuring that critical information can be restored following an incident. In contrast, SQL Server Management Studio is primarily an administration tool that provides users with a graphical interface for managing SQL Server installations and performing various database tasks but does not specialize in recovery from backups. The SharePoint Recovery Tool focuses on SharePoint data rather than SQL Server databases, and Oracle SQL Developer is a tool for managing Oracle databases, which is outside of the scope of SQL Server auditing and recovery.

SAMPLE

5. Which tool is designed to protect websites from SQL injection and other malicious attacks?

A. dotDefender

B. Burp Suite

C. Nessus

D. OWASP ZAP

DotDefender is a web application firewall specifically designed to protect websites from various types of malicious attacks, including SQL injection. It functions by intercepting and analyzing incoming traffic to detect and block harmful requests before they can reach the web application. This proactive approach helps prevent exploitation vulnerabilities that are commonly targeted by attackers. While other tools listed, such as Burp Suite and OWASP ZAP, are primarily utilized for penetration testing and vulnerability assessment, they are not primarily designed for ongoing protection and defense. Instead, they help identify vulnerabilities in web applications so that developers can fix them. Nessus is a vulnerability scanner that focuses on identifying potential security issues across various network devices and systems but does not provide the specific web application protection that dotDefender offers. Choosing dotDefender as the right tool reflects an understanding of Web Application Firewalls (WAFs) and their essential role in safeguarding web environments from SQL injection and other attacks.

6. Which practice should an incident responder avoid during the containment of email security incidents?

A. Isolate affected email accounts

B. Allow automatic email forwarding to remote domains

C. Change employee email passwords

D. Notify relevant stakeholders

In the context of incident response, particularly during the containment phase of email security incidents, allowing automatic email forwarding to remote domains is a practice that should be avoided. This action can facilitate unauthorized access to sensitive information, as it may enable attackers to receive copies of all emails sent to and from the compromised account. This can further exacerbate the situation by allowing attackers to maintain control over the information exchange and potentially exploit it for malicious purposes. On the other hand, isolating affected email accounts, changing employee email passwords, and notifying relevant stakeholders are all critical practices that enhance security. Isolating affected accounts helps to prevent further unauthorized access, changing passwords can cut off the attackers' access, and notifying stakeholders ensures that those who need to respond to or be aware of the incident can take appropriate action.

SAMPLE

7. Which type of coding error can lead to attacks that exploit memory vulnerabilities?

A. Buffer Overflows

B. SQL Injection

C. Cross-Site Scripting

D. Data Leakage

Buffer overflows are a type of coding error that occurs when a program writes more data to a buffer than it can hold, which can overwrite adjacent memory. This behavior can be exploited by attackers to inject malicious code or manipulate the execution flow of a program. When the overflow happens, the attacker can gain control over the program's execution, potentially allowing them to execute arbitrary code, escalate privileges, or cause denial of service. In contrast, SQL injection focuses on manipulating queries to databases, targeting input validation issues rather than memory management. Cross-site scripting also exploits web applications but involves injecting scripts into web pages rather than manipulating memory. Data leakage pertains to the unauthorized transmission of data, which, while serious, does not specifically relate to memory vulnerabilities or exploitation through coded errors. Therefore, buffer overflows are the most relevant type of coding error associated with the exploitation of memory vulnerabilities, making it the accurate choice.

8. What tool is used to detect insider threats before they cause damage?

A. DataRobot

B. Vectra Cognito

C. Wireshark

D. Nuix Adaptive Security

Vectra Cognito is a tool specifically designed to detect insider threats as part of its advanced threat detection capabilities. It utilizes artificial intelligence to analyze network behavior and identify anomalies that may indicate malicious activity from within the organization. By monitoring user activity and network traffic, Vectra Cognito can flag unusual patterns that may suggest a potential insider threat, allowing organizations to take corrective actions before any significant damage occurs. This proactive approach is crucial because insider threats can be difficult to detect with traditional security measures, which often focus more on external threats. The advanced analytics and machine learning capabilities of Vectra Cognito make it particularly effective in identifying potential risks stemming from insider actions, such as data exfiltration or privilege misuse. Other tools listed, while useful in different contexts, do not focus on insider threat detection in the same proactive, behavior-driven manner. For example, Wireshark is primarily a network packet analysis tool that captures and analyzes traffic, but it does not inherently analyze for insider threats. Nuix Adaptive Security also deals with security, but its primary focus is on data management and responding to security incidents rather than active detection of insider threats. DataRobot, as a machine learning platform, is generally not specifically aimed at security analytics for insider threats.

SAMPLE

9. What is the name of the SIEM tool that assists in detecting real-time network threats?

A. loggly

B. ArcSight Enterprise Security Manager

C. Graylog

D. FortiSIEM

The choice of ArcSight Enterprise Security Manager as the correct answer is based on its specific design and functionality as a Security Information and Event Management (SIEM) tool. ArcSight is well-known for its capabilities in real-time threat detection across the network. It aggregates and analyzes log and event data from various sources, allowing security professionals to identify suspicious activities and potential security breaches as they occur. ArcSight's powerful correlation and analysis features enable organizations to gain insights into security events, helping them respond promptly to threats before they escalate. Its ability to provide centralized visibility across complex environments makes it an effective tool in identifying patterns and anomalies related to network threats in real time. While Loggly, Graylog, and FortiSIEM have their own strengths, they may not specifically focus on the advanced features and real-time detection capabilities that are characteristic of ArcSight. These tools serve different purposes or target audiences, which is why ArcSight stands out as the primary choice for detecting real-time network threats in this context.

10. Which of the following types of email attacks was identified when unsolicited email links requested personal information from company employees?

A. Spamming

B. Phishing

C. Spimming

D. Malware

The correct answer is phishing because this type of email attack specifically involves deceptive emails that trick recipients into revealing sensitive personal information, such as passwords or banking details. Phishing attacks often contain links that, when clicked, lead victims to fraudulent websites designed to appear legitimate, with the intent of collecting sensitive data under false pretenses. In the context of the scenario provided, unsolicited emails requesting personal information from company employees clearly fit the definition of a phishing attempt, as they are aimed at misleading recipients into providing confidential information by exploiting trust and creating a sense of urgency or importance. Other options describe different types of threats or attacks. Spamming refers to the bulk sending of unsolicited messages, often for advertising purposes, rather than seeking personal information. Spimming is a more specific term related to spam that involves instant messaging and chat applications to distribute unwanted messages, which does not align with the email context. Malware encompasses various software designed to harm or exploit devices and systems, but it does not specifically relate to requesting personal information through deceptive emails. Hence, phishing is the most accurate choice in this scenario.

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://certifiedincidenthandler.examzify.com

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

SAMPLE