

Professional CCFH-202b Valid Exam Cost & Leading Offer in Qualification Exams & Free Download CCFH-202b: CrowdStrike Certified Falcon Hunter

Pass CrowdStrike CCFH-202 Exam with Real Questions

CrowdStrike CCFH-202 Exam

CrowdStrike Certified Falcon Hunter

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



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/>

175

If you feel that you always suffer from procrastination and cannot make full use of your spare time, maybe our CCFH-202b study materials can help you solve your problem. We are willing to recommend you to try the CCFH-202b study materials from our company. Our CCFH-202b training guide are high quality and efficiency test tools for all people. If you buy our CCFH-202b Preparation questions, we can promise that you can use our CCFH-202b study materials for study in anytime and anywhere. Because we have three version of CCFH-202b exam questions that can satisfy all needs of our customers.

Our experts are well-aware of the problems of exam candidates particularly of those who can't manage to spare time to study the CCFH-202b exam questions due to their heavy work pressure. Hence, our CCFH-202b study materials have been developed into a simple content and language for our worthy customers all over the world. What is more, you will find there are only the keypoints in our CCFH-202b learning guide.

>> CCFH-202b Valid Exam Cost <<

100% Pass Quiz CCFH-202b - CrowdStrike Certified Falcon Hunter Updated Valid Exam Cost

Many candidates felt worried about their exam for complex content and too extensive subjects to choose and understand. Our CCFH-202b exam materials successfully solve this problem for them. with the simplified language and key to point subjects, you are easy to understand and grasp all the information that in our CCFH-202b training guide. For Our professionals compiled them with the purpose that help all of the customer to pass their CCFH-202b exam.

CrowdStrike Certified Falcon Hunter Sample Questions (Q34-Q39):

NEW QUESTION # 34

Which field should you reference in order to find the system time of a *FileWritten event?

- A. ProcessStartTime_decimal
- B. timestamp
- C. ContextTimeStamp_decimal
- D. FileTimeStamp_decimal

Answer: C

Explanation:

ContextTimeStamp_decimal is the field that shows the system time of the event that triggered the sensor to send data to the cloud. In this case, it would be the time when the file was written. FileTimeStamp_decimal is the field that shows the last modified time of the file, which may not be the same as the time when the file was written. ProcessStartTime_decimal is the field that shows the start time of the process that performed the file write operation, which may not be the same as the time when the file was written. Timestamp is the field that shows the time when the sensor data was received by the cloud, which may not be the same as the time when the file was written.

NEW QUESTION # 35

The Events Data Dictionary found in the Falcon documentation is useful for writing hunting queries because:

- A. It provides pre-defined queries you can customize to meet your specific threat hunting needs
- B. It provides a list of all the detect names and descriptions found in the Falcon Cloud
- C. It provides a reference of information about the events found in the Investigate > Event Search page of the Falcon Console
- D. It provides a list of compatible splunk commands used to query event data

Answer: C

Explanation:

This is the correct answer for the same reason as above. The Events Data Dictionary provides a reference of information about the events found in the Investigate > Event Search page of the Falcon Console, which is useful for writing hunting queries. It does not provide pre-defined queries, detect names and descriptions, or compatible splunk commands.

NEW QUESTION # 36

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

Answer: A

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 # 37

Event Search data is recorded with which time zone?

- A. PST
- B. EST

- C. UTC
- D. GMT

Answer: C

Explanation:

Event Search data is recorded with UTC (Coordinated Universal Time) time zone. UTC is a standard time zone that is used as a reference point for other time zones. PST (Pacific Standard Time), GMT (Greenwich Mean Time), and EST (Eastern Standard Time) are not the time zones that Event Search data is recorded with.

NEW QUESTION # 38

Which of the following best describes the purpose of the Mac Sensor report?

- A. The Mac Sensor report provides a comprehensive view of activities occurring on Mac hosts, including items of interest that may be hunting or investigation leads
- B. The Mac Sensor report displays a listing of all Mac hosts without a Falcon sensor installed
- C. The Mac Sensor report displays a listing of all Mac hosts with a Falcon sensor installed
- D. The Mac Sensor report provides a detection focused view of known malicious activities occurring on Mac hosts, including machine-learning and indicator-based detections

Answer: A

Explanation:

This is the correct answer for the same reason as above. The Mac Sensor report provides a comprehensive view of activities occurring on Mac hosts, including items of interest that may be hunting or investigation leads. It does not display a listing of all Mac hosts with or without a Falcon sensor installed, nor does it provide a detection focused view of known malicious activities occurring on Mac hosts.

NEW QUESTION # 39

.....

What is your dream? Don't you want to make a career? The answer must be ok. Then, you need to upgrade and develop yourself. You worked in the IT industry, through what methods can you realize your dream? Taking IT certification exam and getting the certificate are the way to upgrade yourself. At present, CrowdStrike CCFH-202b Exam is very popular. Do you want to get CrowdStrike CCFH-202b certificate? If it is ok, don't hesitate to sign up for the exam. And don't worry about how to pass the test, DumpsValid certification training will be with you.

New CCFH-202b Exam Question: <https://www.dumpsvalid.com/CCFH-202b-still-valid-exam.html>

Different with some other exam questions, the CCFH-202b original questions are changing on the positive way---it will be renewed at once when there is any change of CrowdStrike exam, which maintains the utter pass rate, CrowdStrike CCFH-202b Valid Exam Cost I can guarantee that our study materials will be your best choice, CCFH-202b real questions are crucial for passing the CCFH-202b exam.

Learn Adobe Premiere Pro CC for Video Communication: Adobe Certified CCFH-202b Associate Exam Preparation, You can change these settings by choosing Final Cut Express > Easy Setup and choosing a different option.

100% Pass CrowdStrike - CCFH-202b - CrowdStrike Certified Falcon Hunter –Valid Valid Exam Cost

Different with some other exam questions, the CCFH-202b Original Questions are changing on the positive way---it will be renewed at once when there is any change of CrowdStrike exam, which maintains the utter pass rate.

I can guarantee that our study materials will be your best choice, CCFH-202b real questions are crucial for passing the CCFH-202b exam, We ensure success on the first attempt if you use our CrowdStrike CCFH-202b exam dumps according to our instructions.

It will create many career opportunities and benefits for you by CCFH-202b pass exam files.

