2026 Newest CrowdStrike CCFH-202b: CrowdStrike Certified Falcon Hunter Reliable Study Materials

CCFH-202b exam and they all got help from real and updated CrowdStrike CCFH-202b exam questions. You can also be the next successful candidate for the CCFH-202b certification exam. No doubt the CrowdStrike CCFH-202b Certification Exam is one of the most difficult CrowdStrike certification exams in the modern CrowdStrike world. This CCFH-202b exam always gives a tough time to their candidates.

CrowdStrike CCFH-202b Exam Syllabus Topics:

Topic	Details
Topic 1	• Hunting Methodology: This domain covers conducting active hunts, performing outlier analysis, testing hunting hypotheses, constructing queries, and investigating process trees.
Topic 2	• 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 3	• Reports and References: This domain covers using built-in Hunt and Visibility reports and leveraging Events Full Reference documentation for event information.

>> CCFH-202b Reliable Study Materials <<

Realistic CrowdStrike CCFH-202b Reliable Study Materials Are Leading Materials & Trusted CCFH-202b: CrowdStrike Certified Falcon Hunter

If you really intend to pass the CCFH-202b exam, our software will provide you the fast and convenient learning and you will get the best study materials and get a very good preparation for the exam. The content of the CCFH-202b guide torrent is easy to be mastered and has simplified the important information. What's more, our CCFH-202b prep torrent conveys more important information with less questions and answers. The learning is relaxed and highly efficiently with our CCFH-202b exam questions.

CrowdStrike Certified Falcon Hunter Sample Questions (Q55-Q60):

NEW QUESTION # 55
The Process Timeline Events Details table will populate the Parent Process ID and the Parent File columns when the cloudable Event data contains which event field?

- A. RawProcessId_decimal
- B. ParentProcessId_decimal
- C. RpcProcessId_decimal
- D. ContextProcessId_decimal

Answer: B

Explanation:
The ParentProcessId_decimal event field is what the Process Timeline Events Details table will populate the Parent Process ID and the Parent File columns with when the cloudable Event data contains it. The ParentProcessId_decimal event field is the decimal representation of the process identifier for the parent process of the target process. It can be used to trace the process ancestry and identify potential malicious activity. The ContextProcessId_decimal, RawProcessId_decimal, and RpcProcessId_decimal event fields are not used to populate the Parent Process ID and the Parent File columns.

NEW QUESTION # 56
Which document provides information on best practices for writing Splunk-based hunting queries, predefined queries which may be customized to hunt for suspicious network connections, and predefined queries which may be customized to hunt for suspicious processes?

- A. Real Time Response and Network Containment
- B. Hunting and Investigation
- C. Events Data Dictionary
- D. Incident and Detection Monitoring

Answer: B

Explanation:
The Hunting and Investigation document provides information on best practices for writing Splunk-based hunting queries, predefined queries which may be customized to hunt for suspicious network connections, and predefined queries which may be customized to hunt for suspicious processes. As explained above, the Hunting and Investigation document is a guide that provides sample hunting queries, select walkthroughs, and best practices for hunting with Falcon. The other documents do not provide the same information.

NEW QUESTION # 57
The Falcon Detections page will attempt to decode Encoded PowerShell Command line parameters when which PowerShell Command line parameter is present?

- A. -nop
- B. -Hidden
- C. -e
- D. -Command

Answer: D

Explanation:
The Falcon Detections page will attempt to decode Encoded PowerShell Command line parameters when the -Command parameter is present. The -Command parameter allows PowerShell to execute a specified script block or string. If the script block or string is encoded using Base64 or other methods, the Falcon Detections page will try to decode it and show the original command. The -Hidden, -e, and -nop parameters are not related to encoding or decoding PowerShell commands.

NEW QUESTION # 58
What do you click to jump to a Process Timeline from many pages in Falcon, such as a Hash Search?

- A. Process ID or Parent Process ID
- B. CID
- C. PID
- D. Process Timeline Link

Answer: D

Explanation:
The Process Timeline Link is what you click to jump to a Process Timeline from many pages in Falcon, such as a Hash Search. The Process Timeline Link is an icon that looks like three horizontal bars with dots on them. It appears next to each process name or ID on various pages in Falcon, such as Hash Search results, Detection details, Event Search results, etc. Clicking on it will open a new tab with the Process Timeline for that process. The PID, the Process ID or Parent Process ID, and the CID are not what you click to jump to a Process Timeline.

NEW QUESTION # 59
SPL (Splunk) eval statements can be used to convert Unix times (Epoch) into UTC readable time Which eval function is correct