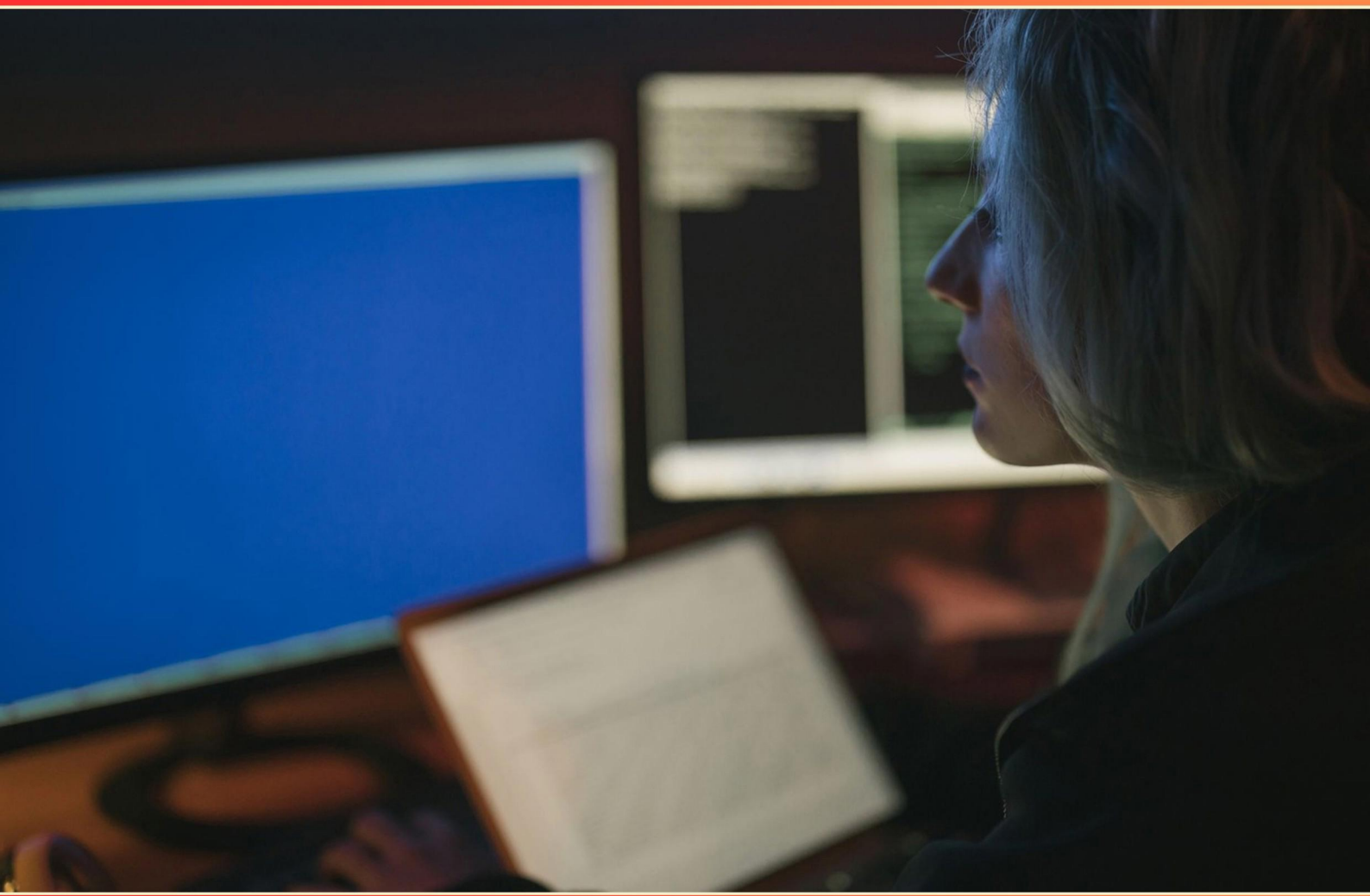
MICROSOFT SECURITY OPERATIONS ANALYST (SC-200) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://mcsecurityoperationsanalyst.examzify.com

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. 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!

Questions

1. **If a security administrator does not receive email alerts for certain activities in Microsoft Defender, what should they configure?**

   A. The integration settings for Threat detection.

   B. The Azure Defender plans.

   C. The severity level of email notifications.

   D. A cloud connector.

2. **What action should be taken if Microsoft Defender for Identity flags a security issue with user accounts authenticating with clear-text passwords?**

   A. Enforce password complexity requirements and require password changes.

   B. Review and update network perimeter defenses.

   C. Conduct an educational session on safe internet practices.

   D. Immediately encrypt all network traffic.

3. **What is the primary objective of deploying Microsoft Defender for Identity sensors on domain controllers?**

   A. To manage user accounts more effectively.

   B. To detect suspicious activities within the network.

   C. To streamline software deployment processes.

   D. To enhance data recovery techniques.

4. **What does "No threats found > Phishing or Junk" mean in the User reported messages tab of Microsoft Defender?**

   A. The message was confirmed to be malicious.

   B. The message was initially suspected to be malicious but was later determined to be harmless.

   C. The message was flagged as suspicious and requires further investigation.

   D. The message was reported as safe by the user.

5. **Which feature of the Threat Explorer allows you to identify the specific users targeted by malware attacks?**

   A. Threat families overview.

   B. Top threats dashboard.

   C. Sender email filter.

   D. Users tab.

6. What is the primary purpose of restoring user access to corporate resources after a security incident has been remediated?

A. To test the effectiveness of the remediation measures.

B. To prevent further disruption to business processes.

C. To allow users to resume their normal work activities.

D. To provide additional time for security analysts to monitor the device.

7. What label should be applied to project timelines and organizational charts containing sensitive information, signifying that they can be shared with external partners?

A. Label these documents as "Public," to freely share them within and outside the organization.

B. Label these documents as "Highly Confidential," to restrict their access strictly to top management.

C. Label these documents as "General," indicating they are not for public consumption but can be shared with external partners.

D. Label these documents as "Personal," to restrict their usage to nonbusiness purposes.

8. 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

9. Which role should be assigned to Tier 1 SOC analysts to allow modification of predefined playbooks in Microsoft Sentinel?

A. Azure Sentinel Automation Operator.

B. Azure Sentinel Contributor.

C. Azure Sentinel Responder.

D. Azure Sentinel Reader.

10. In an incident response scenario, which of the following actions is crucial for determining the incident's effect on data?

A. Assess the notifications generated during the incident

B. Determine the categories of alerts triggered

C. Investigate the scope of the impacted areas

D. Examine the overall response time during the incident

Answers

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

Explanations

1. If a security administrator does not receive email alerts for certain activities in Microsoft Defender, what should they configure?

A. The integration settings for Threat detection.

B. The Azure Defender plans.

C. The severity level of email notifications.

D. A cloud connector.

The correct choice focuses on configuring the severity level of email notifications, which directly impacts the alerts that a security administrator receives. In Microsoft Defender, email notifications are often set to trigger based on the severity of the threats detected. If certain activities are overlooked or not generating alerts,it's likely that their severity level is set too low or not configured to notify the administrator. By adjusting the severity level, the security administrator can ensure that they receive alerts for a broader range of activities, particularly those considered critical or high priority. This adjustment allows for timely responses to potential threats, improving the overall security posture of the organization. Alternatives such as integration settings for threat detection and Azure Defender plans pertain more to the broader configuration of security measures rather than directly influencing the alert system. Cloud connectors could relate to linking external data sources or services, which doesn't address the issue of missing email notifications specifically. Thus, adjusting the severity level is the most relevant and effective approach for ensuring that the administrator receives timely alerts regarding critical activities within Microsoft Defender.

2. What action should be taken if Microsoft Defender for Identity flags a security issue with user accounts authenticating with clear-text passwords?

A. Enforce password complexity requirements and require password changes.

B. Review and update network perimeter defenses.

C. Conduct an educational session on safe internet practices.

D. Immediately encrypt all network traffic.

Choosing to enforce password complexity requirements and require password changes is the most appropriate action when Microsoft Defender for Identity flags a security issue with user accounts authenticating with clear-text passwords. This step directly addresses the vulnerability associated with clear-text password usage. By enforcing password complexity requirements, organizations can ensure that passwords are not only more difficult to guess or brute-force but also promote the use of stronger passwords that can help mitigate risk. Additionally, requiring users to change their passwords immediately prevents any potential exploitation that could arise from the clear-text passwords that have been flagged. Since the primary issue here is the clear-text transmission of passwords, taking action to enhance password security is a proactive measure in improving overall security posture. The other options, while beneficial in various contexts, do not directly address the immediate risk posed by clear-text password authentication. Reviewing network perimeter defenses can help in securing the broader network but does not mitigate the specific issue of weak password usage. Conducting educational sessions on safe internet practices can raise awareness but does not provide an immediate solution to the flagged issue. Similarly, encrypting all network traffic is a valuable security measure but may not be viable or necessary to implement immediately and does not resolve the specific concern related to authentication practices.

3. What is the primary objective of deploying Microsoft Defender for Identity sensors on domain controllers?

A. To manage user accounts more effectively.

B. To detect suspicious activities within the network.

C. To streamline software deployment processes.

D. To enhance data recovery techniques.

The primary objective of deploying Microsoft Defender for Identity sensors on domain controllers is to detect suspicious activities within the network. These sensors are critical for monitoring user behaviors and activities, particularly those that indicate potential security threats or malicious actions. By analyzing authentication traffic and other signals, Defender for Identity can identify anomalies that might suggest a compromise, such as unusual logon attempts, unauthorized access, and lateral movement by attackers. This capability is essential for maintaining the security posture of an organization, as domain controllers are central to managing authentication and access within an Active Directory environment. By leveraging these sensors, organizations can gain real-time insights into their security landscape and respond proactively to threats, helping ensure that they can mitigate risks before they escalate into more significant security incidents. This proactive detection plays a vital role in maintaining the integrity and confidentiality of sensitive data within a network.

4. What does "No threats found > Phishing or Junk" mean in the User reported messages tab of Microsoft Defender?

A. The message was confirmed to be malicious.

B. The message was initially suspected to be malicious but was later determined to be harmless.

C. The message was flagged as suspicious and requires further investigation.

D. The message was reported as safe by the user.

The phrase "No threats found > Phishing or Junk" indicates that while a message may have initially raised suspicion, further analysis revealed that it is not harmful. This means that the message was likely scrutinized for possible phishing attempts or junk classification, but it was ultimately assessed and considered safe for the user. As a result, the system or administrator acknowledges that the message does not represent a security threat, aligning with the context of the answer chosen. The other options reference different statuses that do not match this indication—such as confirmation of malicious content or the requirement for further investigation, which would signify that a threat was detected rather than ruled out. The key takeaway here is the assurance that the message is deemed harmless after scrutiny, hence supporting the rationale for the selected answer.

5. Which feature of the Threat Explorer allows you to identify the specific users targeted by malware attacks?

A. Threat families overview.

B. Top threats dashboard.

C. Sender email filter.

D. Users tab.

The Users tab is a specific feature in the Threat Explorer that provides insights into individual users who have been targeted by malware attacks. This feature allows security analysts to review detailed information about user activities related to detected threats, enabling them to pinpoint which users have been affected, the types of attacks aimed at them, and the corresponding responses or necessary actions. In contrast, the other options offer different perspectives or functionalities within Threat Explorer. The Threat families overview typically categorizes threats based on their characteristics and behaviors but does not provide user-specific information. The Top threats dashboard presents a high-level view of the most significant threats but lacks the granularity needed to identify individual users connected to the threats. The Sender email filter focuses on analyzing specific senders of emails but does not directly show user targeting by malware. Thus, the Users tab is uniquely positioned to deliver detailed, targeted insights specifically regarding users, making it the most suitable choice for identifying those affected by malware.

6. What is the primary purpose of restoring user access to corporate resources after a security incident has been remediated?

A. To test the effectiveness of the remediation measures.

B. To prevent further disruption to business processes.

C. To allow users to resume their normal work activities.

D. To provide additional time for security analysts to monitor the device.

Restoring user access to corporate resources after a security incident has been remediated primarily serves to prevent further disruption to business processes. When a security incident occurs, operations can be hindered, affecting productivity and potentially leading to financial losses. By quickly restoring access, organizations can ensure that employees can continue their work without prolonged interruptions, thereby maintaining the efficiency of the business. This approach also keeps workflows intact and supports the overall operational resilience of the organization, as it helps to minimize the impact of the incident on routine activities. Ensuring that users can access the resources they need plays a critical role in the overall recovery strategy following a security incident.

7. What label should be applied to project timelines and organizational charts containing sensitive information, signifying that they can be shared with external partners?

A. Label these documents as "Public," to freely share them within and outside the organization.

B. Label these documents as "Highly Confidential," to restrict their access strictly to top management.

C. Label these documents as "General," indicating they are not for public consumption but can be shared with external partners.

D. Label these documents as "Personal," to restrict their usage to nonbusiness purposes.

Labeling project timelines and organizational charts containing sensitive information as "General" signifies that, while the contents are not classified for public dissemination, they can still be shared with external partners depending on the context and the established sharing protocols. This label strikes a balance, allowing for the sharing of relevant information while ensuring that it is not completely open to unrestricted access. Choosing this label communicates to all stakeholders that the documents contain sensitive data that is intended for specific audiences. It also helps ensure that the information is handled appropriately according to internal policies and external partner agreements. The "General" label maintains a level of confidentiality while being flexible enough to permit sharing with trusted external entities, aligning with best practices in information sharing and collaboration.

8. 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

9. Which role should be assigned to Tier 1 SOC analysts to allow modification of predefined playbooks in Microsoft Sentinel?

A. Azure Sentinel Automation Operator.

B. Azure Sentinel Contributor.

C. Azure Sentinel Responder.

D. Azure Sentinel Reader.

The appropriate role for Tier 1 SOC analysts to modify predefined playbooks in Microsoft Sentinel is the Azure Sentinel Contributor role. This role provides sufficient permissions to create and manage playbooks, which are essential for automating responses to threats and incidents. The Azure Sentinel Contributor role is designed to allow users to have a more active and creative role in handling security incidents. This includes the ability to modify existing playbooks or create new ones, tailoring the automation processes to fit the specific operational needs of the organization. With this role, Tier 1 analysts can ensure that playbooks are effective and aligned with the current security landscape. In contrast, the other roles have more limited permissions. For instance, the Azure Sentinel Reader role is primarily for viewing information without any ability to modify resources. The Azure Sentinel Responder role allows users to respond to incidents but does not grant permissions for creating or modifying playbooks. The Azure Sentinel Automation Operator role focuses on executing playbooks rather than editing them. Therefore, assigning the Azure Sentinel Contributor role is essential for enabling Tier 1 SOC analysts to effectively manage and refine the incident response processes in Microsoft Sentinel.

10. In an incident response scenario, which of the following actions is crucial for determining the incident's effect on data?

A. Assess the notifications generated during the incident

B. Determine the categories of alerts triggered

C. Investigate the scope of the impacted areas

D. Examine the overall response time during the incident

Understanding the scope of the impacted areas during an incident response is essential for assessing the incident's effect on data. This step involves identifying which systems, applications, or data repositories were affected by the incident, as it allows security analysts to comprehend the full extent of the incident's impact. By investigating the scope, analysts can determine if sensitive data was accessed, altered, or exfiltrated. This information is critical for prioritizing remedial actions, communicating with stakeholders, and fulfilling legal or regulatory obligations regarding data breaches. Moreover, understanding the scope sets the groundwork for implementing responses and recovery strategies, ensuring that all affected areas are accounted for. While assessing notifications, determining alert categories, and examining response times are important components of the overall incident response process, they do not directly address the immediate concern of determining the impact on data. Notifications and alerts provide insight into the nature and likelihood of threats, and response times can indicate the efficiency of the response efforts, but they do not directly clarify how data integrity and confidentiality have been affected in the incident.

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!