# Valid CCFH-202b Exam Forum, CCFH-202b Passleader Review

Pass CrowdStrike CCFH-202 Exam with Real Questions

CrowdStrike CCFH-202 Exam

CrowdStrike Certified Falcon Hunter

https://www.passquestion.com/CCFH-202.html

Save 35% OFF All Exams

Coupon: 2023

35% OFF on All, Including CCFH-202 Questions and Answers

Pass CCFH-202 Exam with PassQuestion CCFH-202 questions and answers in the first attempt.

https://www.passquestion.com/

1 / 5

Obtaining an IT certification shows you are an ambitious individual who is always looking to improve your skill set. Most companies think highly of this character. Our CCFH-202b exam original questions will help you clear exam certainly in a short time. You don't need to worry about how difficulty the exams are. ActualVCE release the best high-quality CCFH-202b Exam original questions to help you most candidates pass exams and achieve their goal surely.

It is our mission to help you pass the exam. CCFH-202b guide torrent will provide you with 100% assurance of passing the professional qualification exam. We are very confident in the quality of CCFH-202b study guide. And we believe that all students who have purchased our study materials will be able to successfully pass the professional qualification exam as long as they follow the content provided by CCFH-202b study guide, study it on a daily basis, and conduct regular self-examination through mock exams. Once you unfortunately fail the exam, CCFH-202b Guide Torrent will provide you with a full refund and the refund process is very simple. As long as you provide your staff with your transcripts, you will receive a refund soon. Of course, before you buy, CCFH-202b certification training offers you a free trial service, as long as you log on our website, you can download our trial questions bank for free. I believe that after you try CCFH-202b certification training, you will love them.

**>> Valid CCFH-202b Exam Forum <<**

## 100% Pass Quiz 2026 CCFH-202b: CrowdStrike Certified Falcon Hunter Accurate Valid Exam Forum

We promise to provide a high-quality simulation system with advanced CCFH-202b study materials. With the simulation function, our CCFH-202b training guide is easier to understand and have more vivid explanations to help you learn more knowledge. You can set time to test your study efficiency, so that you can accomplish your test within the given time when you are in the Real CCFH-202b Exam. You will be confident if you have more experience on the CCFH-202b exam questions!

## CrowdStrike Certified Falcon Hunter Sample Questions (Q18-Q23):

**NEW QUESTION # 18**
You need details about key data fields and sensor events which you may expect to find from Hosts running the Falcon sensor. Which documentation should you access?

- A. Hunting and Investigation
- B. Event stream APIs
- C. Events Data Dictionary
- D. Streaming API Event Dictionary

**Answer: C**

Explanation:
The Events Data Dictionary found in the Falcon documentation is useful for writing hunting queries because it provides a reference of information about the events found in the Investigate > Event Search page of the Falcon Console. The Events Data Dictionary describes each event type, field name, data type, description, and example value that can be used to query and analyze event data. The Streaming API Event Dictionary, Hunting and Investigation, and Event stream APIs are not documentation that provide details about key data fields and sensor events.

**NEW QUESTION # 19**
In the Powershell Hunt report, what does the "score" signify?

- A. Maliciousness score determined by NGAV
- B. A cumulative score of the various potential command line switches
- C. Number of hosts that ran the PowerShell script
- D. How recently the PowerShell script executed

**Answer: B**

Explanation:
In the Powershell Hunt report, the score signifies a cumulative score of the various potential command line switches that were used in the PowerShell script execution. The score is based on a weighted system that assigns different values to different switches based on their potential maliciousness or usefulness for threat hunting. For example, -EncodedCommand has a higher value than -NoProfile. The score does not signify the number of hosts that ran the PowerShell script, how recently the PowerShell script executed, or the maliciousness score determined by NGAV.

**NEW QUESTION # 20**
SPL (Splunk) eval statements can be used to convert Unix times (Epoch) into UTC readable time Which eval function is correct