

Quiz CrowdStrike - CCFA-200b - CrowdStrike Falcon Administrator Accurate Sure Pass

CrowdStrike CCFA-200b Exam

CrowdStrike Certified Falcon Administrator

<https://www.passquestion.com/ccfa-200b.html>



Pass CrowdStrike CCFA-200b Exam with PassQuestion CCFA-200b questions and answers in the first attempt.

<https://www.passquestion.com/>

1/6

BONUS!!! Download part of Prep4pass CCFA-200b dumps for free: https://drive.google.com/open?id=1K6hgsJzgMjghnIwn8030CHpQjlrOq_ZC

After choosing CCFA-200b training engine, you will surely feel very pleasantly surprised. First of all, our CCFA-200b study materials are very rich, so you are free to choose. At the same time, you can switch to suit your learning style at any time. Because our CCFA-200b learning quiz is prepared to meet your diverse needs. If you are not confident in your choice, you can seek the help of online services.

If you are the first time to prepare the CCFA-200b exam, it is better to choose a type of good study materials. After all, you cannot understand the test syllabus of the CCFA-200b exam in the whole round. It is important to predicate the tendency of the CCFA-200b study materials if you want to easily pass the exam. And our CCFA-200b Exam Questions are the one which can exactly cover the latest information of the exam in the first time for our professionals are good at this subject and you can totally rely on us.

>> CCFA-200b Sure Pass <<

CCFA-200b Actual Exam & CCFA-200b Exam Guide & CCFA-200b Practice Exam

We also fully consider the characteristics of the user on studying the CCFA-200b exam questions. For example, many people who

choose to obtain a CCFA-200b certificate don't have a lot of time to prepare for the exam. Based on this point, our team of experts really took a lot of thought in the layout of the content. The contents of CCFA-200b Exam Materials are carefully selected by experts. We hope you can get the most effective knowledge in the shortest possible time.

CrowdStrike Falcon Administrator Sample Questions (Q92-Q97):

NEW QUESTION # 92

You can create Fusion SOAR workflows to precisely define the actions you want Falcon to perform in response to incidents. Which three items must be defined in every trigger so that it executes successfully?

- A. Rule Type, Filter, Objective
- B. Rule Type, Condition, Action
- C. Trigger, Filter, Objective
- **D. Trigger, Condition, Action**

Answer: D

NEW QUESTION # 93

You have been provided with a list of 100 hashes that are not malicious but your company has deemed to be inappropriate for work computers. They have asked you to ensure that they are not allowed to run in your environment. You have chosen to use Falcon to do this. Which is the best way to accomplish this?

- A. Using Custom Alerts in the Investigate App, create a new alert using the template "Process Execution" and within that rule, select the option to "Block Execution"
- B. Using the Support Portal, create a support ticket and include the list of binary hashes, asking support to create an "Execution Prevention" rule to prevent these processes from running
- C. Using the API, gather the list of SHA256 or MD5 hashes for each binary and then upload them, setting them all to "Never Allow"
- **D. Using IOC Management, gather the list of SHA256 or MD5 hashes for each binary and then upload them. Set all hashes to "Block" and ensure that the prevention policy these computers are using includes the option for "Custom Blocking" under Execution Blocking.**

Answer: D

Explanation:

The best way to ensure that a list of 100 hashes that are not malicious but your company has deemed to be inappropriate for work computers are not allowed to run in your environment is to use IOC Management, gather the list of SHA256 or MD5 hashes for each binary and then upload them. Set all hashes to "Block" and ensure that the prevention policy these computers are using includes the option for "Custom Blocking" under Execution Blocking. This will allow Falcon to block the execution of these hashes on the hosts using this policy. The other options are either incorrect or not efficient to achieve this goal.

NEW QUESTION # 94

How do you disable all detections for a host?

- A. Contact support and provide them with the Agent ID (AID) for the machine and they will put it on the Disabled Hosts list in your Customer ID (CID)
- **B. In Host Management, select the host and then choose the option to Disable Detections**
- C. You cannot disable all detections on individual hosts as it would put them at risk
- D. Create an exclusion rule and apply it to the machine or group of machines

Answer: B

Explanation:

The administrator can disable all detections for a host by selecting the host and then choosing the option to Disable Detections in the Host Management page. This will prevent the host from sending any detection events to the Falcon Cloud. The other options are either incorrect or not available.

NEW QUESTION # 95

Where can you modify settings to permit certain traffic during a containment period?

- **A. Containment Policy**
- B. Host Settings
- C. Firewall Settings
- D. Prevention Policy

Answer: A

Explanation:

The administrator can modify settings to permit certain traffic during a containment period by creating or editing a Containment Policy. This policy allows users to specify which ports, protocols and IP addresses are allowed or blocked during network containment. The other options are either incorrect or not related to network containment.

NEW QUESTION # 96

Your organization wants to monitor the use of remote access software that is currently authorized. The executable is called remote.exe.

How would you trigger a detection for review of any process named remote.exe?

- A. Assign an aggressive detection level machine-learning prevention policy to the applicable hosts
- **B. Write an IOA rule to monitor process creation of.*\\remote.exe**
- C. Create an exclusion for remote.exe and set a workflow to email you every time the exclusion is used
- D. Write a scheduled search looking for ProcessRollup2 events for remote.exe

Answer: B

NEW QUESTION # 97

.....

You will be able to assess your shortcomings and improve gradually without having anything to lose in the actual CrowdStrike Falcon Administrator exam. You will sit through mock exams and solve actual CrowdStrike CCFA-200b dumps. In the end, you will get results that will improve each time you progress and grasp the concepts of your syllabus. The desktop-based CrowdStrike CCFA-200b Practice Exam software is only compatible with Windows.

CCFA-200b Real Brain Dumps: https://www.prep4pass.com/CCFA-200b_exam-braindumps.html

CrowdStrike CCFA-200b Sure Pass Guaranteed to help you Pass Your Exam, If you are prepared to take the CCFA-200b exam with the help of excellent CCFA-200b learning materials on our website, the choice is made brilliant, There are many online resources for preparing the CCFA-200b test , Hope your journey to success is full of joy by using our CCFA-200b test questions: CrowdStrike Falcon Administrator and having a phenomenal experience, The CCFA-200b study materials are valuable, but knowledge is priceless.

What is the exact shape, Proximal third section CCFA-200b of the small intestines, Guaranteed to help you Pass Your Exam, If you are prepared to take the CCFA-200b exam with the help of excellent CCFA-200b learning materials on our website, the choice is made brilliant.

Free PDF Quiz CCFA-200b - CrowdStrike Falcon Administrator Marvelous Sure Pass

There are many online resources for preparing the CCFA-200b test , Hope your journey to success is full of joy by using our CCFA-200b test questions: CrowdStrike Falcon Administrator and having a phenomenal experience.

The CCFA-200b study materials are valuable, but knowledge is priceless.

- Useful 100% Free CCFA-200b – 100% Free Sure Pass | CCFA-200b Real Brain Dumps ☐ Easily obtain ➡ CCFA-200b ☐ for free download through ➡ www.examcollectionpass.com ☐ ☐ ☐ CCFA-200b Exam Success
- CCFA-200b Reliable Test Practice ☐ CCFA-200b Real Dump ☐ CCFA-200b Valid Exam Cost ☐ Search for ☐ CCFA-200b ☐ on > www.pdfvce.com < immediately to obtain a free download ☐ Relevant CCFA-200b Questions

- [illegible]

P.S. Free 2026 CrowdStrike CCFA-200b dumps are available on Google Drive shared by Prep4pass:
https://drive.google.com/open?id=1K6hgsJzgMjghnIwn8030CHpQjlrOq_ZC