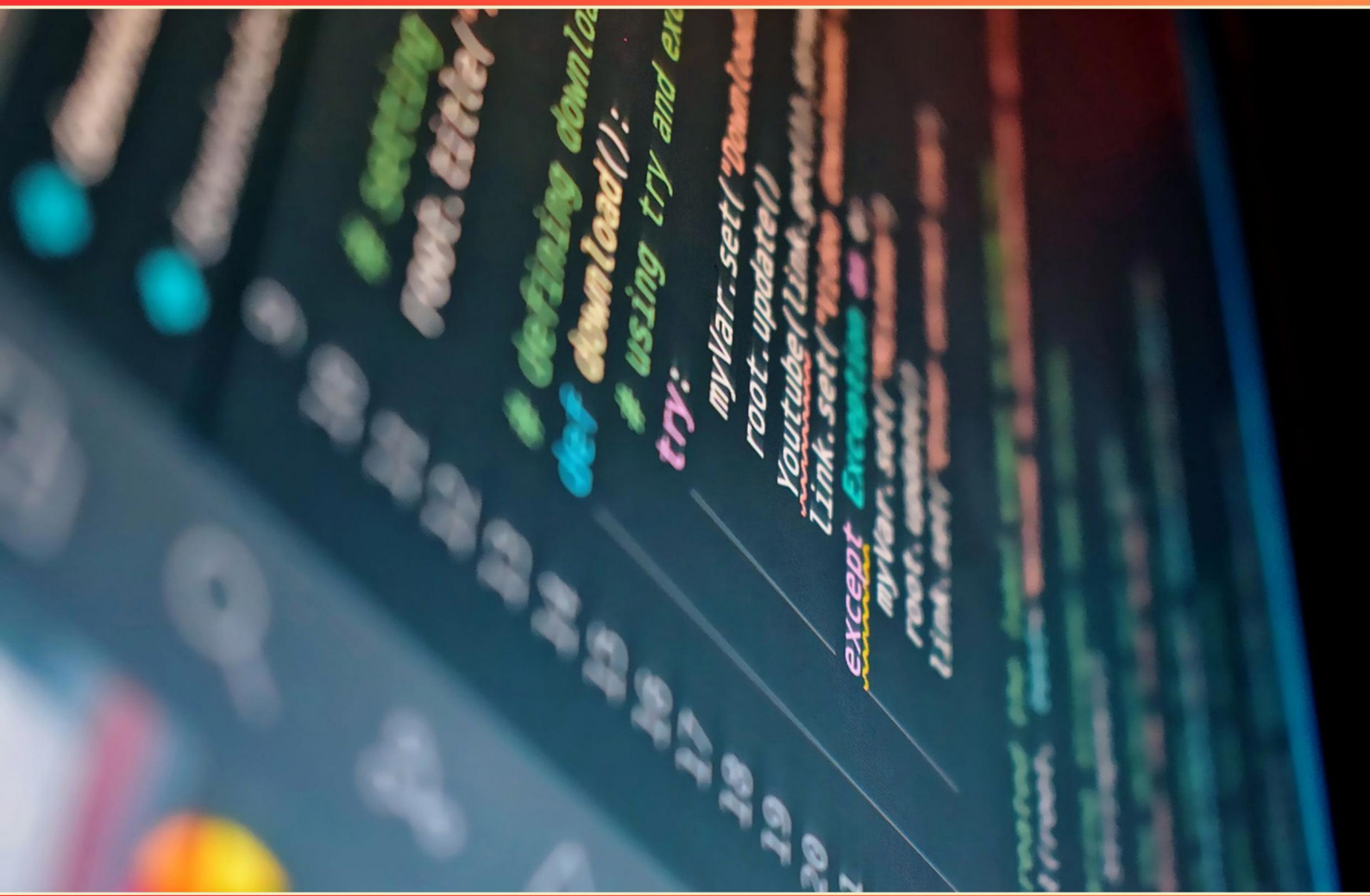
TREND MICRO DEEP SECURITY CERTIFICATION PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://trendmicrodeepsecurity.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. Which rule will be applied first if priorities are the same?

A. Force Allow

B. Log Only

C. Deny

D. Bypass

2. What capability does Behavior Monitoring offer in anti-malware solutions?

A. Identifies all virus signatures

B. Helps in defining malware scan schedules

C. Detects suspicious files that may indicate emerging malware

D. Prevents all file access without user permission

3. What is the purpose of event tags in Deep Security Manager?

A. To categorize events based on severity

B. To denote events that require action versus those that have been resolved

C. To store event metadata for auditing

D. To generate automatic reports

4. Can you incorporate the results of a recommendation scan in a new policy?

A. No, it's not possible

B. Yes, but only certain configurations

C. Yes, you can select recommended application types and rules

D. Yes, but only for anti-malware settings

5. How does Standard Auto-Tagging work in Deep Security Manager?

A. It tags events occurring on all computers

B. It uses an existing event model for tagging similar events

C. It automatically creates tags based on user settings

D. It removes tags from events that are considered fixed

6. Which Intrusion Prevention rule specifically targets Cross-Site Scripting (XSS) vulnerabilities?

A. 1000608

B. 1000552

C. 1000100

D. 1000200

SAMPLE

7. What should a tenant user do if they do not receive the activation email after account creation?

A. Contact support for manual activation

B. Wait for 24 hours for automatic activation

C. Resend the account creation request

D. Log in directly with default credentials

8. When creating an NSX Security Policy, what service must be enabled for Deep Security?

A. Network Counseling Service

B. Guest Introspection Service

C. Network Introspection Service

D. Service Profile Management

9. Which of the following is NOT true about Deep Security Virtual Appliance activation?

A. It works the same way as Deep Security Agent activation

B. It initiates Virtual Agent instantiation

C. It can be activated on unprepared ESXi machines

D. It allows for self-protection of the virtual appliance

10. What is the purpose of the Add Directory Wizard in Deep Security Manager?

A. To add users to the system

B. To populate the Computers list using Active Directory information

C. To configure firewall rules automatically

D. To perform vulnerability assessments

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which rule will be applied first if priorities are the same?

A. Force Allow

B. Log Only

C. Deny

D. Bypass

When multiple rules have the same priority in a security configuration, the system will typically apply the rule that is defined as the "Bypass" first. This is because the Bypass rule allows the specified traffic to pass through without any further inspection or control, which serves as a means to allow certain traffic to avoid all processing for efficiency or performance reasons. In many security systems, Bypass rules are designed to ensure that critical applications or traffic that must not be hindered by other security checks are processed immediately, regardless of other rules at the same priority level. This ensures business continuity and optimal performance for essential services, as these rules take precedence over others that may apply additional constraints or logging. While other types of rules such as Force Allow, Log Only, and Deny also serve important functions in managing security policy, they do not take priority over the Bypass rule when priorities are equal. Force Allow explicitly allows traffic; Log Only would just log the instance for future reference without taking action; Deny, conversely, blocks traffic. However, when the rules have identical priorities, the need to bypass certain checks for operational efficiency results in the Bypass rule being applied first.

2. What capability does Behavior Monitoring offer in anti-malware solutions?

A. Identifies all virus signatures

B. Helps in defining malware scan schedules

C. Detects suspicious files that may indicate emerging malware

D. Prevents all file access without user permission

Behavior Monitoring in anti-malware solutions plays a crucial role in identifying potentially malicious activity by observing the behavior of files and applications in real-time. The correct choice highlights its capability to detect suspicious files that may indicate emerging malware. This is vital because it allows the anti-malware software to identify threats that may not yet have a known signature in the virus database, thus providing a proactive approach to security. This type of monitoring can flag files that exhibit characteristics typical of malware, such as unauthorized network communication, unusual file modifications, or attempts to exploit vulnerabilities. By detecting such behaviors, the system can take action before the malware fully executes or spreads, thus enhancing overall protection for users. In contrast, the other options do not encapsulate the primary function of Behavior Monitoring. Identifying all virus signatures relates more to traditional signature-based detection methods, which rely on a database of known threats. Defining malware scan schedules pertains to system administration tasks, while preventing all file access without user permission would severely limit system functionality and is not a practical approach for anti-malware solutions.

SAMPLE

3. What is the purpose of event tags in Deep Security Manager?

A. To categorize events based on severity

B. To denote events that require action versus those that have been resolved

C. To store event metadata for auditing

D. To generate automatic reports

Event tags in Deep Security Manager serve the purpose of denoting different states or categories of events, particularly highlighting those that require action and distinguishing them from those that have already been resolved. This tagging facilitates efficient monitoring and responsiveness by allowing administrators to quickly identify which issues need immediate attention. By enabling clear differentiation between open and resolved events, it enhances the workflow of security operations, making it easier for teams to prioritize their efforts in managing security incidents. The capability to apply and track event tags streamlines the incident response process, ensuring that critical threats are addressed promptly while allowing resolved issues to be archived for reference. Each of the other choices does play a role in event management in security contexts, but they do not specifically align with the primary function of event tags in Deep Security Manager. For instance, categorizing events based on severity is a separate function that involves prioritizing incidents but does not focus on the actionable versus resolved status. Similarly, storing event metadata for auditing is crucial for compliance and analysis, but it does not pertain to the immediate operational status of events. Lastly, generating automatic reports is a key feature for statistical insight, yet it stands apart from the tagging system, which is aimed more at real-time event management and response.

4. Can you incorporate the results of a recommendation scan in a new policy?

A. No, it's not possible

B. Yes, but only certain configurations

C. Yes, you can select recommended application types and rules

D. Yes, but only for anti-malware settings

The ability to incorporate the results of a recommendation scan into a new policy is a powerful feature of Trend Micro's Deep Security. When a recommendation scan is performed, it evaluates the environment and provides suggestions for security measures based on the current configuration and any vulnerabilities detected. Selecting recommended application types and rules allows administrators to tailor their security policies to align with best practices and specific needs of the environment. This means you can enhance your security posture by implementing recommendations that are well-suited for the applications and services running within your infrastructure. Such customization can help in efficiently managing security settings, minimizing risks, and ensuring compliance with security standards. Incorporating these recommendations not only assists in improving security but also aids in streamlining configuration management by adopting best practices that are specifically relevant to the applications being used. This options provides flexibility to security teams looking to enhance their policies and defenses without starting from scratch.

SAMPLE

5. How does Standard Auto-Tagging work in Deep Security Manager?

A. It tags events occurring on all computers

B. It uses an existing event model for tagging similar events

C. It automatically creates tags based on user settings

D. It removes tags from events that are considered fixed

Standard Auto-Tagging in Deep Security Manager functions by utilizing an existing event model to tag similar events. This means that the system can automatically categorize and label events based on predefined criteria and patterns identified within the event model. By doing so, it simplifies the management and organization of events, making it easier for users to track and respond to security incidents. This method ensures consistency in how events are tagged, as it leverages a structured approach rather than random or ad-hoc tagging. It allows organizations to maintain clarity and coherence in their event data, enabling efficient filtering and reporting processes. The event model serves as a reference framework that enhances the accuracy and relevance of the tags applied to the events, thus aiding in effective monitoring and responses through improved visibility. In the context of why the other options are less valid: one option suggests tagging all events universally, which would lead to excessive noise and make it difficult to focus on meaningful data. Another option refers to creating tags based on user settings, which implies a manual process that could introduce inconsistencies and inefficiencies. The last option discusses the removal of tags from events, which is not the primary function of Standard Auto-Tagging, as it focuses on tagging rather than tag removal.

6. Which Intrusion Prevention rule specifically targets Cross-Site Scripting (XSS) vulnerabilities?

A. 1000608

B. 1000552

C. 1000100

D. 1000200

The rule that specifically targets Cross-Site Scripting (XSS) vulnerabilities is designed to detect and mitigate attempts by attackers to inject malicious scripts into web pages viewed by other users. Cross-Site Scripting is a prevalent security vulnerability that can allow attackers to bypass access controls and access cookies, session tokens, or other sensitive information from the user's browser. Rule 1000552 is specifically associated with identifying patterns and behaviors that are indicative of XSS attacks, thereby helping to protect web applications against these types of attacks effectively. By implementing this rule, Deep Security can analyze incoming HTTP requests and filter out those that exhibit suspicious behavior consistent with XSS attempts. This proactive approach is essential for safeguarding both the application's integrity and the user's data. Other rules might address different vulnerabilities or broader categories of threats, but 1000552's specificity towards XSS makes it the appropriate choice for targeting this particular security concern.

SAMPLE

7. What should a tenant user do if they do not receive the activation email after account creation?

A. Contact support for manual activation

B. Wait for 24 hours for automatic activation

C. Resend the account creation request

D. Log in directly with default credentials

When a tenant user does not receive the activation email after creating an account, the most appropriate course of action is to contact support for manual activation. This step is crucial because it ensures that any issues related to the email delivery or account setup can be addressed by the support team. They can investigate potential problems, such as incorrect email addresses or technical issues within the system. Relying on other options may not be effective. For instance, waiting for a specified time could result in prolonged inaccessibility to the platform if there is an underlying problem that needs immediate attention. Resending the account creation request might not resolve the issue if the original request was successfully registered but simply not activated due to email issues. Additionally, attempting to log in with default credentials when the account has not been activated would not work, as the account is not yet functional. By choosing to contact support, the user actively seeks a solution and enhances the chances of timely resolution, allowing them to start using the services without unnecessary delays.

8. When creating an NSX Security Policy, what service must be enabled for Deep Security?

A. Network Counseling Service

B. Guest Introspection Service

C. Network Introspection Service

D. Service Profile Management

When creating a Network Security Policy within VMware NSX for use with Trend Micro Deep Security, the correct service that must be enabled is the Network Introspection Service. This service is crucial because it allows the integration of Deep Security with NSX, facilitating the inspection of network traffic for security threats. The Network Introspection Service works by leveraging VMware's distributed firewall capabilities to provide advanced threat protection directly at the network level. By enabling this service, security policies can be enforced directly on virtual machines, providing a layer of security that is tightly integrated with the VMware environment. This capability is essential for maintaining a strong security posture in a software-defined data center by allowing the Deep Security agent to monitor traffic flows and apply security measures accordingly. In contrast, other services mentioned may serve different roles within the NSX ecosystem but do not specifically cater to the integration of Deep Security for network-level inspections and protections. For example, the Guest Introspection Service focuses on processes as they run within VM guests for anti-malware operations rather than broader network traffic monitoring. Overall, the effective deployment of Deep Security in an NSX environment hinges on the enabling of the Network Introspection Service.

SAMPLE

9. Which of the following is NOT true about Deep Security Virtual Appliance activation?

A. It works the same way as Deep Security Agent activation

B. It initiates Virtual Agent instantiation

C. It can be activated on unprepared ESXi machines

D. It allows for self-protection of the virtual appliance

The statement that it can be activated on unprepared ESXi machines is not true regarding Deep Security Virtual Appliance activation. For effective operation, a Deep Security Virtual Appliance must be deployed in a prepared environment, specifically within an ESXi host that meets the necessary prerequisites. This includes ensuring that the host has been configured appropriately and is compatible with the Deep Security infrastructure required for management and protection features. The other statements reflect accurate aspects of Deep Security Virtual Appliance activation. For instance, the activation process for the Virtual Appliance parallels that of the Deep Security Agent, allowing for a familiar approach for users who have experience with the Agent. Additionally, the activation does indeed initiate the instantiation of a Virtual Agent, which plays a critical role in extending security functionalities to virtual machines. Furthermore, self-protection is a feature available, ensuring that the appliance itself is secured against various threats.

10. What is the purpose of the Add Directory Wizard in Deep Security Manager?

A. To add users to the system

B. To populate the Computers list using Active Directory information

C. To configure firewall rules automatically

D. To perform vulnerability assessments

The purpose of the Add Directory Wizard in Deep Security Manager is specifically to populate the Computers list using Active Directory information. This feature enables seamless integration with Active Directory, allowing administrators to import computers and their associated attributes directly into the Deep Security Manager. By doing so, it simplifies the management of security policies, enabling organizations to ensure that all relevant systems are monitored and secured effectively. This functionality is crucial for organizations that rely on Active Directory for user and resource management, as it provides a streamlined method to track and secure devices across the network. Effective population of the Computers list helps in maintaining an accurate and organized view of the infrastructure requiring protection, facilitating easier management of security tasks. The other options, while related to security management in some aspects, do not align with the primary role of the Add Directory Wizard. For instance, adding users relates to user management in the system, configuring firewall rules pertains to network security settings, and performing vulnerability assessments involves checking for security weaknesses, none of which are directly concerned with importing and managing computer resources through Active Directory.

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://trendmicrodeepsecurity.examzify.com

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

SAMPLE