Reliable CCFH-202b Test Practice | CCFH-202b Preparation Store

For candidates who buy CCFH-202b test materials online, they may care more about the privacy protection. We can ensure you that your personal information such as your name and email address will be protected well if you choose us. Once the order finishes, your personal information will be concealed. Furthermore, CCFH-202b exam braindumps are high-quality, and we can help you pass the exam just one time. We promise that if you fail to pass the exam, we will give you full refund. If you have any questions for CCFH-202b Exam Test materials, you can contact with us online or by email, we will give you reply as quickly as we can.

CrowdStrike CCFH-202b Exam Syllabus Topics:

Topic	Details
Topic 1	• Search and Investigation Tools: This domain covers analyzing file and process metadata, using Investigate Module tools, performing various searches, and interpreting dashboard results.
Topic 2	• 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 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	• 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 5	• 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.

>> Reliable CCFH-202b Test Practice <<

Top Reliable CCFH-202b Test Practice | Efficient CrowdStrike CCFH-202b: CrowdStrike Certified Falcon Hunter 100% Pass

The great advantage of our CrowdStrike CCFH-202b study prep is that we offer free updates for one year long. On one hand,

these free updates can greatly spare your money since you have the right to free download CrowdStrike Certified Falcon Hunter real dumps as long as you need to. On the other hand, we offer this after-sales service to all our customers to ensure that they have plenty of opportunities to successfully pass their CCFH-202b Actual Exam and finally get their desired certification of CCFH-202b practice materials.

CrowdStrike Certified Falcon Hunter Sample Questions (Q40-Q45):

NEW QUESTION # 40
In which of the following stages of the Cyber Kill Chain does the actor not interact with the victim endpoint(s)?

- A. Weaponization
- B. Installation
- C. Command & control
- D. Exploitation

Answer: A

Explanation:
Weaponization is the stage of the Cyber Kill Chain where the actor does not interact with the victim endpoint(s). Weaponization is where the actor prepares or packages the exploit or payload that will be used to compromise the target. This stage does not involve any communication or interaction with the victim endpoint(s), as it is done by the actor before delivering the weaponized content. Exploitation, Command & Control, and Installation are all stages where the actor interacts with the victim endpoint(s), either by executing code, establishing communication, or installing malware.

NEW QUESTION # 41
In the Powershell Hunt report, what does the filtering condition of commandLine! ="*badstring* " do?

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

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 # 42
What kind of activity does a User Search help you investigate?

- A. A list of DNS queries by the specified user account
- B. A history of Falcon Ul logon activity
- C. A list of process activity executed by the specified user account
- D. A count of failed user logon activity

Answer: C

Explanation:
User Search is an Investigate tool that helps you investigate a list of process activity executed by the specified user account. It shows information such as process name, command line, parent process name, parent command line, etc. for each process that was executed by the user account on any host in your environment. It does not show a history of Falcon UI logon activity, a count of failed user logon activity, or a list of DNS queries by the specified user account.

NEW QUESTION # 43
Which of the following is a way to create event searches that run automatically and recur on a schedule that you set?

- A. Scheduled Searches
- B. Workflows
- C. Scheduled Reports
- D. Event Search

Answer: A

Explanation:
Scheduled Searches are a way to create event searches that run automatically and recur on a schedule that you set. You can use Scheduled Searches to monitor your environment for specific conditions or patterns, generate reports or alerts, or enrich your data with additional fields or tags. Workflows, Event Search, and Scheduled Reports are not ways to create event searches that run automatically and recur on a schedule.

NEW QUESTION # 44
The Events Data Dictionary found in the Falcon documentation is useful for writing hunting queries because:

- A. It provides pre-defined queries you can customize to meet your specific threat hunting needs
- B. It provides a reference of information about the events found in the Investigate > Event Search page of the Falcon Console
- C. It provides a list of all the detect names and descriptions found in the Falcon Cloud
- D. It provides a list of compatible splunk commands used to query event data

Answer: B

Explanation:
This is the correct answer for the same reason as above. The Events Data Dictionary provides a reference of information about the events found in the Investigate > Event Search page of the Falcon Console, which is useful for writing hunting queries. It does not provide pre-defined queries, detect names and descriptions, or compatible splunk commands.

NEW QUESTION # 45
.....

I think these smart tips will help you to study well for the exam and get a brilliant score without any confusion. To get the CrowdStrike Certified Falcon Hunter CCFH-202b practice test, find a reliable source that provides the CCFH-202b Exam Dumps to their clients. CrowdStrike Certified Falcon Hunter CCFH-202b certification exams are not easy but quite tricky to know whether the applicant has complete knowledge regarding the subject or not.

Format

- Test CCFH-202b Questions Fee □ CCFH-202b Exam Online □ CCFH-202b Practice Braindumps □ Search for □ CCFH-202b □ and obtain a free download on " www.torrentvce.com " □CCFH-202b Study Materials Review
- TOP Reliable CCFH-202b Test Practice - CrowdStrike CrowdStrike Certified Falcon Hunter - High-quality CCFH-202b Preparation Store □ Copy URL ➡ www.pdfvce.com □□□ open and search for （ CCFH-202b ） to download for free □CCFH-202b Exam Price
- New Reliable CCFH-202b Test Practice | High-quality CCFH-202b: CrowdStrike Certified Falcon Hunter 100% Pass □ Search on ➡ www.testkingpass.com □□□ for ▹ CCFH-202b ◃ to obtain exam materials for free download □CCFH-202b Exam Online
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, 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, 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, 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, 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, Disposable vapes