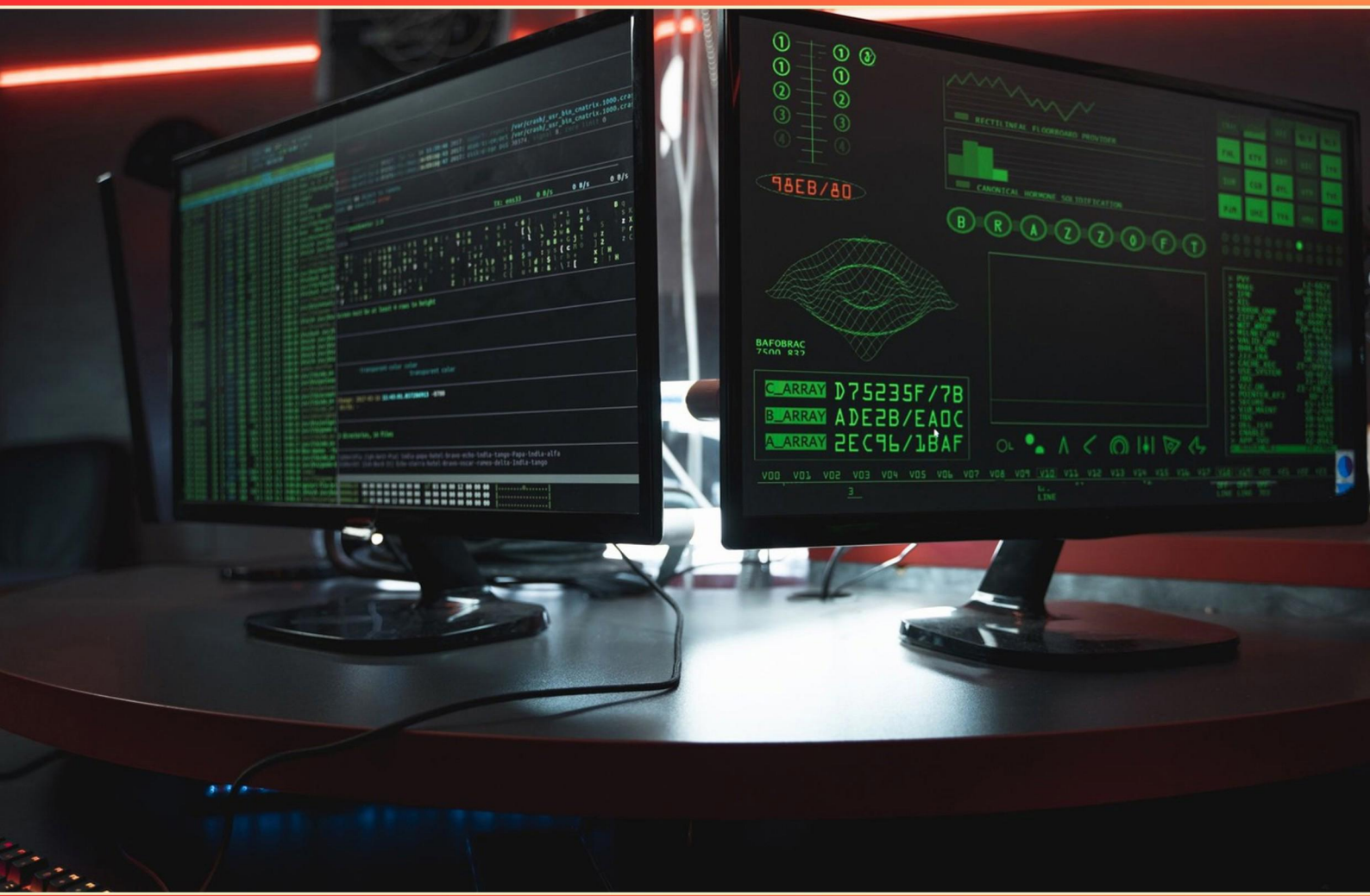
THREATLOCKER PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://threatlocker.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. **Where is the InstallKey located according to the ThreatLocker Portal documentation?**

   A. In the configuration settings

   B. In the MSI or Stub Installer file names

   C. In the user's profile

   D. In the deployment reports

2. **If both an organization-level policy and a computer group-level Elevation policy exist for the same application, which policy takes precedence?**

   A. The computer group-level Elevation policy

   B. The organization-level policy

   C. The policy with the most recent modification date

   D. There is no precedence; both policies function simultaneously

3. **Which types of files are included in the protected files by default?**

   A. External drives and local files

   B. Network shares and external storage

   C. USB devices and cloud storage

   D. Application logs and local configuration files

4. **What status should you strive to keep your endpoints in to ensure maximum protection?**

   A. Learning mode

   B. Audit mode

   C. Secure mode

   D. Warning mode

5. **What is the default selection for creating and applying policies after the Baseline upload?**

   A. User policies only

   B. Computer policies only

   C. Device policies only

   D. Network policies only

SAMPLE

6. What happens once the elevation on an application expires?

A. The application will no longer be accessible

B. The application can be run as a normal user

C. The user must request an extension

D. The application is automatically uninstalled

7. In the context of ThreatLocker, what does 'Info' signify regarding threat levels?

A. Log the event

B. Increase threat level by 10

C. Increase threat level by 1

D. Increase threat level by 5

8. How does ThreatLocker assist in compliance regulations?

A. By encrypting all data transfers

B. By providing visibility and control over applications and data

C. By conducting regular audits

D. By limiting user access to essential services

9. Which component allows for the organized grouping of computers in the ThreatLocker Portal?

A. Device management

B. Computer groups

C. Policy settings

D. Installation icons

10. Which ThreatLocker Module(s) can ThreatLocker Ops interact with?

A. Only the Configuration Manager

B. Specific security modules only

C. All ThreatLocker modules

D. Only custom modules created by the user

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Where is the InstallKey located according to the ThreatLocker Portal documentation?

A. In the configuration settings

B. In the MSI or Stub Installer file names

C. In the user's profile

D. In the deployment reports

The InstallKey is found in the MSI or Stub Installer file names according to the ThreatLocker Portal documentation. This key is crucial for identifying and authenticating the software installation process within the ThreatLocker environment. The integration of the InstallKey in these file names ensures that the installation adheres to the security protocols set by ThreatLocker, allowing for a streamlined deployment process. Using the InstallKey from the installer file ensures that only authorized installations take place, enhancing the overall security framework of the system. This method of embedding the key within the installer files also simplifies tracking and management of installations across devices in an organization.

2. If both an organization-level policy and a computer group-level Elevation policy exist for the same application, which policy takes precedence?

A. The computer group-level Elevation policy

B. The organization-level policy

C. The policy with the most recent modification date

D. There is no precedence; both policies function simultaneously

In the scenario where both an organization-level policy and a computer group-level Elevation policy are defined for the same application, the organization-level policy is the one that takes precedence. This is because organization-level policies are typically designed to provide a broader, overarching framework that applies to all relevant entities within the organization, including all groups and computers unless specifically overridden. In practice, this means that any restrictions or permissions set at the organization level will govern how the application behaves across various departments or computer groups. The organization-level policies ensure a standardized approach to security and application usage, aligning with the organization's overall compliance and operational strategies. The other considerations, such as modification dates or the idea of simultaneous operation, do not apply in this context since the organization-level policy is inherently intended to supersede more localized policies unless explicitly stated otherwise.

SAMPLE

3. Which types of files are included in the protected files by default?

A. External drives and local files

B. Network shares and external storage

C. USB devices and cloud storage

D. Application logs and local configuration files

The correct choice highlights that by default, ThreatLocker includes network shares and external storage as protected file types. This is significant because these types of files are commonly accessed in a business environment and often contain sensitive or critical information that could be at risk if not adequately protected. Network shares serve as central repositories for files that multiple users can access over a network, making them particularly vulnerable to unauthorized access or data breaches. External storage, such as USB drives or external hard drives, can easily be connected to a system and pose security risks if the data they carry is not properly secured. Protecting these file types helps to ensure that sensitive information remains secure from potential threats such as malware, accidental deletion, or unauthorized access In contrast, while other options may include file types that could be relevant in different contexts, they do not represent the default settings of protected files within ThreatLocker. This distinction emphasizes the focus on securing files that are frequently shared and stored outside of local environments.

4. What status should you strive to keep your endpoints in to ensure maximum protection?

A. Learning mode

B. Audit mode

C. Secure mode

D. Warning mode

To ensure maximum protection for your endpoints, maintaining them in Secure mode is essential. In Secure mode, the endpoint operates with strict controls over what applications and processes can execute. This helps to minimize potential vulnerabilities by ensuring that only trusted applications are allowed to run, effectively reducing the risk of malware and unauthorized access. In this mode, the system actively blocks any applications or processes that are not explicitly allowed, providing a robust defense against threats. This proactive approach is fundamental for maintaining the integrity and security of the endpoint environment, protecting sensitive data and resources from cyber threats. By ensuring that all applications are vetted and authorized, organizations can achieve a high level of security and compliance with industry regulations.

SAMPLE

5. What is the default selection for creating and applying policies after the Baseline upload?

A. User policies only

B. Computer policies only

C. Device policies only

D. Network policies only

The default selection for creating and applying policies after the Baseline upload is related to the way ThreatLocker manages security policies. When managing security through ThreatLocker, policies can be established based on the attributes of computers, users, devices, or networks. Focusing on computer policies, they provide a means to control applications and processes at the machine level. This is crucial because it allows for a standard configuration that fits the security needs of the organization. After the Baseline upload, the emphasis on computer policies ensures that the foundational rules governing application behavior on devices are set, providing a baseline of security that can then be expanded upon with additional user, device, or network policies as necessary. By prioritizing computer policies by default, ThreatLocker helps organizations ensure that the machines are already under secure guidelines before any additional layers are added. This method ensures a more secure starting position from which to build out further, granular controls.

6. What happens once the elevation on an application expires?

A. The application will no longer be accessible

B. The application can be run as a normal user

C. The user must request an extension

D. The application is automatically uninstalled

Once the elevation on an application expires, the application can indeed be run as a normal user. When elevation is applied to an application, it allows increased permissions for specific tasks. Once the time limit for that elevated state runs out, those elevated privileges are revoked, and the application defaults back to operating under the standard user permissions level. This means that while the application is still accessible, it will no longer have the extra permissions granted during elevation. This evolution is an important part of maintaining security; it reduces the risk associated with running applications with elevated privileges unnecessarily. Users can still run the application, but they may encounter limitations based on their current user permissions.

7. In the context of ThreatLocker, what does 'Info' signify regarding threat levels?

A. Log the event

B. Increase threat level by 10

C. Increase threat level by 1

D. Increase threat level by 5

'Info' in the context of ThreatLocker signifies an increase in threat level by 1. This classification is typically associated with events that may not pose an immediate or critical threat but are still noteworthy for monitoring and awareness. By assigning a threat level increase of 1, ThreatLocker helps organizations prioritize their response to potential security issues without overreacting to minor events. This incremental approach allows security teams to build a comprehensive understanding of the threat landscape while maintaining focus on more significant threats that might require urgent attention. A lower-level threat adjustment, such as 1, ensures that the overall threat management system remains responsive and effective, fostering a proactive security posture. Understanding the significance of distinguishing between different threat levels is essential for effective incident response and resource allocation in cybersecurity practices.

SAMPLE

8. How does ThreatLocker assist in compliance regulations?

A. By encrypting all data transfers

B. By providing visibility and control over applications and data

C. By conducting regular audits

D. By limiting user access to essential services

ThreatLocker assists in compliance regulations primarily by providing visibility and control over applications and data. This functionality is critical for organizations striving to adhere to various compliance standards, such as GDPR, HIPAA, and PCI-DSS. Visibility allows organizations to monitor and track application usage, ensuring that only authorized applications are running in their environments. This helps to limit unauthorized data access and reduces the potential for data breaches, which is a significant compliance concern. Control mechanisms available through ThreatLocker enable organizations to enforce policies surrounding application and data usage. This includes whitelisting trusted applications and blocking unapproved ones, creating a more secure IT environment that is crucial for meeting regulatory requirements. In contrast, while encryption, audits, and limiting access can contribute to compliance efforts, they do not specifically address the need for comprehensive visibility and control that ThreatLocker offers. Encryption protects data in transit, audits assess compliance after the fact, and limiting user access is just one aspect of a broader strategy for managing applications and data. Hence, ThreatLocker's primary value lies in its capability to provide detailed oversight and governance, which is a cornerstone of effective compliance management.

9. Which component allows for the organized grouping of computers in the ThreatLocker Portal?

A. Device management

B. Computer groups

C. Policy settings

D. Installation icons

The ability to organize and manage computers effectively within the ThreatLocker Portal is achieved through the use of computer groups. This feature allows administrators to categorize computers based on various factors such as department, function, or security level. By grouping computers in this manner, it becomes easier to implement specific policies and manage access controls for those specific groups, enhancing the overall security and efficiency of operations. Organizing computers into groups fosters a streamlined administration process, enabling more efficient policy management and monitoring. For instance, an organization might want to apply stricter security measures on computers used for sensitive operations. By creating a dedicated group for this purpose, the administrator can easily manage and enforce relevant policies tailored to that group. The other choices refer to distinct functionalities within the ThreatLocker system but do not specifically focus on the aspect of organized grouping of computers. Device management pertains more to the management and oversight of individual devices rather than grouping. Policy settings involve the rules and guidelines applicable to the devices but do not provide a mechanism for organization. Installation icons are related to the software's user interface and do not directly influence how computers are grouped or managed within the portal.

SAMPLE

10. Which ThreatLocker Module(s) can ThreatLocker Ops interact with?

A. Only the Configuration Manager

B. Specific security modules only

C. All ThreatLocker modules

D. Only custom modules created by the user

The correct response, emphasizing that ThreatLocker Ops can interact with all ThreatLocker modules, underscores the versatility and comprehensive functionality of the Ops platform. This capability allows ThreatLocker Ops to manage and oversee various aspects of security, ensuring cohesive operation across different modules. By interacting with every module, ThreatLocker Ops enables users to streamline operations, efficiently implement policies, and optimize security measures across the entire ThreatLocker ecosystem. This broad access empowers users to adjust settings and configure multiple components from a single interface, enhancing their ability to respond to security needs dynamically and definitively. Moreover, it facilitates better monitoring and reporting, as users can assess the performance and compliance of all modules in real time. This holistic approach is vital for effective cybersecurity management, ensuring all threats can be addressed uniformly without gaps in security protocols.

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://threatlocker.examzify.com

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

SAMPLE