Get Free Updates For CrowdStrike CCFH-202b Exam Dumps Questions

[Full-Version] 2023 New CCFR-201 Actual Exam
Dumps, CrowdStrike Practice Test [Q12-Q32]

The passing rate of our CCFH-202b study materials is the issue the client mostly care about and we can promise to the client that the passing rate of our product is 99% and the hit rate is also high. Our study materials are selected strictly based on the real CCFH-202b exam and refer to the exam papers in the past years. Our expert team devotes a lot of efforts on them. We also update frequently to guarantee that the client can get more learning CCFH-202b resources and follow the trend of the times. So if you use our CCFH-202b study materials you will pass the CCFH-202b test with high success probability.

For candidates who choose CCFH-202b test materials for the exam, the quality must be one of most important standards for consideration. We have a professional team to collect the first-rate information for the exam, and we also have reliable channel to ensure you that CCFH-202b exam braindumps you receive is the latest one. We are strict with the quality and answers, and CCFH-202b Exam Materials we offer you is the best and the latest one. In addition, we provide you with free update for 365 days, so that you can know the latest information for the exam, and the latest version for CCFH-202b training materials will be sent to your email address autonmatically.

>> CCFH-202b Exam Fee <<

Free PDF CCFH-202b Exam Fee & Leader in Qualification Exams & Well-Prepared CCFH-202b: CrowdStrike Certified Falcon Hunter

To pass the CrowdStrike CCFH-202b exam on the first try, candidates need CrowdStrike Certified Falcon Hunter updated practice material. Preparing with real CCFH-202b exam questions is one of the finest strategies for cracking the exam in one go. Students who study with CCFH-202b Real Questions are more prepared for the exam, increasing their chances of succeeding. The CCFH-202b exam preparation calls for a strong preparation and precise CrowdStrike CCFH-202b practice 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	• 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	• Reports and References: This domain covers using built-in Hunt and Visibility reports and leveraging Events Full Reference documentation for event information.

Topic 4	• Hunting Methodology: This domain covers conducting active hunts, performing outlier analysis, testing hunting hypotheses, constructing queries, and investigating process trees.
Topic 5	• Search and Investigation Tools: This domain covers analyzing file and process metadata, using Investigate Module tools, performing various searches, and interpreting dashboard results.
Topic 6	• Detection Analysis: This domain focuses on analyzing Host and Process Timelines in Falcon to understand events and detections, and pivoting to additional investigative tools.

CrowdStrike Certified Falcon Hunter Sample Questions (Q31-Q36):

NEW QUESTION # 31
In the Powershell Hunt report, what does the "score" signify?

- A. A cumulative score of the various potential command line switches
- B. Number of hosts that ran the PowerShell script
- C. Maliciousness score determined by NGAV
- D. How recently the PowerShell script executed

Answer: A

Explanation:
In the Powershell Hunt report, the score signifies a cumulative score of the various potential command line switches that were used in the PowerShell script execution. The score is based on a weighted system that assigns different values to different switches based on their potential maliciousness or usefulness for threat hunting. For example, -EncodedCommand has a higher value than -NoProfile. The score does not signify the number of hosts that ran the PowerShell script, how recently the PowerShell script executed, or the maliciousness score determined by NGAV.

NEW QUESTION # 32
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. IN
- B. OR
- C. AND
- D. NOT

Answer: B

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 # 33
What elements are required to properly execute a Process Timeline?

- A. Agent ID (AID) and Target Process ID
- B. Hostname and Local Process ID
- C. Target Process ID only
- D. Agent ID (AID) only

Answer: A

Explanation:
The Agent ID (AID) and the Target Process ID are the elements that are required to properly execute a Process Timeline. The Agent ID (AID) is a unique identifier for each host that has a Falcon sensor installed. The Target Process ID is the decimal representation of the process identifier for the process that you want to investigate. These two elements are used to query the cloud for the events related to the process on the host. The Agent ID (AID) only, the Hostname and Local Process ID, and the Target Process ID only are not sufficient to execute a Process Timeline.

NEW QUESTION # 34
Which of the following is TRUE about a Hash Search?

- A. The Hash Search is available on Linux
- B. The Hash Search provides Process Execution History
- C. Wildcard searches are not permitted with the Hash Search
- D. Module Load History is not presented in a Hash Search

Answer: B

Explanation:
The Hash Search is an Investigate tool that allows you to search for a file hash and view its process execution history across all hosts in your environment. It shows information such as process name, command line, parent process name, parent command line, etc. for each execution of the file hash. Wildcard searches are permitted with the Hash Search, as long as they are at least four characters long. The Hash Search is available on Linux, as well as Windows and Mac OS X. Module Load History is presented in a Hash Search, along with other information such as File Write History and Detection History.

NEW QUESTION # 35
In the Powershell Hunt report, what does the filtering condition of commandLine! ="*badstring* " do?

- A. Prevents command lines containing "badstring" from being displayed
- B. Highlights only the command lines containing "badstring"
- C. Displays only the command lines containing "badstring"
- D. Highlights "badstring" in all command lines in the output

Answer: A

Explanation:
In the Powershell Hunt report, the filtering condition of commandLine! ="badstring " prevents command lines containing "badstring" from being displayed. The ! operator is used to negate or exclude a condition from the search results. The * operator is used as a wildcard to match any number of characters before or after the specified string. Therefore, commandLine! ="badstring " means to filter out any command line that has "badstring" anywhere in it. The other options are not correct, as they do not describe what the filtering condition does.

NEW QUESTION # 36
......

Our CCFH-202b exam guide have also set a series of explanation about the complicated parts certificated by the syllabus and are based on the actual situation to stimulate exam circumstance in order to provide you a high-quality and high-efficiency user experience. In addition, the CCFH-202b exam guide function as a time-counter, and you can set fixed time to fulfill your task, so that promote your efficiency in real test. The key strong-point of our CCFH-202b Test Guide is that we impart more important knowledge with fewer questions and answers, with those easily understandable CCFH-202b study braindumps, you will find more interests in them and experience an easy learning process.

CCFH-202b Reliable Study Notes: https://www.testbraindump.com/CCFH-202b-exam-prep.html

- CCFH-202b Exam Topics Pdf □ Valid CCFH-202b Test Question □ New CCFH-202b Test Sims □ Download ➠ CCFH-202b □ for free by simply searching on （ www.dumpsmaterials.com ） □CCFH-202b Test Voucher
- CCFH-202b Exam Fee | High Pass-Rate CrowdStrike CCFH-202b Reliable Study Notes: CrowdStrike Certified Falcon Hunter □ ➥ www.pdfvce.com □ is best website to obtain （ CCFH-202b ） for free download □Minimum CCFH-202b Pass Score

- Minimum CCFH-202b Pass Score □ Downloadable CCFH-202b PDF □ CCFH-202b Key Concepts □ Easily obtain ▶ CCFH-202b ◀ for free download through ➤ www.exam4labs.com □ □CCFH-202b Key Concepts
- CCFH-202b Key Concepts □ Minimum CCFH-202b Pass Score □ CCFH-202b Answers Real Questions ✏ Immediately open □ www.pdfvce.com □ and search for □ CCFH-202b □ to obtain a free download □CCFH-202b Key Concepts
- CCFH-202b Exam Fee | High Pass-Rate CrowdStrike CCFH-202b Reliable Study Notes: CrowdStrike Certified Falcon Hunter □ Search for 「CCFH-202b」 and download exam materials for free through [www.vce4dumps.com] □ □CCFH-202b Key Concepts
- CCFH-202b Exam Topics Pdf □ New CCFH-202b Exam Cram □ Training CCFH-202b Online □ （www.pdfvce.com） is best website to obtain 【CCFH-202b】 for free download □Downloadable CCFH-202b PDF
- Test CCFH-202b Sample Questions □ Free CCFH-202b Exam Questions □ CCFH-202b Valid Test Review □ Download ▶ CCFH-202b ◀ for free by simply searching on □ www.easy4engine.com □ □CCFH-202b Answers Real Questions
- Free PDF Quiz 2026 CCFH-202b: CrowdStrike Certified Falcon Hunter High Hit-Rate Exam Fee □ Immediately open □ www.pdfvce.com □ and search for □ CCFH-202b □ to obtain a free download □Valid CCFH-202b Exam Cram
- Free PDF 2026 High-quality CCFH-202b: CrowdStrike Certified Falcon Hunter Exam Fee □ Go to website 「www.pass4test.com」 open and search for □ CCFH-202b □ to download for free □Downloadable CCFH-202b PDF
- 100% Free CCFH-202b – 100% Free Exam Fee | Excellent CrowdStrike Certified Falcon Hunter Reliable Study Notes □ □ Simply search for □ CCFH-202b □ for free download on { www.pdfvce.com } □Minimum CCFH-202b Pass Score
- CCFH-202b Exam Topics Pdf □ New CCFH-202b Test Objectives □ New CCFH-202b Test Objectives □ Download ➡ CCFH-202b □□□ for free by simply entering ➤ www.examcollectionpass.com □ website □Training CCFH-202b Online
- lms.mfdigitalbd.com, career-aouom.bringsell.com, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, bbs.t-firefly.com, Disposable vapes