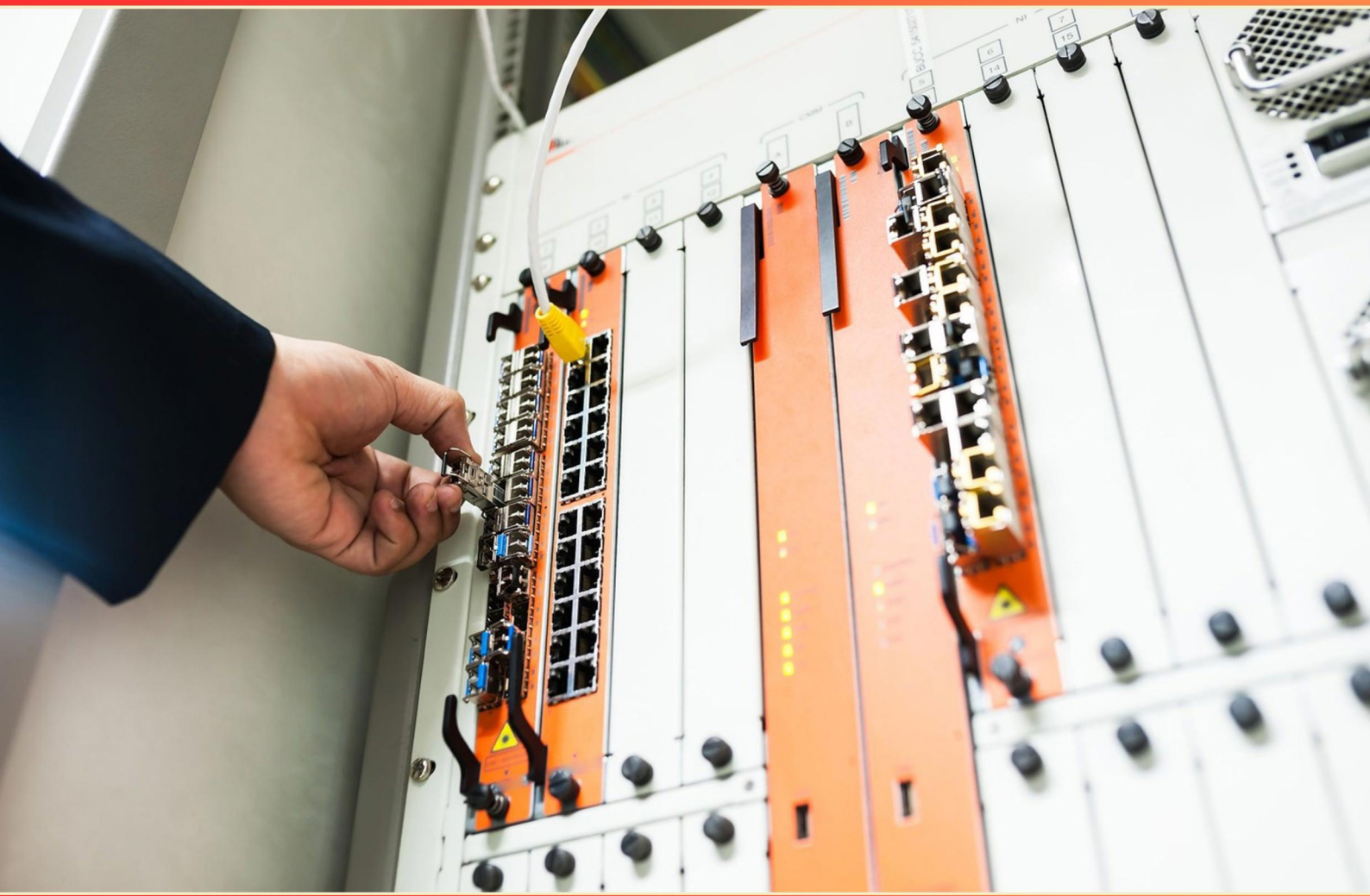
CERTIFIED INCIDENT HANDLER (CIH) PRACTICE ECAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://certifiedincidenthandler.examzify.com

Table of Contents

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.

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!

Questions

1. **Which practice will not help incident responders recover resources after a Google Cloud security incident?**

   A. Take snapshots for recreating the disks

   B. Recreate the environment from recent backups

   C. Never take snapshots for recreating the disks

   D. Use disaster recovery plans

2. **Which tool helps incident responders monitor and analyze user-based insider threats?**

   A. Wireshark

   B. Ekran System

   C. Infoblox

   D. Vectra Cognito

3. **What attack involves an insider entering a restricted area by following an authorized person?**

   A. Impersonation

   B. Tailgating

   C. Physical Breach

   D. Access Control Breach

4. **What is the main purpose of deploying an email filtering tool within an organization?**

   A. To enhance user experience

   B. To screen and filter out malicious emails

   C. To track employee productivity

   D. To manage company calendar

5. **What is the reporting timeframe for a DoS attack on a US Federal agency network?**

   A. 24 hours

   B. 2 hours

   C. 1 hour

   D. 48 hours

6. Which activity should an incident handler not perform while addressing email security incidents?

A. Restore from a reliable backup

B. Restore affected systems from an untrusted backup

C. Analyze email access logs

D. Communicate with email service providers

7. Identify the responsibility assigned to Jack in the described scenario.

A. Documenting the incident

B. Collecting the information about the incident

C. Securing the crime scene

D. Analyzing physical evidence

8. What tool helps verify email validity during the investigation of an email security incident?

A. Spamhaus

B. ZeroBounce

C. Mailgun

D. SendGrid

9. Which offense involves malware that replicates itself to spread to other systems?

A. Trojan

B. Worm

C. Spyware

D. Ransomware

10. What tool did George use to search and analyze ICS log data?

A. Flowmon

B. Wireshark

C. NetworkMiner

D. Splunk Enterprise

Answers

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

Explanations

1. Which practice will not help incident responders recover resources after a Google Cloud security incident?

A. Take snapshots for recreating the disks

B. Recreate the environment from recent backups

C. Never take snapshots for recreating the disks

D. Use disaster recovery plans

The choice to avoid taking snapshots for recreating disks is significant in the context of incident response and resource recovery following a security incident in Google Cloud. Snapshots are critical for preserving the state of a virtual machine's disks at a specific point in time. They allow responders to restore data and configurations to a known good state, which is essential for recovering from incidents and minimizing downtime. By not utilizing snapshots, incident responders miss an opportunity to quickly revert back to a pre-incident state or recover lost data efficiently. Snapshots can serve as a cost-effective and timely solution for regeneration of affected resources without the need to rely solely on longer recovery methods, such as restoring from backups. Snapshots not only aid in resource recovery but also facilitate forensic analysis by allowing responders to access the system state at the moment before the incident. This can provide critical insights for understanding what occurred and how to prevent similar events in the future. In summary, avoiding snapshots impedes effective incident recovery processes, thereby hindering the overall incident response efforts in a cloud environment.

2. Which tool helps incident responders monitor and analyze user-based insider threats?

A. Wireshark

B. Ekran System

C. Infoblox

D. Vectra Cognito

The Ekran System is designed specifically for monitoring and analyzing user activity, making it particularly effective in identifying potential insider threats. This tool focuses on user behavior and allows incident responders to track various activities within systems and applications. It offers features such as session recording, access control, and real-time alerts, all of which are crucial for detecting unusual patterns that may signify malicious intent from within the organization. By leveraging this capability, organizations can gain insights into user actions, investigate suspicious activities promptly, and take necessary responses to mitigate potential threats. In contrast, other tools like Wireshark are primarily used for network traffic analysis, while Infoblox is known for DNS management and security, and Vectra Cognito focuses on network-based threats and anomalies rather than specifically addressing user behavior. Thus, the Ekran System is uniquely positioned to address the challenges associated with insider threats effectively.

3. What attack involves an insider entering a restricted area by following an authorized person?

A. Impersonation

B. Tailgating

C. Physical Breach

D. Access Control Breach

The correct answer is tailgating. This type of attack occurs when an unauthorized individual gains access to a restricted area by closely following an authorized person, taking advantage of the legitimate entry granted to the authorized individual. Tailgating exploits social engineering techniques, where the unauthorized person relies on the trust or unawareness of the authorized individual to gain entry without proper credentials. In scenarios like this, the unauthorized person typically maintains proximity to the authorized user, entering through secure doors and access points without using their own access credentials. This method can be particularly effective in organizations where physical security measures do not prevent someone from following another person closely, thus highlighting the importance of awareness and vigilance in security protocols. The other options highlight different aspects of security and attack methods but do not directly describe the specific action of following someone to gain unauthorized access to a restricted area. Impersonation involves pretending to be someone else to gain access, while a physical breach refers to a more direct unauthorized entry. An access control breach can encompass a variety of unauthorized access methods but does not specifically capture the scenario of following an authorized individual.

4. What is the main purpose of deploying an email filtering tool within an organization?

A. To enhance user experience

B. To screen and filter out malicious emails

C. To track employee productivity

D. To manage company calendar

The primary purpose of deploying an email filtering tool within an organization is to screen and filter out malicious emails. This is crucial for maintaining the security and integrity of the organization's digital communication. Email filtering tools are designed to identify and block spam, phishing attempts, and other potentially harmful content before they reach users' inboxes. By implementing such systems, organizations can significantly reduce the risk of malware infections, data breaches, and other security incidents that often originate from insecure email traffic. While enhancing user experience, tracking employee productivity, and managing company calendars may be beneficial functionalities in different contexts, they do not directly address the critical need for protecting the organization from the threats posed by malicious emails. The focus of email filtering is explicitly on security and the prevention of attacks, making this choice the most relevant answer to the question.

5. What is the reporting timeframe for a DoS attack on a US Federal agency network?

A. 24 hours

B. 2 hours

C. 1 hour

D. 48 hours

The reporting timeframe for a Denial of Service (DoS) attack on a US Federal agency network is indeed 2 hours. This timeframe is established to ensure that any potential threats to agency operations and national security are communicated swiftly and effectively. Early reporting allows for more timely intervention, investigation, and mitigation efforts to be initiated, minimizing the impact of the attack. The urgency in this reporting requirement underscores the critical nature of maintaining operational integrity in federal networks, as DoS attacks can disrupt services and impact the ability to perform essential government functions. Reporting within this 2-hour window allows for coordinated responses, involving necessary cybersecurity teams and other relevant stakeholders, facilitating a rapid and organized approach to addressing the incident. Overall, this timeframe reflects a balance between immediate awareness and practical operational capabilities for incident responders while ensuring that appropriate measures can be taken to safeguard information and systems from further risk or deterioration.

6. Which activity should an incident handler not perform while addressing email security incidents?

A. Restore from a reliable backup

B. Restore affected systems from an untrusted backup

C. Analyze email access logs

D. Communicate with email service providers

Restoring affected systems from an untrusted backup is a critical activity that an incident handler should avoid when addressing email security incidents. When dealing with security incidents, particularly those related to email, the integrity and trustworthiness of backups are paramount. Using an untrusted backup can lead to reintroducing compromised data or systems, which could perpetuate the security breach or introduce new vulnerabilities. In an incident response situation, it is essential first to ensure that any backups used for restoration are verified and known to be secure, as they might contain malware or other malicious artifacts that the previous incident allowed to infiltrate. By relying on untrusted backups, there is a significant risk of further compromising the environment rather than recovering from the incident effectively. In contrast, restoring from a reliable backup, analyzing email access logs, and communicating with email service providers are sound practices that contribute to identifying the scope of the incident, recovering from it effectively, and ensuring better defenses against future incidents.

7. Identify the responsibility assigned to Jack in the described scenario.

A. Documenting the incident

B. Collecting the information about the incident

C. Securing the crime scene

D. Analyzing physical evidence

In the context of incident management, collecting information about the incident is a crucial responsibility. This task involves gathering relevant data, evidence, and context surrounding the incident to understand what occurred effectively. It includes interviews with involved parties, retrieving log files, and collecting any other pertinent documentation or observations that can provide insight into the incident's nature and extent. This action is foundational for subsequent steps in incident handling, such as analyzing the data to determine the cause or implementing measures to prevent future occurrences. Effective information collection informs decisions and strategies for response and recovery, making it a vital aspect of incident management. Collecting accurate and comprehensive information ensures that other team members, including those analyzing and documenting the incident, have the necessary context and details to perform their roles effectively.

8. What tool helps verify email validity during the investigation of an email security incident?

A. Spamhaus

B. ZeroBounce

C. Mailgun

D. SendGrid

The tool that is particularly effective in verifying email validity during the investigation of an email security incident is ZeroBounce. This service specializes in email verification by checking email addresses against a variety of databases to determine their validity, separating legitimate emails from invalid or disposable ones. ZeroBounce not only identifies whether an email is still active but also provides additional insights, such as whether the email is associated with a temporary service, and helps reduce the risk of bouncing emails during communications. This is crucial during an email security incident, as verifying the legitimacy of senders and recipients can aid in identifying potential phishing attempts or malicious communications. The other tools mentioned, while having their own unique functionalities—like Spamhaus, which is more focused on blocking known spam sources, and Mailgun and SendGrid, which are more geared towards email sending and delivery services—do not specifically emphasize the verification of email validity in the same manner that ZeroBounce does. Thus, ZeroBounce stands out as the go-to tool for validating emails in the context of an investigation.

9. Which offense involves malware that replicates itself to spread to other systems?

A. Trojan

B. Worm

C. Spyware

D. Ransomware

The correct answer is a worm. Worms are a type of malware that are specifically designed to replicate themselves and spread across networks without needing to attach themselves to a host file, unlike other types of malware. They exploit network vulnerabilities to gain access to other systems and can propagate rapidly, which often leads to significant disruption. Trojan, while a serious threat, serves a different function as it disguises itself as legitimate software to trick users into downloading it, rather than focusing on replication. Spyware primarily gathers information from the user's device without their consent, and while it can cause harm, it does not focus on self-replication. Ransomware, on the other hand, encrypts the victim's files and demands a ransom for the decryption key, and does not replicate itself across systems. Thus, the distinguishing feature of a worm is its ability to self-replicate and spread independently, which precisely defines its role in the malware landscape.

10. What tool did George use to search and analyze ICS log data?

A. Flowmon

B. Wireshark

C. NetworkMiner

D. Splunk Enterprise

The selection of Splunk Enterprise as the tool used to search and analyze Industrial Control System (ICS) log data is correct because Splunk is a powerful platform designed for searching, monitoring, and analyzing machine-generated big data via a web-style interface. It excels at handling large volumes of log data, making it exceptionally suited for parsing and examining ICS logs, which can come from various devices, sensors, and applications. Splunk allows users to perform detailed queries, generate insights, and visualize the data, all of which are crucial when monitoring ICS environments for potential security incidents. It also offers advanced functionalities, such as real-time data analytics and the ability to correlate events from diverse sources, enhancing operational visibility within ICS networks. In contrast, while the other tools listed serve specific purposes, they do not match the comprehensive capabilities of Splunk for analyzing log data from ICS. Flowmon focuses primarily on network performance monitoring and security analytics but lacks the broader log management and search functionalities. Wireshark is primarily a network protocol analyzer, suitable for capturing and inspecting traffic, but it does not specialize in log management. NetworkMiner is a network forensic analysis tool, mainly for passive network sniffing and analysis, which may not provide the extensive log analytical capabilities that Splunk offers.

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!