CROWDSTRIKE CERTIFIED FALCON ADMINISTRATOR (CCFA) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://crowdstrikefalconadmin.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. To minimize false positives for required applications, what can be created?

A. Network security groups

B. ML Exclusions

C. Firewall rules

D. Incident reports

2. What is the character limit for a Falcon grouping tag?

A. 100 characters

B. 237 characters

C. 255 characters

D. 500 characters

3. How can Mac sensor tags be managed?

A. Via Falcon console

B. Through Command Line with a sensor restart

C. Only by API calls

D. Directly through the BIOS settings

4. What is the main scenario where reduced functionality mode (RFM) is most commonly encountered?

A. During Windows updates

B. During installation of new software

C. When connecting to the internet

D. During system startup

5. What information is needed to add IOCs to the management system?

A. Only the hash

B. Description and Severity

C. Description, Severity, and Action

D. Hash, Description, and Host Group

6. What is the purpose of ML exclusions?

A. To stop all network traffic

B. To stop static file-based detections through ML techniques

C. To disable host sensors

D. To enhance detections on trusted hosts

SAMPLE

7. How long are quarantined files retained in the CrowdStrike cloud?

A. 30 days

B. 60 days

C. 90 days

D. 120 days

8. Which role in Prevent Roles allows viewing and managing remediation actions?

A. Detections Exceptions Manager

B. Quarantine Manager

C. Falcon Analyst

D. Remediation Manager

9. Which feature allows for the dynamic assignment of hosts to groups based on custom keywords?

A. Sensor Grouping Tags

B. Falcon Grouping Tags

C. Best Practice Groups

D. Policy Settings

10. What is the main function of a containment policy in CrowdStrike?

A. Auto Quarantine mechanism

B. Network traffic allow list

C. Data Encryption

D. Access Control

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. To minimize false positives for required applications, what can be created?

A. Network security groups

B. ML Exclusions

C. Firewall rules

D. Incident reports

Creating ML Exclusions is an effective way to minimize false positives for required applications. Machine Learning (ML) algorithms used in threat detection can sometimes misidentify benign applications or behaviors as malicious, leading to false positives. By establishing ML Exclusions, you inform the system to disregard certain applications or behavioral patterns during its analysis, thereby allowing legitimate applications to run without being flagged as potential threats. This helps maintain operational integrity and reduces unnecessary alerts while ensuring that the security posture remains strong. While other options, such as network security groups, firewall rules, and incident reports, serve important roles in a security framework, they are not specifically aimed at minimizing false positives in the way that ML Exclusions are. Network security groups can manage access and control traffic flows, firewall rules are set to block or allow certain types of traffic, and incident reports are used for documenting security events but do not directly influence the algorithmic classification of applications. Therefore, the establishment of ML Exclusions specifically targets the challenge of minimizing false detections related to trusted applications.

2. What is the character limit for a Falcon grouping tag?

A. 100 characters

B. 237 characters

C. 255 characters

D. 500 characters

The correct character limit for a Falcon grouping tag is 255 characters. This limit allows users to create meaningful and descriptive tags without overwhelming the system or sacrificing functionality. Grouping tags help organize and categorize endpoints within the Falcon platform, enabling more efficient management and analysis of security data. Understanding this character limit is important for effectively using the tagging system within the CrowdStrike Falcon platform, as it ensures that tags are both practical and fit within system constraints. This character count supports a significant amount of descriptive text while maintaining performance and usability standards. Knowing this limit also aids administrators in planning and structuring their tags thoughtfully, ensuring that they remain concise and relevant for people viewing or utilizing this information later. The other options exceed this limit or fall outside of typical constraints set by Falcon for tagging purposes, thereby not being applicable to the Falcon grouping tag system.

SAMPLE

3. How can Mac sensor tags be managed?

A. Via Falcon console

B. Through Command Line with a sensor restart

C. Only by API calls

D. Directly through the BIOS settings

Managing Mac sensor tags involves a variety of methods, with the most effective way being through the Falcon console. The Falcon console provides an intuitive graphical interface for administering all aspects of sensor management, including tagging, configuration, and monitoring. While command line usage from a local terminal session can facilitate certain tasks, such as restarting the sensor, it is not the primary method for managing these tags. Moreover, API calls, although useful for automation and integration with other systems, are not the main interface used for direct management. Lastly, BIOS settings are not applicable for managing Mac sensor tags since the BIOS is specific to Windows-based systems and does not pertain to Mac functionalities or Falcon sensor operations. Thus, the correct approach emphasizes operational efficiency via Falcon console for managing Mac sensor tags, enabling administrators to effectively organize and control security measures.

4. What is the main scenario where reduced functionality mode (RFM) is most commonly encountered?

A. During Windows updates

B. During installation of new software

C. When connecting to the internet

D. During system startup

Reduced functionality mode (RFM) is most commonly encountered during Windows updates because it is a state in which the operating system limits the available features and functionality to protect the integrity of the system during critical updates. This mode is implemented to prevent any active processes from interfering with the installation of updates, ensuring that the operating system can maintain stability and security while applying necessary patches or upgrades. During this mode, the system may restrict access to certain applications and functionalities temporarily, allowing the update process to complete successfully. Once the updates are finalized, the system will revert to its normal operating mode, fully restoring all functionalities and features. This scenario is particularly important for maintaining the overall health and security of Windows systems, which is why understanding RFM in relation to updates is crucial for IT professionals and administrators. Other scenarios, such as installing new software, connecting to the internet, or during system startup, typically do not involve the same level of restriction or management of system features as RFM does during updates.

5. What information is needed to add IOCs to the management system?

A. Only the hash

B. Description and Severity

C. Description, Severity, and Action

D. Hash, Description, and Host Group

To successfully add Indicators of Compromise (IOCs) to the management system, it is essential to provide a comprehensive set of information that includes the hash, a description, and the host group. The hash serves as a unique identifier for the IOC, allowing the system to specifically identify and track malicious files or signatures accurately. The description provides necessary context about the IOC, offering insights into what the threat is, how it behaves, and potential implications for the organization. Additionally, specifying the host group is crucial because this delineates which endpoints the IOC should be applicable to, enabling the system to target responses and remediation efforts effectively. This combination of information ensures that the management system can adequately assess, prioritize, and respond to the threats represented by the IOCs, ultimately enhancing the security posture of the organization.

SAMPLE

6. What is the purpose of ML exclusions?

A. To stop all network traffic

B. To stop static file-based detections through ML techniques

C. To disable host sensors

D. To enhance detections on trusted hosts

The purpose of ML exclusions is specifically to stop static file-based detections through machine learning techniques. In contexts like cybersecurity and endpoint protection, machine learning is utilized to analyze and detect potential threats by observing patterns and behaviors associated with files. However, there are instances where certain files or applications, deemed safe or trusted, may trigger false positives in these ML algorithms. By implementing ML exclusions, administrators can instruct the system to ignore these specific files during the detection process, thereby preventing them from being flagged as threats. This ensures that legitimate applications or files are not incorrectly labeled as harmful, thus minimizing disruptions and maintaining operational efficiency on the network. The other options do not accurately reflect the purpose of ML exclusions. Stopping all network traffic pertains to a much broader action that would not be effective in targeted detection efforts. Disabling host sensors or enhancing detections on trusted hosts do not align with the specific function of mitigating unnecessary detections through the exclusion of certain classifications by machine learning processes.

7. How long are quarantined files retained in the CrowdStrike cloud?

A. 30 days

B. 60 days

C. 90 days

D. 120 days

Quarantined files in the CrowdStrike cloud are retained for 90 days. This retention period is essential for maintaining a balance between managing potential threats and ensuring that legitimate files can be reviewed and restored if needed. During this period, security administrators have the opportunity to analyze the quarantined files, make decisions about their disposition, and take necessary actions to protect the organization's environment. The 90-day retention period provides enough time for thorough investigations while still allowing for efficient storage management in the cloud environment.

SAMPLE

8. Which role in Prevent Roles allows viewing and managing remediation actions?

A. Detections Exceptions Manager

B. Quarantine Manager

C. Falcon Analyst

D. Remediation Manager

The role that allows viewing and managing remediation actions is the Remediation Manager. This role is designed specifically to oversee the remediation process, which includes the assessment of threats and the implementation of necessary actions to mitigate those threats. The Remediation Manager is equipped with the necessary permissions to view current incidents, track the status of remediations, and execute the actions required to resolve issues identified by the system. This role is critical in maintaining the security posture of an organization as it ensures that threats are not only detected but also effectively managed. Individuals in this role collaborate with other stakeholders, often using insights from detection and monitoring tools to inform their remediation strategies. Having a dedicated role for remediation actions helps prevent overlaps and confusion in responsibilities, thereby streamlining the response to security incidents. In contrast, other roles, while important, do not focus primarily on remediation actions. For instance, the Detections Exceptions Manager may work on setting exceptions for certain detections but does not manage the actual remediation processes. The Quarantine Manager handles the quarantine of detected threats but is not responsible for the entire remediation scope. The Falcon Analyst examines and analyzes incidents but may not directly engage with remediation actions in the same comprehensive manner as the Remediation Manager.

9. Which feature allows for the dynamic assignment of hosts to groups based on custom keywords?

A. Sensor Grouping Tags

B. Falcon Grouping Tags

C. Best Practice Groups

D. Policy Settings

The correct answer is Falcon Grouping Tags, which enable the dynamic assignment of hosts to groups based on custom keywords. This feature is particularly useful for organizations that need to organize their hosts efficiently according to certain attributes or criteria defined by the admin. By assigning keywords as tags, hosts are automatically grouped, allowing for streamlined management and the ability to apply tailored security policies more effectively. Falcon Grouping Tags improve operational efficiency by dynamically adapting the grouping based on the keywords assigned, which can change as the environment evolves. This ensures that the correct policies and responses are applied to the appropriate groups of hosts without manual intervention, thereby enhancing overall security posture and reducing the risk of misconfiguration. Other options do not offer the same level of dynamic assignment based on custom keywords. Sensor Grouping Tags provide a way to organize sensors, but they are less flexible in terms of adapting to changes in host characteristics without manual updates. Best Practice Groups are more focused on predefined classifications and do not incorporate user-defined keywords. Policy Settings refer to the configurations that determine the security measures in place but do not facilitate dynamic grouping based on custom attributes.

SAMPLE

10. What is the main function of a containment policy in CrowdStrike?

A. Auto Quarantine mechanism

B. Network traffic allow list

C. Data Encryption

D. Access Control

The main function of a containment policy in CrowdStrike is to manage and control the communications and interactions of devices on your network, specifically by establishing a network traffic allow list. This allows administrators to define which applications or processes can communicate across the network, essentially limiting potential threats by preventing unauthorized or harmful network traffic from taking place. Containment policies are crucial for ensuring that only trusted and verified processes can establish connections, which helps in reducing the attack surface that malicious actors can exploit. By focusing on controlling network traffic, organizations can effectively contain the threat within their environment and prevent further propagation or compromise of sensitive data. In this context, auto quarantine mechanisms, data encryption, and access control, while important aspects of cybersecurity strategies, do not specifically represent the primary focus of containment policies within CrowdStrike. Instead, containment policies are distinctly designed to regulate network interactions and enhance organizational security posture by managing how data flows between devices in the network.

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://crowdstrikefalconadmin.examzify.com

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

SAMPLE