Certified Incident Handler (CIH) Practice Ecam (Sample)

Study Guide

Everything you need from our exam experts!

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. **What should an incident responder consider if the data is lost after eliminating the cause of the incident?**

   A. Try to recover from the incident's logs

   B. Recover data from backup

   C. Notify stakeholders only

   D. Wait for instructions from management

2. **Which tool did John use to analyze activities on the victim's Android device during a security incident investigation?**

   A. ADB (Android Debug Bridge)

   B. LogRabbit

   C. Sysinternals Suite

   D. Android Monitor

3. **What tool is specifically designed to identify DoS/DDoS attacks?**

   A. Firepower Threat Defense

   B. FastNetMon

   C. Snort

   D. Splunk

4. **What risk can emerge due to inadequate logical segregation in cloud computing?**

   A. Data Breach

   B. Cost Overruns

   C. Multi-tenancy and Physical Security

   D. Service Downtime

5. **What tool is used by incident handlers to monitor and control HTTP/HTTPS traffic?**

   A. ClamAV

   B. Proxy Switcher

   C. Atomic OSSEC

   D. BrowseControl

6. What attack vector allows an attacker to exploit third-party vendor vulnerabilities?

A. Supply Chain

B. Phishing

C. Social Engineering

D. Insider Attack

7. What is the primary objective of incident management?

A. Increase profit margins

B. Enhance user interface

C. Prevent incidents and attacks

D. Improve application performance

8. What tool did David use to gain full visibility while investigating a Google Cloud security incident?

A. Dynatrace

B. CloudTrail

C. Service Account

D. Cloud Monitoring

9. Which recovery strategy is essential after handling an insider threat?

A. Implement a person-to-person rule for backups

B. Use cloud storage for all backups

C. Allow unrestricted access to backup resources

D. Discard old backups immediately

10. Identify the tool employed by Caleb to analyze malware components and suspicious events.

A. Splunk Enterprise Security

B. Cylance

C. Malwarebytes

D. Avast Business

Answers

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

Explanations

1. What should an incident responder consider if the data is lost after eliminating the cause of the incident?

A. Try to recover from the incident's logs

B. Recover data from backup

C. Notify stakeholders only

D. Wait for instructions from management

The focus for an incident responder in the situation where data has been lost after the cause has been eliminated is to prioritize recovery efforts. Recovering data from backups is typically the most effective and efficient method for restoring lost information, as backups are intentionally created to protect against data loss. This process enables the organization to restore critical files and information to a state prior to the incident, minimizing further disruptions and allowing for continuity of operations. Utilizing backups is essential because it not only provides a means to recover lost data but also ensures that the organization can revert to a known-good configuration, safeguarding against potential remnants of the incident that may still be present in the environment. Moreover, recovery from backups can help the organization understand the impact of the incident and allow for a more comprehensive analysis moving forward. While examining incident logs could provide insights into the event and help in understanding the incident's timeline and impact, it does not directly contribute to recovering the lost data. Additionally, notifying stakeholders is essential for communication, but it doesn't aid in restoring the integrity of lost data. Waiting for management's instructions may neglect the urgency required in data recovery efforts, especially in time-sensitive incidents. Therefore, promptly recovering data from backups is the most strategic course of action in this scenario.

2. Which tool did John use to analyze activities on the victim's Android device during a security incident investigation?

A. ADB (Android Debug Bridge)

B. LogRabbit

C. Sysinternals Suite

D. Android Monitor

The accurate choice for analyzing activities on the victim's Android device during a security incident investigation is LogRabbit. This tool is specifically designed to capture and log events from Android devices, making it especially useful for forensic investigations. It allows investigators to gather data on application behavior, system events, and log entries, providing insight into the activities that occurred on the device. LogRabbit helps handle Android's unique architecture and data formats, providing a more reliable and effective method of obtaining logs directly from the device. Investigators can use this information to piece together the sequence of events leading up to and during the incident, assess the potential impact, and identify any malicious activity. While ADB (Android Debug Bridge) is a powerful tool for developers and can be utilized in investigations, it is more general and less tailored for forensic purposes compared to LogRabbit. Similarly, the Sysinternals Suite is excellent for Windows environments, and Android Monitor, while useful for debugging Android applications, does not focus specifically on capturing logs in a way that is beneficial for forensic purposes. Therefore, when analyzing activities on an Android device, LogRabbit offers a focused approach that aligns with the needs of a security incident investigation.

3. What tool is specifically designed to identify DoS/DDoS attacks?

A. Firepower Threat Defense

B. FastNetMon

C. Snort

D. Splunk

FastNetMon is specifically designed to identify Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks. It works by monitoring network traffic in real-time to detect unusual patterns or spikes that typically characterize these types of attacks. FastNetMon can analyze traffic data, calculate bandwidth usage, and identify packet rates, enabling it to spot the signs of a DDoS attack very effectively. While other tools listed have capabilities to monitor network security or analyze traffic, they do not focus exclusively on DDoS detection. For instance, Firepower Threat Defense provides a broader range of security features, including firewall capabilities, intrusion prevention, and advanced threat protection but is not specialized in DDoS identification. Snort, being an intrusion detection system (IDS), can detect various network attacks with its signature-based detection but may not have built-in capabilities specifically targeted at DDoS attack identification. Splunk is a powerful data analysis tool that enables various forms of data aggregation and analysis but requires additional configuration and implementations to be effective specifically for DDoS detection. FastNetMon's specialization and design make it particularly effective for identifying and managing the specific challenges posed by DoS and DDoS attacks, making it the optimal choice in

4. What risk can emerge due to inadequate logical segregation in cloud computing?

A. Data Breach

B. Cost Overruns

C. Multi-tenancy and Physical Security

D. Service Downtime

In the context of cloud computing, inadequate logical segregation can lead to significant risks, particularly concerning multi-tenancy and physical security. Logical segregation refers to the manner in which data and computing resources are separated and managed within a cloud environment. If this segregation is not effectively implemented, it can enable unauthorized access to sensitive data and resources by users or tenants who do not have the appropriate permissions. Multi-tenancy is a key characteristic of cloud computing, where multiple users or clients share the same physical resources while maintaining the privacy of their individual data. When logical segregation is insufficient, it can lead to scenarios where one tenant could inadvertently gain access to another tenant's data, increasing the risk of data theft or exposure, which is a serious security concern. Moreover, the lack of proper logical controls can also impact physical security. For example, if resources are not appropriately segregated, it can complicate the monitoring and management of physical data centers hosting cloud services, making them more vulnerable to physical breaches. This lack of clear delineation can lead to a variety of security incidents stemming from both logical and physical vulnerabilities within the infrastructure. By understanding the implications of inadequate logical segregation in cloud environments, organizations can better assess their risks and take appropriate measures to enhance their cloud security posture

5. What tool is used by incident handlers to monitor and control HTTP/HTTPS traffic?

A. ClamAV

B. Proxy Switcher

C. Atomic OSSEC

D. BrowseControl

The selection of Proxy Switcher as the correct tool for monitoring and controlling HTTP/HTTPS traffic is well-founded because it functions as a middleware solution that facilitates the management of web requests. Proxy Switchers allow incident handlers to route web traffic through designated proxy servers, providing the ability to monitor and filter the content being accessed. Additionally, they can enforce security policies by controlling which websites users can visit and logging access patterns for analysis. This is especially critical in an incident response context, where understanding web activity can reveal potential security incidents and help in safeguarding sensitive information. By using Proxy Switchers, incident handlers gain better visibility into HTTP/HTTPS transactions, making it easier to detect anomalies, enforce access controls, and implement security measures. The other options, while useful in different aspects of cybersecurity, do not provide the focused capabilities for HTTP/HTTPS traffic management that Proxy Switcher does. ClamAV is primarily an antivirus tool designed to detect malware, Atomic OSSEC is an intrusion detection system that monitors logs and file integrity, and BrowseControl is more focused on managing web browsing policies rather than directly monitoring traffic. Thus, Proxy Switcher stands out as the most appropriate tool for the specified purpose.

6. What attack vector allows an attacker to exploit third-party vendor vulnerabilities?

A. Supply Chain

B. Phishing

C. Social Engineering

D. Insider Attack

The correct choice highlights the concept of supply chain attacks, which exploit vulnerabilities in third-party vendors that organizations depend upon for goods or services. Supply chain attacks occur when an attacker targets an organization by compromising a vendor or service provider that has access to the organization's systems or data. This method is particularly dangerous as these third-party vendors may have varying levels of security practices in place, which can be less stringent than the primary organization's own security measures. By infiltrating the supply chain, attackers can access sensitive information, introduce malware, or create backdoors without directly attacking the primary target, making these attacks harder to detect and mitigate. In contrast, the other options focus on different approaches to attacks. Phishing specifically targets individuals through deceiving emails or messages to gather sensitive information. Social engineering circles around manipulating individuals psychologically to breach security protocols, while insider attacks involve threats from within the organization itself, such as employees or contractors. These methods do not emphasize the exploitation of vulnerabilities associated with third-party vendors, thus distinguishing supply chain attacks as the appropriate answer.

7. What is the primary objective of incident management?

A. Increase profit margins

B. Enhance user interface

C. Prevent incidents and attacks

D. Improve application performance

The primary objective of incident management is to prevent incidents and attacks. This encompasses a proactive approach where organizations aim to minimize the risk of security incidents occurring in the first place. Effective incident management involves identifying potential vulnerabilities within systems, implementing preventive measures, and establishing protocols for rapid response to any incidents that may arise. The goal is to maintain the integrity, availability, and confidentiality of the organization's information systems while reducing the overall impact of security threats. Other choices, while important in their own contexts, do not align with the core purpose of incident management. Increasing profit margins is more related to financial performance than to managing security incidents. Enhancing user interface focuses on improving user experience rather than addressing security. Improving application performance, although beneficial for users, is separate from the objectives of incident management, which centers on safeguarding data and systems against threats and vulnerabilities.

8. What tool did David use to gain full visibility while investigating a Google Cloud security incident?

A. Dynatrace

B. CloudTrail

C. Service Account

D. Cloud Monitoring

In the context of investigating a Google Cloud security incident, Dynatrace stands out as a tool that provides full visibility into application performance monitoring and user experiences. It offers insights into the complete technology stack, enabling investigators to trace transactions, monitor performance, and detect anomalies. This level of visibility is crucial when assessing the impact of any security incidents, allowing responders to analyze the behavior of applications and infrastructure in real-time. Other tools mentioned may play a role in cloud security but do not provide the comprehensive overview that Dynatrace offers. For instance, CloudTrail is primarily used for logging and monitoring actions taken within the AWS environment, which might not cater to Google Cloud specifically. Service Account refers to a type of account used to interact with services, but it does not provide monitoring capabilities. Cloud Monitoring can offer insights into the performance and health of applications but may not match the depth of visibility that Dynatrace provides through its detailed analytics and monitoring features. Thus, Dynatrace is recognized for its capability to deliver a holistic view during a security investigation, making it the appropriate choice.

9. Which recovery strategy is essential after handling an insider threat?

A. Implement a person-to-person rule for backups

B. Use cloud storage for all backups

C. Allow unrestricted access to backup resources

D. Discard old backups immediately

Implementing a person-to-person rule for backups is a crucial recovery strategy after handling an insider threat. This approach helps ensure that backup processes are carried out with a level of accountability and oversight. By requiring that two individuals are involved in the creation, storage, and recovery of backups, organizations can reduce the likelihood of further data manipulation or deletion by individuals with malicious intent. This strategy not only enhances security but also establishes checks and balances in the backup process, thereby minimizing risks associated with insider threats. In addition to enhancing security, this method fosters a culture of collaboration and diligence within the organization when managing critical data. It also provides a clear audit trail, making it easier to track any actions taken with sensitive data, which is particularly valuable when recovering from an incident involving insider threats. The effectiveness of this strategy stands in contrast to the other options, which may not provide a structured approach to dealing with backup integrity and security in the aftermath of insider threats.

10. Identify the tool employed by Caleb to analyze malware components and suspicious events.

A. Splunk Enterprise Security

B. Cylance

C. Malwarebytes

D. Avast Business

The identification of the tool used by Caleb to analyze malware components and suspicious events is rooted in the functionalities and capabilities of the chosen option. Splunk Enterprise Security is a robust security information and event management (SIEM) tool that excels in aggregating, analyzing, and visualizing data from various sources, including logs from different systems and devices. It is specifically designed for security monitoring and incident response, allowing analysts to detect anomalies, conduct investigations, and generate reports on security incidents. With its ability to handle large volumes of data and provide real-time insights, it is an ideal choice for analyzing suspicious events and understanding malware behaviors. The platform supports threat intelligence integration and can also be enhanced by custom searches and queries, making it versatile for security professionals who need to dissect and analyze potential malware activities effectively. While other options like Cylance, Malwarebytes, and Avast Business also provide various levels of malware detection and protection, they do not offer the broad analytical capabilities or the comprehensive data aggregation that a SIEM tool like Splunk does. Therefore, the selection of Splunk Enterprise Security is fitting for the task of malware analysis and investigation of suspicious events.

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!