Cyber Hero Certification Practice Test (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. Don’t worry about getting everything right, 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, and take breaks to retain information better.

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.

7. Use Other Tools

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 be monitored closely with respect to elevation of policy?**

   A. Change of system files

   B. Interaction of applications

   C. Incoming network traffic

   D. Performance of the operating system

2. **What does the CIA triad represent in cybersecurity?**

   A. Confidentiality, Integrity, and Availability

   B. Control, Information, and Access

   C. Compliance, Integration, and Assurance

   D. Confidentiality, Integrity, and Authentication

3. **When deploying ThreatLocker with a script via RMM, what should match your organization name?**

   A. identifier (lms-mm)

   B. deploymentID

   C. versionCode

   D. serviceName

4. **How does social media exploitation impact personal security?**

   A. It increases the risk of identity theft and phishing attacks

   B. It promotes awareness of online threats

   C. It helps to build strong online relationships

   D. It guarantees privacy in personal communications

5. **What feature is crucial when setting a policy in a secured state?**

   A. Allowing all changes to be made

   B. Having maximum restrictions on changing registry

   C. Monitoring without enforcement

   D. Allowing unlimited application access

6. What is "threat intelligence"?

- **A. Information that helps organizations understand potential cyber threats**
- **B. A method of improving network speed**
- **C. A type of firewall protection**
- **D. A software used for data encryption**

7. Which of the following is NOT a common type of malware?

- **A. Spyware**
- **B. Ransomware**
- **C. Router**
- **D. Trojan**

8. What does ThreatLocker do when it cannot match applications to built-in definitions?

- **A. It automatically denies the applications**
- **B. It creates custom rules for allowing updates**
- **C. It removes the applications from the system**
- **D. It generates alerts for manual review**

9. Which of the following best describes the role of a SIEM system?

- **A. To provide antivirus protection**
- **B. To aggregate and analyze security data**
- **C. To facilitate network speed enhancements**
- **D. To backup critical data regularly**

10. Where can tags be added within a policy?

- **A. On the user settings page**
- **B. Policy, internet, and custom rules dropdown**
- **C. Only in the main policy settings**
- **D. Tags cannot be added to policies**

Answers

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

Explanations

1. What should be monitored closely with respect to elevation of policy?

A. Change of system files

B. Interaction of applications

C. Incoming network traffic

D. Performance of the operating system

Monitoring the interaction of applications is crucial when it comes to policy elevation because this aspect directly affects the security and integrity of the system. When applications interact, especially with elevated privileges, there is a potential risk for malicious activity. Malicious actions can arise when one application, having gained elevated privileges, interacts with another application in ways that could compromise security policies or system integrity. Close monitoring of application interactions can help identify potential vulnerabilities, such as privilege escalation attacks, which exploit flaws in software to gain unauthorized access or control over system resources. By overseeing how these applications communicate and share data, organizations can ensure that no malicious processes are introduced and that security policies are adhered to. In contrast, while change of system files, incoming network traffic, and performance of the operating system are important for overall system health and security, they do not specifically address the risks associated with policy elevation in the way that monitoring application interactions does. Only by paying close attention to how applications interact can one fully understand the implications of elevated privileges on security policy compliance.

2. What does the CIA triad represent in cybersecurity?

A. Confidentiality, Integrity, and Availability

B. Control, Information, and Access

C. Compliance, Integration, and Assurance

D. Confidentiality, Integrity, and Authentication

The CIA triad is a foundational concept in cybersecurity that stands for Confidentiality, Integrity, and Availability. Confidentiality ensures that sensitive information is accessed only by authorized individuals or systems, thereby protecting private data from unauthorized exposure. This principle is crucial for maintaining the privacy and trust of users whose data is being processed or stored. Integrity refers to the accuracy and consistency of data over its lifecycle. It involves ensuring that data is not altered or tampered with, whether intentionally or accidentally. Maintaining data integrity is essential for reliability in decision-making processes based on that data. Availability ensures that systems and data are accessible when needed by authorized users. This principle emphasizes the importance of maintaining up-to-date and functioning systems that prevent downtime or loss of access that could disrupt business operations or critical services. Together, these three principles form the core goals of cybersecurity efforts, guiding strategies and measures to protect information systems and data. The other options introduce terms that are not foundational to the security framework and focus on aspects that do not encapsulate the primary concerns in the cybersecurity realm.

3. When deploying ThreatLocker with a script via RMM, what should match your organization name?

A. identifier (lms-mm)

B. deploymentID

C. versionCode

D. serviceName

In the context of deploying ThreatLocker with a script via Remote Monitoring and Management (RMM), the identifier (lms-mm) is crucial as it directly links to your organization. This identifier is used to ensure that the deployment process targets the correct environment and applies the necessary configurations specific to your organization. When an organization conducts software deployments, especially with security products like ThreatLocker, it is essential to maintain consistency and coherence in identifiers to avoid conflicts or misconfigurations. By ensuring that the identifier matches your organization name, you facilitate accurate deployment, tracking, and management of the software without the risk of affecting other organizations or misallocating resources. The other options—deploymentID, versionCode, and serviceName—play different roles in the deployment process. The deploymentID typically represents a unique identifier for a specific deployment instance but does not inherently tie back to your organization's identity. VersionCode refers to the version of the software being deployed, which is necessary for keeping the software current but does not signify organizational alignment. ServiceName indicates the particular service being utilized, which, while relevant, does not pertain to the identification of your organization. Thus, matching the identifier to your organization name is essential for ensuring that the deployment is recognized and associated with the correct

4. How does social media exploitation impact personal security?

A. It increases the risk of identity theft and phishing attacks

B. It promotes awareness of online threats

C. It helps to build strong online relationships

D. It guarantees privacy in personal communications

Social media exploitation significantly increases the risk of identity theft and phishing attacks due to the vast amount of personal information shared on these platforms. When individuals disclose details such as their full names, birthdays, locations, and even personal interests, this information can be leveraged by malicious actors to impersonate them or to craft targeted phishing schemes. For instance, a fraudster might use information gathered from a person's social media profile to create convincing messages that appear to be from trusted sources, ultimately tricking the individual into providing sensitive information or access to accounts. Moreover, social media often encourages sharing of experiences, which can inadvertently reveal additional personal data that increases vulnerability. Consequently, the open nature of social media platforms makes it easier for cybercriminals to gather information that can be used to exploit individuals. It underscores the importance of understanding privacy settings and being cautious about the information shared online, as the consequences can directly impact personal security.

5. What feature is crucial when setting a policy in a secured state?

A. Allowing all changes to be made

B. Having maximum restrictions on changing registry

C. Monitoring without enforcement

D. Allowing unlimited application access

The feature that is crucial when setting a policy in a secured state is having maximum restrictions on changing the registry. This is because the registry is a critical component of the operating system that controls many settings and functions. If changes to the registry are not properly restricted, it can lead to unauthorized alterations that may compromise system integrity, security, and performance. By implementing maximum restrictions on registry changes, organizations can prevent malware and unauthorized users from making harmful modifications. This also ensures that only approved changes are made by authorized personnel, which is essential for maintaining a secure environment. In a secured state, it is vital to control who can make alterations to important system configurations, thus reinforcing the overall security posture. The other options suggest a lack of control or oversight, which would be detrimental to maintaining security. Allowing all changes, monitoring without enforcement, or granting unlimited application access could lead to vulnerabilities and risks within the system.

6. What is "threat intelligence"?

A. Information that helps organizations understand potential cyber threats

B. A method of improving network speed

C. A type of firewall protection

D. A software used for data encryption

Threat intelligence refers to the information that organizations gather and analyze to understand potential and existing cyber threats. This encompasses insights into hacker tactics, techniques, and procedures, as well as knowledge about vulnerabilities that could be exploited. By utilizing threat intelligence, organizations can enhance their defensive strategies, anticipate possible attacks, and respond effectively to security incidents. This proactive approach allows businesses to adapt their cybersecurity measures based on the evolving threat landscape. The other choices do not align with the definition of threat intelligence. Improving network speed pertains to performance optimization rather than security threats. Firewall protection relates specifically to establishing barriers against unauthorized access, while data encryption is focused on securing data through obfuscation. Thus, only the first option accurately describes what threat intelligence encompasses in the context of cybersecurity.

7. Which of the following is NOT a common type of malware?

A. Spyware

B. Ransomware

C. Router

D. Trojan

The choice identified as the correct answer refers to "Router," which is not classified as a common type of malware. Malware encompasses various malicious software designed to disrupt, damage, or gain unauthorized access to computer systems. Common types of malware include spyware, ransomware, and trojans, each serving different malicious purposes. Spyware secretly observes user activity and can collect sensitive information. Ransomware is designed to encrypt files on a victim's system, demanding payment for the decryption key. Trojans disguise themselves as legitimate software to trick users into installing them, often leading to unauthorized access or damage. A router, on the other hand, is a hardware device that directs data traffic between devices on a network. It does not fit into the category of malware because it is not inherently malicious software; rather, it is a vital component of networking infrastructure. Understanding these distinctions is essential for recognizing and identifying the threats posed by malware as well as the legitimate roles of network devices.

8. What does ThreatLocker do when it cannot match applications to built-in definitions?

A. It automatically denies the applications

B. It creates custom rules for allowing updates

C. It removes the applications from the system

D. It generates alerts for manual review

ThreatLocker is designed to enhance security by controlling which applications are allowed to run on a system. When it encounters an application that does not match any of its built-in definitions, the standard procedure is to create custom rules for that specific application. This approach ensures that legitimate software can continue to operate while also maintaining a strong security posture. Creating custom rules allows administrators to tailor security measures according to specific needs and use cases without outright denying access to potentially necessary applications. This flexibility helps organizations avoid disruptions in their operations, facilitating updates and installations while still adhering to security protocols. Ultimately, this process balances security with usability, allowing for dynamic responses to new or unidentified applications in the environment.

9. Which of the following best describes the role of a SIEM system?

A. To provide antivirus protection

B. To aggregate and analyze security data

C. To facilitate network speed enhancements

D. To backup critical data regularly

A Security Information and Event Management (SIEM) system plays a crucial role in cybersecurity by aggregating and analyzing security data from various sources within an organization's IT infrastructure. This includes log data from servers, network devices, and security appliances, as well as event information from various applications. The primary function of a SIEM system is to provide real-time analysis of security alerts generated by applications and network hardware. By correlating different types of events and data points, a SIEM can identify potential security threats, detect anomalies, and assist in responding to incidents more effectively. In contrast, antivirus protection focuses specifically on detecting and mitigating malware; enhancing network speed pertains to improving the performance of data transmission; and backing up critical data regularly is aimed at data recovery and integrity rather than security analysis. Therefore, the role of a SIEM system is accurately described by its capacity to aggregate and analyze security data for improved monitoring and incident response.

10. Where can tags be added within a policy?

A. On the user settings page

B. Policy, internet, and custom rules dropdown

C. Only in the main policy settings

D. Tags cannot be added to policies

Tags play an important role in organizing and managing policies, allowing for easier identification and filtering. Within a policy structure, tags can typically be added across various settings and areas of a policy management system. The correct answer indicates that tags can be integrated in multiple places such as the policy itself, internet settings, and custom rules dropdowns. This flexibility enhances the ability to categorize and quickly access relevant policies based on specific tags, thereby streamlining policy management processes. In contrast, other options present more restrictive views. The suggestion that tags can only be added in the main policy settings overlooks the wider utility and application of tags in related areas. Additionally, implying that tags cannot be added to policies dismisses their invaluable function in enhancing organizational efficiency and clarity in policy management.

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://cyberherocert.examzify.com

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