SECURITY INCIDENT RESPONSE (SIR) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://securityincidentrespo.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 information is measured during the "Measure" step of the SIR Customer Adoption Journey - Modernize Maturity Level 2?

A. # of trained analysts

B. # of SLA results

C. # of incidents closed over trends

D. Basic Dashboarding improvements

2. What does 'forensics' refer to in the context of Security Incident Response (SIR)?

A. The process of creating security policies

B. The application of scientific methods to investigate incidents

C. Implementing software to monitor threats

D. Conducting training sessions for staff

3. Which role is considered the Security Basic?

A. admin

B. sn_si.admin

C. sn_si.analyst

D. sn_si.basic

4. What factors should be included when building a Security Incident Response team?

A. Skills

B. Knowledge

C. All of the above

D. Metrics

5. What are potential resources to use during an incident response?

A. Office supplies and support staff

B. Cybersecurity tools, threat intelligence feeds, and legal counsel

C. Retail security personnel and alarms

D. Social media contacts for public relations

SAMPLE

6. Which of the following is a common type of security incident that organizations encounter?

A. Server upgrades

B. Phishing attacks

C. Software development

D. Physical inventory checks

7. Who typically performs analysis related to security incidents?

A. admin

B. sn_si.admin

C. sn_si.manager

D. sn_si.analyst

8. Which role is designated for read-only access to security incidents, primarily for reporting and monitoring?

A. sn_si.read

B. sn_si.external

C. sn_si.ciso

D. sn_si.knowledge_admin

9. Which step should you focus on when tailoring forms and fields for SIR?

A. Measure

B. Refine

C. Connect

D. Launch

10. What is a common outcome of a well-executed incident response?

A. Increased customer trust

B. Widespread recognition of the company's brand

C. Higher occurrence of future incidents

D. Decreased employee morale

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What information is measured during the "Measure" step of the SIR Customer Adoption Journey - Modernize Maturity Level 2?

A. # of trained analysts

B. # of SLA results

C. # of incidents closed over trends

D. Basic Dashboarding improvements

The "Measure" step of the SIR Customer Adoption Journey, particularly at Modernize Maturity Level 2, focuses on evaluating performance based on the effectiveness and efficiency of incident handling. Measuring the number of incidents closed over trends is particularly relevant because it provides insight into the team's responsiveness and effectiveness in resolving security incidents. Analyzing this metric helps organizations understand their incident response capabilities over time, assess improvements, and identify patterns that can guide further enhancements. This kind of data allows organizations to evaluate their operational performance, spot areas that may require additional training or resources, and ultimately improve their incident response process. Insights gained from this measurement can lead to data-driven decisions that enhance overall security posture and improve customer confidence in the organization's incident response protocols.

2. What does 'forensics' refer to in the context of Security Incident Response (SIR)?

A. The process of creating security policies

B. The application of scientific methods to investigate incidents

C. Implementing software to monitor threats

D. Conducting training sessions for staff

In the context of Security Incident Response (SIR), 'forensics' refers specifically to the application of scientific methods to investigate incidents. This involves a systematic approach to collecting, preserving, analyzing, and presenting data in a manner that is legally admissible and useful in understanding the nature and scope of security incidents. Forensics enables investigators to uncover the how, when, and why of a security breach, as well as to identify attackers and mitigate future risks. The field combines elements of computer science, law, and investigative techniques to gather evidence from digital environments, ensuring that the integrity of the information is maintained and that it can be used in legal contexts if necessary. This ability to accurately reconstruct events surrounding an incident is crucial for both immediate response efforts and long-term security improvement strategies. Other choices, while relevant to security practices, do not capture the essence of forensics. Creating security policies involves establishing guidelines to prevent incidents but not investigating them. Monitoring threats pertains to proactive measures rather than the post-incident analysis that forensics provides. Training sessions for staff are integral to enhancing overall security awareness but do not relate to the scientific investigation aspect central to forensic efforts. Thus, the emphasis on the investigative and analytical processes uniquely identifies option focused on forensics.

SAMPLE

3. Which role is considered the Security Basic?

A. admin

B. sn_si.admin

C. sn_si.analyst

D. sn_si.basic

The role referred to as "Security Basic" is typically linked to fundamental access and privileges within a security incident response framework. This role is designed to provide essential capabilities appropriate for individuals who may not require extensive permissions or advanced functionalities found in higher-level roles. In many security platforms, roles are structured hierarchically, with different levels of access based on the user's responsibilities. The Security Basic role typically includes access to standard features necessary for conducting basic security tasks without compromising the system's integrity or security. On the other hand, roles like admin and sn_si.admin generally represent elevated permission levels that allow for wider control over the system, including the ability to manage users and overall system configurations. Similarly, the sn_si.analyst role will likely include analytical and investigative capabilities, which go beyond the basic level needed for regular operations. By limiting privileges to the essential functions, the Security Basic role ensures that users can perform their responsibilities while minimizing risks and maintaining the security posture of the organization. This is an important principle in role-based access control, which seeks to provide just enough permissions to perform a job effectively while safeguarding sensitive information and system integrity.

4. What factors should be included when building a Security Incident Response team?

A. Skills

B. Knowledge

C. All of the above

D. Metrics

When building a Security Incident Response team, it is essential to consider a comprehensive set of factors that contribute to the effectiveness of the team's response capabilities. The inclusion of skills, knowledge, and metrics is vital for several reasons. Skills refer to the technical expertise and practical abilities that team members bring to the table. This can include proficiency in handling security tools, performing forensic analysis, and implementing remediation strategies. A team rich in diverse skills is better equipped to address a wide range of security incidents and respond effectively to various threats. Knowledge encompasses the understanding of security protocols, regulatory requirements, and the latest threat intelligence. Team members need to be knowledgeable about current vulnerabilities, attack vectors, and defense mechanisms. This foundational understanding helps the team to anticipate potential incidents and respond more effectively when they arise. Metrics, while sometimes overlooked, are also crucial in assessing the team's performance and the effectiveness of the incident response processes. By tracking key performance indicators and establishing benchmarks, teams can evaluate their response times, the effectiveness of their communications during incidents, and their overall impact on reducing the risks and effects of security incidents. These metrics guide ongoing improvements, training, and strategies for the team. In summary, a well-rounded approach that incorporates skills, knowledge, and metrics ensures that the Security Incident

SAMPLE

5. What are potential resources to use during an incident response?

A. Office supplies and support staff

B. Cybersecurity tools, threat intelligence feeds, and legal counsel

C. Retail security personnel and alarms

D. Social media contacts for public relations

The correct choice emphasizes the key resources that are critical in managing an incident during a cybersecurity event. Cybersecurity tools are essential as they help in identifying, containing, and remediate security incidents effectively. These tools may include intrusion detection systems, antivirus software, and incident management platforms, which enable teams to analyze vulnerabilities and respond swiftly. Threat intelligence feeds are another vital resource because they provide current information about potential threats and vulnerabilities in the cybersecurity landscape. This information can guide response teams in prioritizing their actions and understanding the nature of the threats they are facing. Legal counsel plays a significant role during an incident response, particularly in navigating compliance with laws and regulations, managing liability issues, and advising on the proper course of action regarding disclosures and communications following a breach. This legal insight ensures that the organization minimizes risk while responding to an incident. While the other options mention resources that could be useful in specific contexts, they do not align directly with the critical needs and specificities of an effective cybersecurity incident response strategy. Office supplies and support staff might assist in coordination efforts, but they lack direct relevance to technical response actions. Retail security personnel and alarms address physical security, which may not be applicable in cyber incidents. Social media contacts can be helpful for communication, but they do not

6. Which of the following is a common type of security incident that organizations encounter?

A. Server upgrades

B. Phishing attacks

C. Software development

D. Physical inventory checks

Phishing attacks are a prevalent type of security incident that organizations frequently encounter. This tactic involves cybercriminals sending deceptive messages, often through email, to manipulate individuals into revealing sensitive information, such as login credentials or financial information. The success of phishing attacks is largely due to their ability to exploit human vulnerabilities, making them a significant concern for organizations aiming to protect their data and resources. In contrast, server upgrades and software development are routine operational tasks that, while they may present risks if not managed properly, do not inherently constitute security incidents. Physical inventory checks are also standard processes typically unrelated to security incidents. Overall, the existence of phishing as a direct threat to organizational security underscores its classification as a common security incident.

SAMPLE

7. Who typically performs analysis related to security incidents?

A. admin

B. sn_si.admin

C. sn_si.manager

D. sn_si.analyst

The role of an analyst in the context of security incidents is critically important as they are primarily responsible for monitoring, analyzing, and responding to security events. Analysts possess the necessary skills and training to identify patterns, determine the nature of threats, and assess the impact of incidents. Their tasks often include investigating alerts, correlating data from various sources, and producing reports that inform decision-making for remediation and prevention. In contrast, the administration roles typically focus more on maintaining systems and performing operational tasks rather than deep analytical work specific to security incident responses. Managers, while they may oversee the security incident response process, are generally involved in strategic planning and resource allocation rather than hands-on analysis. An analyst's specialized expertise is essential in effectively addressing and resolving security incidents, thereby making them the correct choice for who performs this critical analysis.

8. Which role is designated for read-only access to security incidents, primarily for reporting and monitoring?

A. sn_si.read

B. sn_si.external

C. sn_si.ciso

D. sn_si.knowledge_admin

The role designated for read-only access to security incidents, primarily for reporting and monitoring, is the one that specifically includes "read" in its designation. This role is tailored to provide users with the ability to view security incidents without granting any privileges that would allow them to make changes or modifications. Having read-only access is essential for individuals who need to monitor incidents and generate reports but should not participate in the actual response or remediation activities. It ensures that sensitive incident details remain protected while still allowing visibility for oversight, compliance, and informative purposes. The other roles mentioned either imply broader access or pertain to functions that do not focus solely on read-only capabilities related to security incidents, making them unsuitable for this specific requirement of monitoring and reporting.

SAMPLE

9. Which step should you focus on when tailoring forms and fields for SIR?

A. Measure

B. Refine

C. Connect

D. Launch

Focusing on refining forms and fields for Security Incident Response (SIR) is essential because this step allows for the optimization and customization of data collection methods to better fit the specific requirements of an organization. During the refinement phase, you assess the existing forms and fields, ensuring they capture all necessary details relevant to incidents, while eliminating any superfluous information that could hinder effective data collection. This process involves reviewing and possibly restructuring prompts to improve clarity and usability, ensuring that responders can input information efficiently without confusion. By prioritizing refinement, you create a more streamlined and effective reporting process, which is crucial for timely and accurate incident response. Other steps like measuring, connecting, and launching are important in their own right but come later in the overall process. Measuring typically focuses on assessing the effectiveness of the forms after refinement has occurred, connecting may relate to integrating the forms within broader systems or teams, and launching refers to the implementation of the refined forms into the incident management workflow. However, without a solid refinement process, the forms may not yield the best results, making this step fundamental.

10. What is a common outcome of a well-executed incident response?

A. Increased customer trust

B. Widespread recognition of the company's brand

C. Higher occurrence of future incidents

D. Decreased employee morale

A well-executed incident response can significantly bolster customer trust. When an organization responds effectively to security incidents, it demonstrates to its customers that they are committed to protecting sensitive data and maintaining robust security protocols. This proactive approach reassures customers that the company can manage risks competently and that their personal information is safeguarded against potential breaches. In contrast, other options may not be outcomes of a successful incident response. For example, widespread recognition of a company's brand is not directly tied to the execution of incident response but rather relates to marketing efforts and overall business performance. The incidence of future security breaches might increase if the underlying vulnerabilities are not addressed properly during the response process. Moreover, incident response actions, especially if they involve significant changes or disruptions, can sometimes affect employee morale negatively if not managed with clear communication and support. Therefore, the focus on customer trust as a positive outcome reflects the central aim of effective incident management.

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://securityincidentrespo.examzify.com

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

SAMPLE