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

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. **Which setting would you choose to ensure a suspicious file is prevented from executing but not shown in detections?**

   A. Block

   B. Detect Only

   C. Block, Hide Detection

   D. Allow

2. **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

3. **What happens to quarantined files once they are released?**

   A. They are deleted from the system immediately

   B. They are permanently removed from all records

   C. They are automatically allowlisted for that host

   D. They require additional approval to restore

4. **What must be verified when checking **SSL/TLS settings** for proper CrowdStrike functionality?**

   A. TLS v1.2 / SSL v3

   B. Only enable TLS v1.0

   C. Disable all SSL and TLS protocols

   D. Use self-signed certificates

5. **Which role has the ability to create and manage machine learning exclusions?**

   A. Firewall Manager

   B. Detections Exceptions Manager

   C. Endpoint Manager

   D. Quarantine Manager

6. During the installation process, what must be accepted to proceed with Falcon installation?

A. The user agreement

B. The EULA

C. The installation checklist

D. The policy consent

7. Which of the following is NOT a feature of sensor update policies?

A. Push out updates automatically

B. Allow manual adjustments for specific hosts

C. Monitor network performance

D. Assign host groups for targeted updates

8. What mode does the Falcon sensor operate in if installed on an unsupported kernel version?

A. Complete mode

B. Reduced Functionality Mode (RFM)

C. Maintenance mode

D. Compatibility mode

9. What is a potential consequence of unauthorized API secret exposure?

A. Enhanced data analytics

B. Loss of API functionality

C. Secret disappears

D. Increased access permissions

10. What purpose does adding known benign files to an allowlist serve?

A. It increases the security of the system.

B. It reduces false positive detections.

C. It ensures all indicators are detected.

D. It blocks all incoming files.

Answers

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

Explanations

1. Which setting would you choose to ensure a suspicious file is prevented from executing but not shown in detections?

A. Block

B. Detect Only

C. Block, Hide Detection

D. Allow

Choosing the setting that allows a suspicious file to be prevented from executing while also not being shown in detections involves a specific approach to threat management. The correct choice, which is to block the execution of the file while hiding the detection, offers several key benefits. Firstly, blocking the execution prevents potentially harmful files from running and causing damage to the system or network. This proactive measure is essential for maintaining security and protecting sensitive data. Secondly, hiding the detection can be advantageous in scenarios where you want to reduce noise in detection reports. This can be particularly useful in environments where a high volume of alerts might lead to alert fatigue among security personnel. By not showing these detections, it allows teams to focus on more critical alerts that require immediate attention, streamlining the incident response process. In this way, the setting effectively balances the need for robust security with the operational efficiency of the security operations team, making it an optimal choice for managing potential threats without overwhelming the detection and response process.

2. 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.

3. What happens to quarantined files once they are released?

A. They are deleted from the system immediately

B. They are permanently removed from all records

C. They are automatically allowlisted for that host

D. They require additional approval to restore

Once quarantined files are released, they are automatically allowlisted for that host. This means that the files are treated differently by the CrowdStrike Falcon platform upon restoration. Allowlisting enables the system to recognize these files as safe going forward, which can prevent them from being flagged or quarantined again for the same reason. This is particularly useful in scenarios where legitimate software may have initially been misclassified as a threat, allowing for smoother operations and reducing unnecessary interruptions. The process of allowlisting indicates a trust relationship has been established for the released files, avoiding further complications that might arise from repeated false alarms. It is essential in managing potential false positives and ensuring that the workflow remains efficient. The other options do not accurately represent the handling of quarantined files once they are released, as they suggest removal or additional hurdles that do not apply in the context of the CrowdStrike Falcon platform's intended management of released files.

4. What must be verified when checking **SSL/TLS settings** for proper CrowdStrike functionality?

A. TLS v1.2 / SSL v3

B. Only enable TLS v1.0

C. Disable all SSL and TLS protocols

D. Use self-signed certificates

Verifying the SSL/TLS settings for proper CrowdStrike functionality involves ensuring that TLS v1.2 is enabled, as it is a secure and widely accepted protocol for encrypted connections. Using outdated protocols like SSL v3 or older versions of TLS can expose systems to vulnerabilities and attacks, as these protocols are no longer considered secure. TLS v1.2 offers improved security features, such as stronger encryption algorithms and protection against specific types of attacks, making it essential for maintaining the integrity and confidentiality of data in transit. Ensuring that only TLS v1.2 is in use helps maintain compliance with security best practices and standards, which is crucial for the effective deployment of CrowdStrike services.

5. Which role has the ability to create and manage machine learning exclusions?

A. Firewall Manager

B. Detections Exceptions Manager

C. Endpoint Manager

D. Quarantine Manager

The role that has the ability to create and manage machine learning exclusions is specifically designated as the Detections Exceptions Manager. This role is integral to managing how the CrowdStrike Falcon platform interprets and uses data related to potential threats, particularly those identified by machine learning models. The Detections Exceptions Manager can create exclusions that allow specific files or behaviors to be recognized as safe, even if they might otherwise trigger alerts due to the way machine learning algorithms assess risks. This significantly enhances the ability to fine-tune the system's ability to differentiate between legitimate and illegitimate behaviors and ensures reduced false positives in threat detection. Other roles, such as the Firewall Manager or the Endpoint Manager, have different scopes and responsibilities, primarily centered on network security settings or overall endpoint administration, which do not include the nuanced management of machine learning exclusions. The Quarantine Manager focuses on handling and managing quarantined items but does not have the capability to create or modify exclusions for threat detection. Thus, the Detections Exceptions Manager is uniquely positioned to handle machine learning exclusions effectively.

6. During the installation process, what must be accepted to proceed with Falcon installation?

A. The user agreement

B. The EULA

C. The installation checklist

D. The policy consent

To proceed with the Falcon installation, it is essential to accept the End User License Agreement (EULA). The EULA is a legal document that delineates the terms and conditions under which the software can be used. By accepting the EULA, the user acknowledges their understanding of these terms and agrees to comply with them, which is a standard practice for software installations. The acceptance of the EULA is crucial because it protects both the software provider and the user, ensuring that the usage rights, liabilities, and obligations are clearly defined. This agreement often covers aspects like restriction of usage, liabilities, and any warranties provided by the company. While the user agreement, installation checklist, and policy consent may be part of different software deployment processes, they do not specifically grant the legal usage rights that the EULA does. Thus, accepting the EULA is a necessary step that must be completed before installation can continue.

7. Which of the following is NOT a feature of sensor update policies?

A. Push out updates automatically

B. Allow manual adjustments for specific hosts

C. Monitor network performance

D. Assign host groups for targeted updates

The correct response is that monitoring network performance is not a feature of sensor update policies. Sensor update policies primarily focus on the distribution and management of updates to the CrowdStrike Falcon sensors installed on various endpoints. Their core functionalities include automatically pushing updates to enhance security and functionality, allowing tailored manual adjustments for specific hosts when necessary, and assigning host groups for targeted updates to optimize the management process. Monitoring network performance, while important within the broader scope of cybersecurity and IT management, is not a direct function of sensor update policies. Sensor update policies are specifically designed to manage how and when updates are applied to sensors rather than assessing or analyzing network performance metrics. This delineation of roles highlights the specific targeting of sensor update policies, emphasizing their focus on update management rather than ongoing network health or performance monitoring.

8. What mode does the Falcon sensor operate in if installed on an unsupported kernel version?

A. Complete mode

B. Reduced Functionality Mode (RFM)

C. Maintenance mode

D. Compatibility mode

The Falcon sensor, when installed on a kernel version that is not supported, operates in Reduced Functionality Mode (RFM). This mode is specifically designed to maintain some level of security monitoring and threat detection capabilities while acknowledging the limitations imposed by the unsupported kernel. In RFM, the sensor has reduced capabilities compared to its full operation in supported environments, meaning that certain advanced features may be disabled or function at a diminished level. This approach allows organizations to retain some protection and visibility while they work toward upgrading to a supported version, thus reducing the risk of exposure during the transition period. In contrast, other modes mentioned, such as Maintenance mode or Compatibility mode, do not pertain specifically to the situation of an unsupported kernel. Maintenance mode is typically associated with temporary activity reductions for updates or maintenance, while Compatibility mode would imply functioning within the parameters of a known compatible environment, which does not apply in this scenario.

9. What is a potential consequence of unauthorized API secret exposure?

A. Enhanced data analytics

B. Loss of API functionality

C. Secret disappears

D. Increased access permissions

When considering the consequence of unauthorized exposure of API secrets, it's essential to understand the role that these secrets play in securing API access. API secrets are credentials that authenticate and authorize access to APIs, ensuring that only authorized users or systems can interact with them. If an API secret is compromised or exposed, it does not simply "disappear." Instead, the consequences can be severe, leading to unauthorized access to sensitive data or functionality. Attackers can use the exposed secret to impersonate legitimate users, potentially leading to data breaches, service disruptions, or misuse of resources. Therefore, the idea that the secret would simply vanish overlooks the significant risks associated with its exposure. A more accurate understanding of the potential consequences includes that without prompt mitigation—or rotating secrets—services might be manipulated or affected, but the secret itself remains present and usable by those who gained unauthorized access. This highlights the critical necessity of protecting API secrets and responding quickly to any potential leakage to prevent security incidents.

10. What purpose does adding known benign files to an allowlist serve?

A. It increases the security of the system.

B. It reduces false positive detections.

C. It ensures all indicators are detected.

D. It blocks all incoming files.

Adding known benign files to an allowlist primarily serves to reduce false positive detections. When files are allowlisted, the security solution recognizes them as safe based on their established reputation and characteristics. This means that when these files are encountered during scans or assessments, the system will not flag them as potential threats. This is crucial for maintaining operational efficiency and reducing unnecessary alerts that can lead to alert fatigue. By minimizing the number of false positives, security teams can focus on genuine threats rather than spending time investigating legitimate files that have been mistakenly flagged. This streamlined process enhances overall productivity and allows for a more effective security posture without the noise created by false alarms. The other options do not align with the primary purpose of an allowlist. For example, while adding files to an allowlist can contribute to overall security by ensuring trust in legitimate applications, this is not its primary purpose. Similarly, while it does not ensure detection of all indicators or block incoming files, these functionalities relate to different aspects of security and not specifically to the function of reducing false positives.

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!