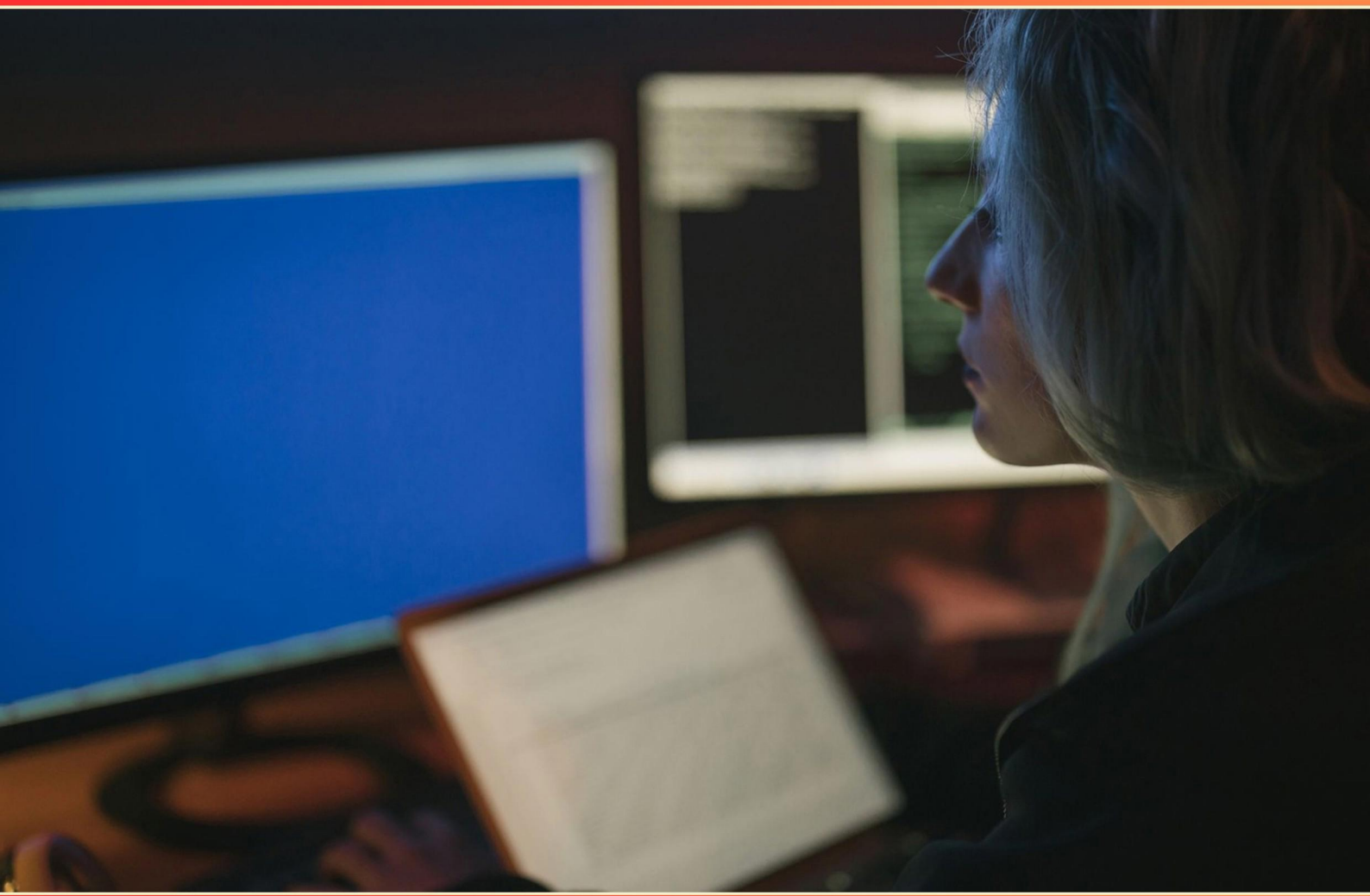
MICROSOFT SECURITY OPERATIONS ANALYST (SC-200) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://mcsecurityoperationsanalyst.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 9

Explanations 11

Next Steps 17

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. **What actions can an administrator take when analyzing the Risky Users report?**

   A. Reset user passwords and dismiss user risk detections

   B. Exclude users from risk policies and close individual detections

   C. Confirm compromised sign-ins and block user sign-ins

   D. Approve pending actions and review completed actions

2. **Which Microsoft service focuses on enabling organizations to respond to security incidents rapidly?**

   A. Microsoft Sentinel

   B. Microsoft Defender for Cloud

   C. Microsoft Defender for Identity

   D. Microsoft 365 Defender

3. **What is an essential focus area when integrating Microsoft Defender for Identity with other security tools?**

   A. Prioritize automation of response actions to security alerts.

   B. Develop specialized, tool-specific strategies for handling security alerts.

   C. Focus on streamlining alert management to quickly address threats.

   D. Concentrate on enhancing detection capabilities through shared intelligence.

4. **What is the purpose of Microsoft 365 compliance solutions?**

   A. To enhance performance of Office applications

   B. To protect sensitive information and reduce risks of data breaches

   C. To simplify user experience across platforms

   D. To ensure faster email delivery

5. **Within Microsoft 365 Defender, which tab should you navigate to identify all entities impacted by an incident?**

   A. Investigations

   B. Alerts

   C. Devices

   D. Evidence and Response

SAMPLE

6. How are automation rules in Microsoft Sentinel different from analytics rules?

A. Automation rules are used to create custom log queries, while analytics rules are used to configure data connectors for external threat intelligence feeds.

B. Automation rules trigger predefined actions based on specific conditions, while analytics rules identify security threats using machine learning algorithms.

C. Automation rules and analytics rules serve the same purpose and are interchangeable terms in Microsoft Sentinel.

D. Automation rules focus on analyzing security data to detect threats, while analytics rules automate response actions.

7. Which roles are required for managing alerts and incidents within Defender for Cloud Apps?

A. Manage alerts, Security admin

B. Security reader, Security admin, View-only recipients

C. Global admin, Security admin, Compliance admin, Security operator, Security reader

D. Security admin, View-only audit logs, Security reader

8. What setting should be configured in Safe Attachments policy to forward flagged attachments to the security team?

A. Apply the malware scanning timeout setting for automatic forwarding

B. Enable redirect of attachments to a security administrator's email address

C. Use Dynamic delivery to analyze attachments before delivery

D. Set the action for unknown malware in attachments to "Monitor"

9. Which tool would you recommend for identifying unused resources in an Azure subscription?

A. Azure Security Center

B. Azure Policy

C. Azure Advisor

D. Azure Cost Management

SAMPLE

10. What is a crucial part of maintaining an effective security posture within an organization?

A. Regular training for employees on security best practices.

B. Allowing bring-your-own-device policies without limitations.

C. Implementing only technical solutions without user engagement.

D. Reducing monitoring of user activities to encourage trust.

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What actions can an administrator take when analyzing the Risky Users report?

A. Reset user passwords and dismiss user risk detections

B. Exclude users from risk policies and close individual detections

C. Confirm compromised sign-ins and block user sign-ins

D. Approve pending actions and review completed actions

The actions an administrator can take when analyzing the Risky Users report typically include resetting user passwords and dismissing user risk detections. When a user is identified as risky, a common administrative response is to reset their password to prevent any potential unauthorized access resulting from compromised credentials. This action can help protect the user's account and secure sensitive information. Additionally, administrators may dismiss user risk detections after reviewing the situation to clear false positives or when the risks have been addressed. This allows for a more manageable risk assessment environment and improves the accuracy of future reports. The other choices involve actions that, while potentially relevant, do not directly correspond to the typical responses for managing risky users as described. Excluding users from risk policies or closing detections may not address the immediate security risks effectively. Confirming compromised sign-ins can be part of the process, but it often requires further investigation before outright blocking sign-ins, which is a more drastic measure. Lastly, approving and reviewing actions may pertain to various administrative tasks but does not specifically address the immediate risk management needed for risky users.

2. Which Microsoft service focuses on enabling organizations to respond to security incidents rapidly?

A. Microsoft Sentinel

B. Microsoft Defender for Cloud

C. Microsoft Defender for Identity

D. Microsoft 365 Defender

Microsoft Sentinel is designed specifically to enhance an organization's ability to respond to security incidents promptly and effectively. It serves as a Security Information and Event Management (SIEM) solution that incorporates artificial intelligence to analyze vast amounts of data and identify potential threats in real time. By providing advanced threat detection, investigation capabilities, and automated response actions, organizations can significantly reduce the time it takes to address security incidents. This platform aggregates security data from various sources, such as on-premises environments and cloud resources, enabling security teams to visualize and understand the security posture across the entire organization. Additionally, with built-in automation and playbooks, Sentinel allows for rapid incident response by orchestrating workflows and initiating predefined actions based on alerts. In contrast, while other options like Microsoft Defender for Cloud, Microsoft Defender for Identity, and Microsoft 365 Defender provide important security features within their respective domains, they do not specialize as much in the comprehensive incident response capabilities that Microsoft Sentinel offers. Defender for Cloud focuses primarily on securing cloud environments, Defender for Identity centers on identity and access concerns, and Microsoft 365 Defender integrates security across various Microsoft 365 applications but does not directly provide the same level of dedicated incident response and investigation tools as Sentinel.

SAMPLE

3. What is an essential focus area when integrating Microsoft Defender for Identity with other security tools?

A. Prioritize automation of response actions to security alerts.

B. Develop specialized, tool-specific strategies for handling security alerts.

C. Focus on streamlining alert management to quickly address threats.

D. Concentrate on enhancing detection capabilities through shared intelligence.

Focusing on enhancing detection capabilities through shared intelligence is crucial when integrating Microsoft Defender for Identity with other security tools. Shared intelligence allows different security solutions to communicate and leverage the knowledge gained from various data sources. This collaborative approach improves the overall security posture by providing a more comprehensive view of threats and vulnerabilities. When Microsoft Defender for Identity shares intelligence with other security tools, it can utilize insights gained from network behavior, identity anomalies, and other inputs to detect potential compromises more effectively. This integration not only enhances real-time threat detection but also boosts the effectiveness of existing security measures by providing context and correlation across different systems. Consequently, it leads to a better response strategy and reduces the time to identify and mitigate threats. In contrast, while automation of response actions, tool-specific strategies, and streamlined alert management are all important considerations, they are secondary to the fundamental need for robust detection capabilities that are enhanced through the sharing of intelligence across platforms. This foundational aspect is what allows organizations to stay proactive and improve their security responses.

4. What is the purpose of Microsoft 365 compliance solutions?

A. To enhance performance of Office applications

B. To protect sensitive information and reduce risks of data breaches

C. To simplify user experience across platforms

D. To ensure faster email delivery

The purpose of Microsoft 365 compliance solutions is centered around protecting sensitive information and reducing the risks of data breaches. These solutions are designed to help organizations manage their compliance with legal and regulatory requirements, safeguard sensitive data, and maintain the confidentiality, integrity, and availability of that data. Efforts within Microsoft 365 compliance include tools that provide governance capabilities, data loss prevention, information protection, and auditing features to ensure that organizations can effectively monitor and protect their data. By employing these solutions, businesses can implement policies that actively mitigate risks associated with data leaks and ensure compliance with standards such as GDPR, HIPAA, and others, thereby maintaining the trust of customers and users. This focus on security and compliance is essential in a landscape where data breaches can lead to severe financial penalties and reputational damage, making this area a crucial priority for many organizations.

SAMPLE

5. Within Microsoft 365 Defender, which tab should you navigate to identify all entities impacted by an incident?

A. Investigations

B. Alerts

C. Devices

D. Evidence and Response

To identify all entities impacted by an incident within Microsoft 365 Defender, navigating to the Evidence and Response tab is the most effective choice. This tab provides a comprehensive view of all entities that are directly related to the incident, including users, devices, and applications that may have been affected. It consolidates relevant evidence and artifacts associated with the incident, making it easier for security analysts to assess the scope and severity of the impact. The Evidence and Response section enables analysts to delve into the details of what occurred, understand the relationships between affected entities, and take appropriate remediation steps. This information is crucial for incident response, as it helps analysts determine the breadth of the incident and any necessary follow-up actions. While the other tabs, like Investigations or Alerts, provide valuable information regarding security events or activities, they do not focus specifically on outlining all entities impacted by a particular incident. Thus, the Evidence and Response tab offers the most relevant information needed for understanding the full impact of an incident.

6. How are automation rules in Microsoft Sentinel different from analytics rules?

A. Automation rules are used to create custom log queries, while analytics rules are used to configure data connectors for external threat intelligence feeds.

B. Automation rules trigger predefined actions based on specific conditions, while analytics rules identify security threats using machine learning algorithms.

C. Automation rules and analytics rules serve the same purpose and are interchangeable terms in Microsoft Sentinel.

D. Automation rules focus on analyzing security data to detect threats, while analytics rules automate response actions.

The distinction between automation rules and analytics rules in Microsoft Sentinel is fundamentally about their functions and purposes within the security operations framework. Automation rules are designed to trigger specific actions automatically based on defined conditions or events. This means that when an event occurs, such as an alert being generated or a specific anomaly being detected, automation rules can initiate a response—like sending notifications, creating tickets, or executing playbooks. This is essential for streamlining incident response processes and ensuring timely action without the need for manual intervention. On the other hand, analytics rules are focused on identifying potential security threats within the data collected. They employ various techniques, including machine learning and heuristic analysis, to analyze event logs and behavior patterns to detect anomalies that may signify a security incident. Essentially, analytics rules serve to enhance the detection capabilities of Microsoft Sentinel by continuously assessing the incoming data for potential threats. In summary, the correct answer highlights how automation rules are actionable responses triggered by specific conditions, while analytics rules are responsible for the initial detection of security threats. This differentiation allows organizations to efficiently manage both the identification of risks and the operational responses needed to mitigate those risks.

SAMPLE

7. Which roles are required for managing alerts and incidents within Defender for Cloud Apps?

A. Manage alerts, Security admin

B. Security reader, Security admin, View-only recipients

C. Global admin, Security admin, Compliance admin, Security operator, Security reader

D. Security admin, View-only audit logs, Security reader

The correct choice involves the roles that are essential for managing alerts and incidents within Microsoft Defender for Cloud Apps. These roles are specifically designed with permissions that enable users to effectively oversee security alerts and incidents, ensuring that the right individuals have the necessary authority to monitor and respond to security issues. In this case, the inclusion of global admin, security admin, compliance admin, security operator, and security reader roles provides a comprehensive framework for incident management. The global admin role is crucial as it holds overarching control over all aspects of the Microsoft 365 environment, allowing full access to manage settings and configurations. The security admin role is specifically designed to navigate security-related tasks, including responding to alerts and managing security incidents. Similarly, the compliance admin role ensures that any compliance-related issues are incorporated into the incident management process, while the security operator can act on security alerts and utilize tools designed for incident response. Finally, the security reader role is vital for users who need to review security reports and alerts without making changes themselves, thereby supporting the team with situational awareness. Together, these roles provide a well-rounded approach to managing security operations effectively within Defender for Cloud Apps. They ensure that multiple facets of security management—administration, compliance, and operational monitoring—are covered, allowing

8. What setting should be configured in Safe Attachments policy to forward flagged attachments to the security team?

A. Apply the malware scanning timeout setting for automatic forwarding

B. Enable redirect of attachments to a security administrator's email address

C. Use Dynamic delivery to analyze attachments before delivery

D. Set the action for unknown malware in attachments to "Monitor"

In a Safe Attachments policy within Microsoft Defender for Office 365, configuring the option to enable redirect of attachments to a security administrator's email address allows for a proactive approach to identifying and responding to potential threats. This setting directs flagged attachments, which may contain malware or other harmful content, to a designated security team member who can review and analyze the attachments in a controlled environment. By allowing these attachments to be forwarded to the security team, organizations can ensure that any suspicious or malicious content is reviewed promptly, minimizing the risk of dangerous files being accessed by end-users. This proactive measure helps to bolster the organization's overall security posture by enabling rapid investigation and remediation of potential risks. While malware scanning timeout, dynamic delivery, and monitoring of unknown malware are all important considerations in a comprehensive security strategy, they do not provide the direct mechanism for sending potentially harmful content to a security team for review and action. Therefore, enabling the redirect to a security administrator's email is an essential setting that enhances collaboration between the automated systems and human analysts in responding to threats.

SAMPLE

9. Which tool would you recommend for identifying unused resources in an Azure subscription?

A. Azure Security Center

B. Azure Policy

C. Azure Advisor

D. Azure Cost Management

The recommendation of Azure Advisor for identifying unused resources in an Azure subscription is grounded in its primary function of providing personalized best practices and recommendations to enhance your Azure environment. Azure Advisor analyzes your usage patterns, configuration, and other operational data to identify areas where you can optimize your resources. This includes highlighting underutilized or over-provisioned resources, enabling organizations to make informed decisions about resource management and cost reduction. By providing actionable insights regarding idle resources, Azure Advisor assists users in optimizing their cloud spend, ensuring that they are only utilizing resources that provide value. This tailored advice not only helps in managing costs but also contributes to improving overall resource efficiency within the Azure subscription. Other tools mentioned serve different primary purposes. For instance, Azure Security Center primarily focuses on security assessments and recommendations rather than resource efficiency. Azure Policy is used to enforce compliance and implement governance rules, and while it can help track resources, it does not specifically target identifying unused resources. Azure Cost Management is focused on budget tracking and cost analysis but does not actively highlight unused resources. Therefore, Azure Advisor is the most effective choice for this particular need.

10. What is a crucial part of maintaining an effective security posture within an organization?

A. Regular training for employees on security best practices.

B. Allowing bring-your-own-device policies without limitations.

C. Implementing only technical solutions without user engagement.

D. Reducing monitoring of user activities to encourage trust.

Regular training for employees on security best practices is fundamental to maintaining an effective security posture within an organization. This is because employees are often the first line of defense against security threats, such as phishing attacks or social engineering attempts. By educating staff on the latest threats, security policies, and best practices, organizations can foster a culture of security awareness. When employees understand the potential risks and how to mitigate them, they are more likely to identify suspicious activities and respond appropriately. Training should be ongoing to adapt to new threats and to refresh knowledge, ensuring that security considerations are top of mind for all employees. In contrast, allowing bring-your-own-device policies without limitations can introduce significant security risks, as personal devices may not have the same protections as company-issued equipment. Relying solely on technical solutions without user engagement overlooks the human element of security, which is critical for managing potential vulnerabilities. Moreover, reducing monitoring of user activities creates a false sense of trust and can leave organizations blind to potentially harmful behavior or security incidents. Therefore, consistent training and engagement with employees are crucial to an organization's overall security effectiveness.

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://mcsecurityoperationsanalyst.examzify.com

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

SAMPLE