ThreatLocker Practice Exam (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. Which statement is true regarding file permissions and security?

A. Combination of path, process, and created is least secure

B. All methods provide equal levels of security

C. Only hash-based permissions are reliable

D. Certificate permissions are always less secure

2. Which modes disable file blocking temporarily?

A. Only installation mode

B. Only learning mode

C. Both installation mode and learning mode

D. None of the above

3. What does Bob's custom rule allow regarding .dll files?

A. Allow any .dll in a specific directory to run if called by a specific process

B. Prevent all .dll files from executing

C. Only allow .dll files created today to run

D. Permit execution based on user credentials

4. Why is regular software updates important?

A. To increase the application size

B. To enhance security and functionality

C. To slow down system performance

D. To limit compatibility with new hardware

5. How can you set a policy to observe registry changes made by an application without blocking those actions?

A. Permit the application with Ringfencing and set status to "Block All"

B. Allow all changes and ignore endpoint security settings

C. Permit the application with Ringfencing, set the status to "Monitor Only", and select "Restrict these applications from making registry changes except for below rules"

D. Set the application to "Disabled" and monitor changes manually

6. In the ThreatLocker Portal, what is the purpose of the Approval Center?

A. To manage application settings

B. To view all approval requests from end users

C. To configure system alerts

D. To review user activity logs

7. Where will you find a list of organizations you have permission to view in the ThreatLocker Portal?

A. Organizations

B. My Accounts

C. Classes

D. Permissions Dashboard

8. What feature allows multiple computers to quickly enter learning mode without individual configuration?

A. Schedule maintenance button

B. Enable learning mode individually

C. Utilize batch processing

D. Access the admin dashboard

9. How often should ThreatLocker policies be reviewed?

A. Annually

B. Monthly

C. Quarterly or upon significant changes

D. Weekly

10. What action is triggered by a health alert with a severity of 'Danger'?

A. No change in threat level

B. Increase threat level by 5

C. Increase threat level by 10

D. Increase threat level by 1

Answers

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

Explanations

1. Which statement is true regarding file permissions and security?

A. Combination of path, process, and created is least secure

B. All methods provide equal levels of security

C. Only hash-based permissions are reliable

D. Certificate permissions are always less secure

The statement regarding file permissions and security that is accurate is that a combination of path, process, and created is the least secure. This is because relying on these factors alone can create vulnerabilities in the security model. Individually, each of these elements plays a role in the overall security framework, but when they are the sole focus, they may fall short of providing comprehensive protection. An attacker could exploit weaknesses in any one of these components to circumvent security measures. For example, if permissions are solely based on the file path, an attacker might manipulate the request to access a location they shouldn't be able to reach. Similarly, focusing only on the process or the creation date can fail to account for newer threats that might bypass these checks. Therefore, a more robust security approach would utilize a combination of more comprehensive security mechanisms, including user roles, dynamic checks, and behavior monitoring, rather than relying on any single or combination of these elements limitedly.

2. Which modes disable file blocking temporarily?

A. Only installation mode

B. Only learning mode

C. Both installation mode and learning mode

D. None of the above

The correct choice indicates that both installation mode and learning mode temporarily disable file blocking. In installation mode, the purpose is to allow new applications and files to be installed without being blocked by existing security policies. This is essential for ensuring that necessary software can be added to a system without unnecessary interruptions. During this mode, file blocking is disabled to facilitate the smooth installation of software. Similarly, learning mode is designed to observe the behavior of applications without imposing strict security constraints. This allows the system to learn which files and processes are benign and should be allowed in the future. By disabling file blocking temporarily during this mode, it enables the system to gather the necessary data to create appropriate security policies based on the observed application behavior. Both modes are focused on ensuring that essential operations can be performed without hindrance, whether it's installing new software or learning from the user's environment. This allows for a seamless user experience while still maintaining overall security once the system reverts back to its normal operational modes.

3. What does Bob's custom rule allow regarding .dll files?

A. Allow any .dll in a specific directory to run if called by a specific process

B. Prevent all .dll files from executing

C. Only allow .dll files created today to run

D. Permit execution based on user credentials

The choice indicating that Bob's custom rule allows any .dll file in a specific directory to run if called by a specific process highlights a key aspect of application control and whitelisting within security frameworks. In this context, the custom rule provides a nuanced approach to security by allowing flexibility where certain .dll files can be executed under controlled circumstances, specifically when invoked by designated processes. This method is beneficial for maintaining system functionality while still enforcing security measures, as it ensures that only designated .dll files are permitted to run, reducing the risk of unauthorized or malicious code execution. By specifying both the location (directory) and the circumstances (called by a specific process), the rule creates a targeted exception to a broader set of restrictions, enhancing operational efficiency without significantly compromising security. Other choices imply more restrictive or broad approaches to file execution that may inhibit necessary operations or lack the precision found in the custom rule. For example, preventing all .dll files from executing would limit necessary system functionalities, while allowing only newly created .dll files or basing execution on user credentials could introduce vulnerabilities or administrative challenges without the same level of specificity in defining safe interactions.

4. Why is regular software updates important?

A. To increase the application size

B. To enhance security and functionality

C. To slow down system performance

D. To limit compatibility with new hardware

Regular software updates are crucial because they serve two primary purposes: enhancing security and improving functionality. Software, by its nature, can have vulnerabilities that malicious actors can exploit. When developers become aware of these security flaws, they issue updates to patch those vulnerabilities, thus protecting users from potential threats such as malware, ransomware, or data breaches. In addition to security enhancements, updates often include new features or improvements to existing functionalities that make the software more efficient and user-friendly. This can lead to better performance and increased capabilities, allowing users to work more effectively. Through regular updates, software remains compatible with the latest technologies and hardware, ensuring a smooth experience for the user. This proactive approach helps to maintain and improve the overall health of the software ecosystem.

5. How can you set a policy to observe registry changes made by an application without blocking those actions?

A. Permit the application with Ringfencing and set status to "Block All"

B. Allow all changes and ignore endpoint security settings

C. Permit the application with Ringfencing, set the status to "Monitor Only", and select "Restrict these applications from making registry changes except for below rules"

D. Set the application to "Disabled" and monitor changes manually

Setting a policy to observe registry changes made by an application without blocking those actions requires a specific configuration that allows monitoring without interference. The correct approach is to permit the application with Ringfencing, set the status to "Monitor Only", and define specific rules that restrict certain applications from making registry changes. This method enables the observation of registry activities while maintaining the functional capability of the application, thus providing insights into its behavior without the risk of blocking critical operations. By selecting "Monitor Only," you ensure that all changes made by the application are logged and can be reviewed later, but they do not automatically trigger any blocking actions that could disrupt the application's operation. The additional customization of restricting which applications can make such changes further refines the monitoring process, allowing you to maintain control over the environment while gaining visibility into registry modifications. In contrast, the other choices do not achieve the intended goal of monitoring registry changes without blocking. Some options suggest altering application statuses in a way that either permits all actions or disables monitoring entirely, which does not provide the nuanced control needed for effective tracking. This comprehensive approach helps maintain security while also enabling thorough oversight of application behaviors.

6. In the ThreatLocker Portal, what is the purpose of the Approval Center?

A. To manage application settings

B. To view all approval requests from end users

C. To configure system alerts

D. To review user activity logs

The Approval Center in the ThreatLocker Portal is specifically designed for the purpose of viewing all approval requests from end users. This functionality is critical in managing and overseeing the requests initiated by users who may require additional permissions to run applications or access certain functionalities that are not readily available under their current configurations. By consolidating these requests in one centralized location, administrators can efficiently review, approve, or deny the requests based on their organization's policies and security protocols. This process enhances the overall workflow within the organization, ensuring that end users have timely access to necessary resources while maintaining strict security measures. The other functions or features mentioned, such as managing application settings, configuring system alerts, or reviewing user activity logs, serve different purposes within the portal and do not directly relate to the specific action of handling user approval requests. These aspects contribute to the comprehensive management of the security environment, but they are distinct from the core purpose of the Approval Center.

7. Where will you find a list of organizations you have permission to view in the ThreatLocker Portal?

A. Organizations

B. My Accounts

C. Classes

D. Permissions Dashboard

The correct choice is "Organizations" because this section provides a centralized location where users can view all the organizations they have access to within the ThreatLocker Portal. It is specifically designed to display the list of organizations to which users have been granted permission, making it easy to manage and navigate their roles and responsibilities. This allows users to efficiently track their access rights and the organizations they are allowed to manage. Other options, while related to user accounts or permissions, do not serve the same purpose. "My Accounts" typically pertains to personal account settings and information. "Classes" may refer to training or categorization within the system but does not directly indicate access permissions. The "Permissions Dashboard" might provide an overview of permissions but does not specifically list the organizations the user can view. Thus, the "Organizations" section is the focused area for checking access listings effectively.

8. What feature allows multiple computers to quickly enter learning mode without individual configuration?

A. Schedule maintenance button

B. Enable learning mode individually

C. Utilize batch processing

D. Access the admin dashboard

The feature that allows multiple computers to quickly enter learning mode without the need for individual configuration is the schedule maintenance button. This functionality streamlines the process by enabling an administrator to set a specific timeframe during which learning mode is activated for all designated machines simultaneously. This is particularly useful for managing multiple devices in an organization, as it reduces the administrative burden and ensures that the systems can be configured for learning mode at once, aligning with network maintenance schedules. In contrast, the other options would require either manual configuration or do not focus specifically on the collective adjustment of settings across multiple devices, which makes them less efficient for this purpose. For instance, enabling learning mode individually necessitates logging into each computer separately, while utilizing batch processing and accessing the admin dashboard may not provide a direct or immediate means to initiate learning mode for multiple devices at once. Therefore, the scheduled maintenance capability is the most effective approach for configuring multiple systems in a unified manner.

9. How often should ThreatLocker policies be reviewed?

A. Annually

B. Monthly

C. Quarterly or upon significant changes

D. Weekly

Regularly reviewing ThreatLocker policies is crucial for maintaining effective security measures in an organization. The choice of reviewing policies quarterly or upon significant changes strikes a balance between ensuring that the policies remain up-to-date and relevant while not overwhelming the administrative processes with unnecessary frequency. A quarterly review allows organizations to assess their policies systematically throughout the year, taking into account any developments in technology, emerging threats, or changes in business operations that may require policy adjustments. Significant changes, such as implementation of new software, changes in the IT infrastructure, or shifts in the company's risk profile, can be pivotal moments that necessitate an immediate review of security policies. This responsive element ensures policies adapt to the evolving landscape of cybersecurity threats effectively. By following this approach, companies can maintain a proactive security posture, minimizing vulnerabilities that could be exploited by attackers, and ensuring that the policies align with the current operational framework.

10. What action is triggered by a health alert with a severity of 'Danger'?

A. No change in threat level

B. Increase threat level by 5

C. Increase threat level by 10

D. Increase threat level by 1

When a health alert is assigned a severity of 'Danger,' it indicates a critical issue that could significantly threaten the security or operational integrity of the system. As such, a health alert with this severity level necessitates a substantial response to reflect the seriousness of the situation. Increasing the threat level by 10 is an appropriate action for a 'Danger' alert because it demonstrates the urgent need for immediate attention and prioritization within the security framework. Such a response allows the system to recalibrate its defenses and actions to address the imminent risk effectively. It ensures that the security measures in place can respond adequately to the severity of the threat represented by a health alert of this nature. In summary, the decision to increase the threat level by 10 corresponds to the gravity of the situation indicated by a 'Danger' health alert, enabling an appropriate and proactive approach to threat 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://threatlocker.examzify.com

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