Buy Today and Save Money with Free CrowdStrike CCFH-202b Questions Updates

Preparation for the professional CrowdStrike Certified Falcon Hunter (CCFH-202b) exam is no more difficult because experts have introduced the preparatory products. With Pass4SureQuiz products, you can pass the CrowdStrike Certified Falcon Hunter (CCFH-202b) exam on the first attempt. If you want a promotion or leave your current job, you should consider achieving a professional certification like CrowdStrike Certified Falcon Hunter (CCFH-202b) exam.

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	• 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 4	• Search and Investigation Tools: This domain covers analyzing file and process metadata, using Investigate Module tools, performing various searches, and interpreting dashboard results.

>> Exam CCFH-202b Overviews <<

Unlimited CCFH-202b Exam Practice - CCFH-202b Reliable Braindumps Book

To suit customers' needs of the CCFH-202b preparation quiz, we make our CCFH-202b exam materials with customer-oriented tenets. Famous brand in the market with combination of considerate services and high quality and high efficiency CCFH-202b study questions. Without poor after-sales services or long waiting for arrival of products, they can be obtained within 5 minutes with well-built after-sales services.

CrowdStrike Certified Falcon Hunter Sample Questions (Q36-Q41):

NEW QUESTION # 36
What information is provided when using IP Search to look up an IP address?

- A. Both internal and external IPs
- B. External IPs only
- C. Internal IPs only
- D. Suspicious IP addresses

Answer: B

Explanation:
IP Search is an Investigate tool that allows you to look up information about external IPs only. It shows information such as geolocation, network connection events, detection history, etc. for each external IP address that has communicated with your hosts. It does not show information about internal IPs, suspicious IPs, or both internal and external IPs.

NEW QUESTION # 37
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.