CCFH-202b Hot Spot Questions | CCFH-202b Valid Dumps Sheet

BONUS!!! Download part of ITexamReview CCFH-202b dumps for free: https://drive.google.com/open?id=18MO96flUtsNpdpeC8aB1UZ-UL1wGBiEq

You will get a lot of personal and professional benefits after passing the CrowdStrike CCFH-202b test. The CrowdStrike CCFH-202b exam is a valuable credential that will assist you to advance your career. The CrowdStrike CCFH-202b is a way to increase your knowledge and skills. You can also trust on ITexamReview and start CrowdStrike Certified Falcon Hunter CCFH-202b test preparation with CrowdStrike CCFH-202b practice test material.

CrowdStrike CCFH-202b Exam Syllabus Topics:

Topic	Details
Topic 1	• Event Search: This domain focuses on using CrowdStrike Query Language to build queries, format and filter event data, understand process relationships and event types, and create custom dashboards.
Topic 2	• Search and Investigation Tools: This domain covers analyzing file and process metadata, using Investigate Module tools, performing various searches, and interpreting dashboard results.
Topic 3	• Reports and References: This domain covers using built-in Hunt and Visibility reports and leveraging Events Full Reference documentation for event information.
Topic 4	• ATT&CK Frameworks: This domain covers understanding the cyber kill chain and using the MITRE ATT&CK Framework to model threat actor behaviors and communicate findings to non-technical audiences.
Topic 5	• Hunting Analytics: This domain focuses on recognizing malicious behaviors, evaluating information reliability, decoding command line activity, identifying infection patterns, distinguishing legitimate from adversary activity, and identifying exploited vulnerabilities.

Topic 6	• Hunting Methodology: This domain covers conducting active hunts, performing outlier analysis, testing hunting hypotheses, constructing queries, and investigating process trees.

>> CCFH-202b Hot Spot Questions <<

CCFH-202b Valid Dumps Sheet, Online CCFH-202b Version

In order to meet a wide range of tastes, our company has developed the three versions of the CCFH-202b preparation questions, which includes PDF version, online test engine and windows software. According to your own budget and choice, you can choose the most suitable one for you. And if you don't know which one to buy, you can free download the demos of the CCFH-202b Study Materials to check it out. The demos of the CCFH-202b exam questions are a small part of the real exam questions.

CrowdStrike Certified Falcon Hunter Sample Questions (Q46-Q51):

NEW QUESTION # 46
What is the main purpose of the Mac Sensor report?

- A. To identify endpoints that are in Reduced Functionality Mode
- B. To provide a dashboard for Mac related detections
- C. To provide a summary view of selected activities on Mac hosts
- D. To provide vulnerability assessment for Mac Operating Systems

Answer: C

Explanation:
The Mac Sensor report is a pre-defined report that provides a summary view of selected activities on Mac hosts. It shows information such as process execution events, network connection events, file write events, etc. that occurred on Mac hosts within a specified time range. The Mac Sensor report does not identify endpoints that are in Reduced Functionality Mode, provide vulnerability assessment for Mac Operating Systems, or provide a dashboard for Mac related detections.

NEW QUESTION # 47
Which field should you reference in order to find the system time of a *FileWritten event?

- A. timestamp
- B. ProcessStartTime_decimal
- 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 # 48
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. Streaming API Event Dictionary
- B. Event stream APIs
- C. Events Data Dictionary

- D. Hunting and Investigation

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 # 49
Adversaries commonly execute discovery commands such as netexe, ipconfig.exe, and whoami exe. Rather than query for each of these commands individually, you would like to use a single query with all of them. What Splunk operator is needed to complete the following query?

- A. OR
- B. AND
- C. NOT
- D. IN

Answer: A

Explanation:
The OR operator is needed to complete the following query, as it allows to search for events that match any of the specified values. The query would look like this:
event_simpleName=ProcessRollup2 FileName=net.exe OR FileName=ipconfig.exe OR FileName=whoami.exe The OR operator is used to combine multiple search terms or expressions and return events that match at least one of them. The IN, NOT, and AND operators are not suitable for this query, as they have different functions and meanings.

NEW QUESTION # 50
When performing a raw event search via the Events search page, what are Event Actions?

- A. Event Actions are pivotable workflows including connecting to a host, pre-made event searches and pivots to other investigatory pages such as host search
- B. Event Actions is the field name that contains the event name defined in the Events Data Dictionary such as ProcessRollup, SyntheticProcessRollup, DNS request, etc
- C. Event Actions contains an audit information log of actions an analyst took in regards to a specific detection
- D. Event Actions contains the summary of actions taken by the Falcon sensor such as quarantining a file, prevent a process from executing or taking no actions and creating a detection only

Answer: A

Explanation:
When performing a raw event search via the Events search page, Event Actions are pivotable workflows that allow you to perform various tasks related to the event or the host. For example, you can connect to a host using Real Time Response, run pre-made event searches based on the event type or name, or pivot to other investigatory pages such as host search, hash search, etc. Event Actions do not contain audit information log, summary of actions taken by the Falcon sensor, or the event name defined in the Events Data Dictionary.

NEW QUESTION # 51
.....

The experts in our company have been focusing on the CCFH-202b examination for a long time and they never overlook any new knowledge. The content of our study materials has always been kept up to date. Don't worry if any new information comes out after your purchase of our CCFH-202b study guide. We will inform you by E-mail when we have a new version. With our great efforts, our study materials have been narrowed down and targeted to the CCFH-202b examination. So you don't need to worry about wasting your time on useless CCFH-202b exam materials information.

CCFH-202b Valid Dumps Sheet: https://www.itexamreview.com/CCFH-202b-exam-dumps.html

- Useful CCFH-202b Dumps □ Accurate CCFH-202b Answers □ Knowledge CCFH-202b Points □ Copy URL □ www.practicevce.com □ open and search for ➤ CCFH-202b □ to download for free □New CCFH-202b Dumps Ebook
- Reliable CCFH-202b Test Dumps □ Useful CCFH-202b Dumps □ Latest CCFH-202b Exam Answers □ Go to website 《 www.pdfvce.com 》 open and search for " CCFH-202b " to download for free □New CCFH-202b Dumps Ebook
- Free PDF Quiz CrowdStrike - CCFH-202b –Trustable Hot Spot Questions □ Search on □ www.examcollectionpass.com □ for [CCFH-202b] to obtain exam materials for free download □CCFH-202b Reliable Cram Materials
- Useful CCFH-202b Dumps □ CCFH-202b Exam Pass4sure □ CCFH-202b Reliable Cram Materials □ Search for [CCFH-202b] and easily obtain a free download on ➤ www.pdfvce.com □ □Test CCFH-202b Preparation
- CCFH-202b Certification Dump □ CCFH-202b New Study Guide □ CCFH-202b Exam Pass4sure □ Search for ✔ CCFH-202b □✔□ and obtain a free download on 「 www.testkingpass.com 」 □CCFH-202b Exam Guide
- CCFH-202b Exam Pass4sure □□ Latest CCFH-202b Exam Answers □ CCFH-202b Reliable Cram Materials □ Enter { www.pdfvce.com } and search for □ CCFH-202b □ to download for free □CCFH-202b Actual Questions
- CCFH-202b Exam Pass4sure □ CCFH-202b Certification Dump □ CCFH-202b Actual Questions □ Search for ➡ CCFH-202b □□□ and download exam materials for free through " www.easy4engine.com " □New CCFH-202b Dumps Ebook
- Quiz CrowdStrike - CCFH-202b - CrowdStrike Certified Falcon Hunter –High-quality Hot Spot Questions □ Enter " www.pdfvce.com " and search for （ CCFH-202b ） to download for free □Accurate CCFH-202b Answers
- CrowdStrike First-grade CCFH-202b - CrowdStrike Certified Falcon Hunter Hot Spot Questions □ ▹ www.prep4away.com ◃ is best website to obtain ⇛ CCFH-202b ⇚ for free download □CCFH-202b Certification Dump
- Free PDF Quiz CrowdStrike - CCFH-202b –Trustable Hot Spot Questions □ Easily obtain free download of ➥ CCFH-202b □ by searching on □ www.pdfvce.com □ □Latest CCFH-202b Exam Answers
- New CCFH-202b Dumps Ebook □ Test CCFH-202b Preparation □ CCFH-202b Exam Simulator Fee □ Copy URL ▸ www.testkingpass.com ◂ open and search for ✔ CCFH-202b □✔□ to download for free □New CCFH-202b Dumps Ebook
- myportal.utt.edu.tt, www.notebook.ai, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, tutors.a-one.ng, trainings.vyyoma.com, experiment.com, pdfexamdumps4.blogspot.com, Disposable vapes

DOWNLOAD the newest ITexamReview CCFH-202b PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=18MO96flUtsNpdpeC8aB1UZ-UL1wGBiEq