New CCFH-202b Valid Test Camp | Efficient CCFH-202b: CrowdStrike Certified Falcon Hunter 100% Pass

BONUS!!! Download part of ActualTestsQuiz CCFH-202b dumps for free: https://drive.google.com/open?id=1cleR9HofJv5bFSx0IqDcNAF-YtCXez1z

Do you want to pass your exam with the least time? Our CCFH-202b learning materials are high-quality, and you just need to spend 48 to 72 hours on learning, you can pass the exam successfully. What's more, free demo for CCFH-202b exam dumps is available, and you can have a try before buying, so that you can have a deeper understanding of what you are going to buy. If you fail to pass the exam by using CCFH-202b Exam Braindumps, we will give you full refund, and no other questions will be asked. We have online and offline chat service, and if you any questions for CCFH-202b training materials, you can have a conversation with us.

Comparing to other training institution, our valid CCFH-202b vce dumps are affordable, latest and cost-effective, which can overcome the difficulty of valid CCFH-202b Actual Test and ensure you pass the exam. It can not only save your time and money, but also help you clear CrowdStrike practice exam with high rate.

>> CCFH-202b Valid Test Camp <<

CCFH-202b latest exam online & CCFH-202b valid test questions & CCFH-202b test training vce

The money you have invested on updating yourself is worthwhile. The knowledge you have learned is priceless. You can obtain many useful skills on our CCFH-202b study guide, which is of great significance in your daily work. Never feel sorry to invest yourself. Our CCFH-202b Exam Materials deserve your choice. If you still cannot make decisions, you can try our free demo of the

CCFH-202b training quiz.

CrowdStrike CCFH-202b Exam Syllabus Topics:

Topic	Details
Topic 1	• Reports and References: This domain covers using built-in Hunt and Visibility reports and leveraging Events Full Reference documentation for event information.
Topic 2	• Hunting Methodology: This domain covers conducting active hunts, performing outlier analysis, testing hunting hypotheses, constructing queries, and investigating process trees.
Topic 3	• Search and Investigation Tools: This domain covers analyzing file and process metadata, using Investigate Module tools, performing various searches, and interpreting dashboard results.

CrowdStrike Certified Falcon Hunter Sample Questions (Q60-Q65):

NEW QUESTION # 60
What information is shown in Host Search?

- A. Quarantined Files
- B. Processes and Services
- C. Intel Reports
- D. Prevention Policies

Answer: B

Explanation:
Processes and Services is one of the information that is shown in Host Search. Host Search is an Investigate tool that allows you to view events by category, such as process executions, network connections, file writes, etc. Processes and Services is one of the categories that shows information such as process name, command line, parent process name, parent command line, etc. for each process execution event on a host. Quarantined Files, Prevention Policies, and Intel Reports are not shown in Host Search.

NEW QUESTION # 61
A benefit of using a threat hunting framework is that it:

- A. Automatically generates incident reports
- B. Eliminates false positives
- C. Provides high fidelity threat actor attribution
- D. Provides actionable, repeatable steps to conduct threat hunting

Answer: D

Explanation:
A threat hunting framework is a methodology that guides threat hunters in planning, executing, and improving their threat hunting activities. A benefit of using a threat hunting framework is that it provides actionable, repeatable steps to conduct threat hunting in a consistent and efficient manner. A threat hunting framework does not automatically generate incident reports, eliminate false positives, or provide high fidelity threat actor attribution, as these are dependent on other factors such as data sources, tools, and analysis skills.

NEW QUESTION # 62
Which of the following best describes the purpose of the Mac Sensor report?

- A. The Mac Sensor report displays a listing of all Mac hosts without a Falcon sensor installed
- B. The Mac Sensor report provides a detection focused view of known malicious activities occurring on Mac hosts, including machine-learning and indicator-based detections
- C. 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

- D. The Mac Sensor report displays a listing of all Mac hosts with a Falcon sensor installed

Answer: C

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 # 63
Which of the following queries will return the parent processes responsible for launching badprogram.exe?

- A. [search (ProcessList) where Name=badprogram.exe] | search ParentProcessName | table ParentProcessName _time
- B. event_simpleName=processrollup2 [search event_simpleName=processrollup2 FileName=badprogram.exe | rename TargetProcessId_decimal AS ParentProcessId_decimal | fields aid TargetProcessId_decimal] | stats count by FileName _time
- C. event_simpleName=processrollup2 [search event_simpleName=processrollup2 FileName=badprogram.exe | rename ParentProcessId_decimal AS TargetProcessId_decimal | fields aid TargetProcessId_decimal] | stats count by FileName _time
- D. [search (ParentProcess) where name=badprogranrexe] | table ParentProcessName _time

Answer: B

Explanation:
This query will return the parent processes responsible for launching badprogram.exe by using a subsearch to find the processrollup2 events where FileName is badprogram.exe, then renaming the TargetProcessId_decimal field to ParentProcessId_decimal and using it as a filter for the main search, then using stats to count the occurrences of each FileName by _time. The other queries will either not return the parent processes or use incorrect field names or syntax.

NEW QUESTION # 64
SPL (Splunk) eval statements can be used to convert Unix times (Epoch) into UTC readable time Which eval function is correct

What's more, part of that ActualTestsQuiz CCFH-202b dumps now are free: https://drive.google.com/open?id=1cleR9HofJv5bFSx0IqDcNAF-YtCXez1z