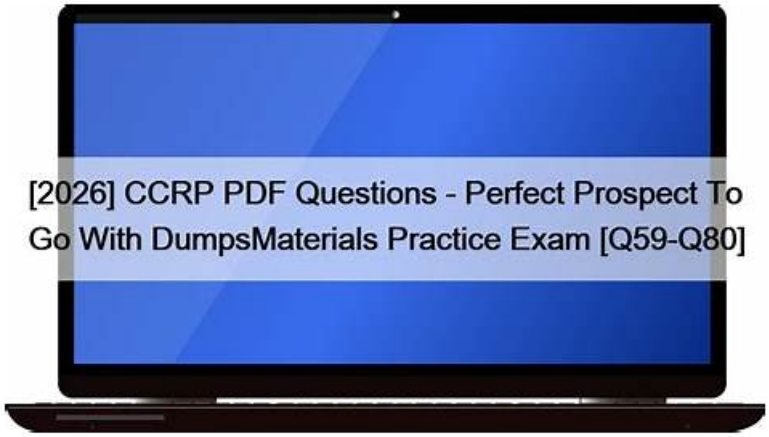
CCFH-202b PDF Questions - Perfect Prospect To Go With CCFH-202b Practice Exam



P.S. Free & New CCFH-202b dumps are available on Google Drive shared by VCEDumps: https://drive.google.com/open?id=1ansTvwYTLXzczuejZyUhbs_HC738ONLy

Our CCFH-202b preparation questions deserve you to have a try. As long as you free download the demos on our website, then you will love our CCFH-202b praparation braindumps for its high quality and efficiency. All you have learned on our CCFH-202b Study Materials will play an important role in your practice. We really want to help you solve all your troubles about learning the CCFH-202b exam. Please give us a chance to prove.

CrowdStrike CCFH-202b Exam Syllabus Topics:

Topic	Details
Topic 1	• Detection Analysis: This domain focuses on analyzing Host and Process Timelines in Falcon to understand events and detections, and pivoting to additional investigative tools.
Topic 2	• 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 3	• Hunting Methodology: This domain covers conducting active hunts, performing outlier analysis, testing hunting hypotheses, constructing queries, and investigating process trees.
Topic 4	• 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.

>> Dumps CCFH-202b Torrent <<

Updated CrowdStrike Dumps Torrent – High Pass Rate Free CCFH-202b Updates

Our company's CCFH-202b exam questions are reliable packed with the best available information. It is always relevant to the real CCFH-202b exam as it is regularly updated by the best and the most professional experts. As long as you study with our CCFH-202b learning braindumps, you will be surprised by the most accurate exam questions and answers that will show up exactly in the real exam. So what are you waiting for? Just put them to the cart and buy!

CrowdStrike Certified Falcon Hunter Sample Questions (Q23-Q28):

NEW QUESTION # 23

Which SPL (Splunk) field name can be used to automatically convert Unix times (Epoch) to UTC readable time within the Flacon Event Search?

- A. utc_time
- B. _time
- C. conv_time
- D. time

Answer: B

Explanation:
_time is the SPL (Splunk) field name that can be used to automatically convert Unix times (Epoch) to UTC readable time within the Falcon Event Search. It is a default field that shows the timestamp of each event in a human-readable format. utc_time, conv_time, and time are not valid SPL field names for converting Unix times to UTC readable time.

NEW QUESTION # 24
Which of the following is a recommended technique to find unique outliers among a set of data in the Falcon Event Search?

- A. Stacking (Frequency Analysis)
- B. Machine Learning
- C. Hunt-and-Peck Search Methodology
- D. Time-based Searching

Answer: A

Explanation:
Stacking (Frequency Analysis) is a recommended technique to find unique outliers among a set of data in the Falcon Event Search. As explained above, stacking involves grouping events by a common attribute and counting their frequency, then sorting them by ascending or descending order to identify rare or common events. This can help find anomalies or deviations from normal behavior that could indicate malicious activity. Hunt-and-Peck Search Methodology, Time-based Searching, and Machine Learning are not specific techniques to find unique outliers among a set of data.

NEW QUESTION # 25
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. PID
- C. CID
- 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 # 26
Which threat framework allows a threat hunter to explore and model specific adversary tactics and techniques, with links to intelligence and case studies?

- A. MITRE ATT&CK
- B. Director of National Intelligence Cyber Threat Framework
- C. Lockheed Martin Cyber Kill Chain
- D. NIST 800-171 Cyber Threat Framework

Answer: A

Explanation:
MITRE ATT&CK is a threat framework that allows a threat hunter to explore and model specific adversary tactics and techniques, with links to intelligence and case studies. It is a knowledge base of adversary behaviors and tactics that covers various platforms, domains, and scenarios. It provides a common language and structure for threat hunters to understand and analyze threats, as well as to share findings and recommendations.

NEW QUESTION # 27
You would like to search for ANY process execution that used a file stored in the Recycle Bin on a Windows host. Select the option to complete the following EAM query.

- A. *$Recycle Bin*
- B. *$Recycle Bin

P.S. Free 2026 CrowdStrike CCFH-202b dumps are available on Google Drive shared by VCEDumps: https://drive.google.com/open?id=1ansTvwYTLXzczuejZyUhbs_HC738ONLy