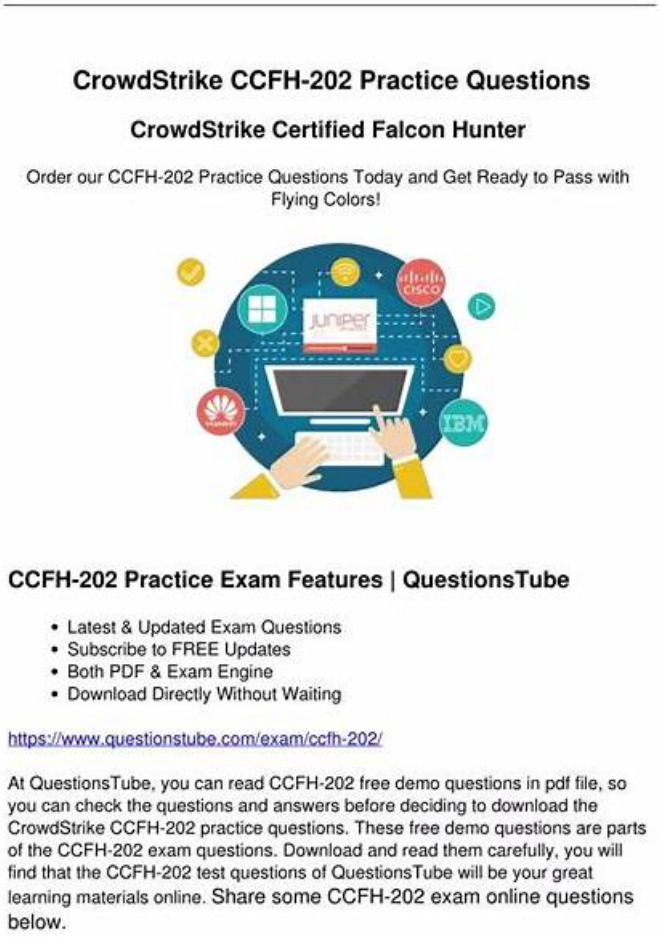
Boost Your Preparation with Braindumpsqa CrowdStrike CCFH-202 Online Practice Test Software



BONUS!!! Download part of Braindumpsqa CCFH-202 dumps for free: https://drive.google.com/open?id=1NJhSZdKdJgELlCFLgpr_FvPxPxHaxwHh

In recent years, some changes are taking place in this line about the new points are being constantly tested in the CCFH-202 real exam. So our experts highlights the new type of questions and add updates into the CCFH-202 practice materials, and look for shifts closely when them take place. At the same time, as we can see that the electronic devices are changing our life day by day, our CCFH-202 study questions are also developed to apply all kinds of eletronic devices.

CrowdStrike CCFH-202 Exam Syllabus Topics:

Topic	Details
Topic 1	• Explain what information a Hash Execution Search provides • Explain what information a Bulk Domain Search provides
Topic 2	• Explain what information a Mac Sensor Report will provide • Conduct hypothesis and hunting lead generation to prove them out using Falcon tools

Topic 3	• Utilize the MITRE ATT&CK Framework to model threat actor behaviors • Explain what information a bulk (Destination) IP search provides
Topic 4	• Explain what information is in the Hunting & Investigation Guide • Differentiate testing, DevOps or general user activity from adversary behavior
Topic 5	• Convert and format Unix times to UTC-readable time • Evaluate information for reliability, validity and relevance for use in the process of elimination
Topic 6	• Demonstrate how to get a Process Timeline • Analyze and recognize suspicious overt malicious behaviors
Topic 7	• Locate built-in Hunting reports and explain what they provide • Identify alternative analytical interpretations to minimize and reduce false positives
Topic 8	• Identify the vulnerability exploited from an initial attack vector • Explain what information is in the Events Data Dictionary

CCFH-202 Reliable Test Book, Latest CCFH-202 Exam Preparation

With the quick development of the eletronic products, more and more eletronic devices are designed to apply to our life. Accordingly there are huge changes on the study models of our CCFH-202 exam dumps as well. There are three different versions of our CCFH-202 Study Guide designed by our specialists in order to satisfy varied groups of people. They are version of the PDF,the Software and the APP online. All these versions of CCFH-202 pratice materials are easy and convenient to use.

CrowdStrike Certified Falcon Hunter Sample Questions (Q56-Q61):

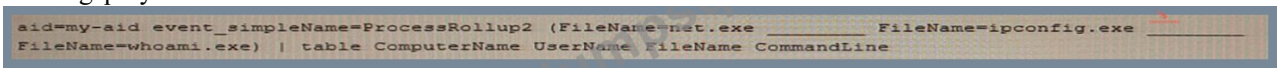
NEW QUESTION # 56
Which of the following is an example of a Falcon threat hunting lead?

- A. An external report describing a unique 5 character file extension for ransomware encrypted files
- B. A routine threat hunt query showing process executions of single letter filename (e.g., a.exe) from temporary directories
- C. A help desk ticket for a user clicking on a link in an email causing their machine to become unresponsive and have high CPU usage
- D. Security appliance logs showing potentially bad traffic to an unknown external IP address

Answer: B

Explanation:
A Falcon threat hunting lead is a piece of information that can be used to initiate or guide a threat hunting activity within the Falcon platform. A routine threat hunt query showing process executions of single letter filename (e.g., a.exe) from temporary directories is an example of a Falcon threat hunting lead, as it can indicate potential malicious activity that can be further investigated using Falcon data and features. Security appliance logs, help desk tickets, and external reports are not examples of Falcon threat hunting leads, as they are not directly related to the Falcon platform or data.

NEW QUESTION # 57
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. AND

- B. OR
- C. NOT
- D. IN

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 # 58
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.

```
aid=my-aid ImageFileName=_____ event_simpleName=ProcessRollup2
```

- A.

What's more, part of that Braindumpsqa CCFH-202 dumps now are free: https://drive.google.com/open?id=1NJhSZdKdJgELlCFLgpr_FvPxPxHaxwHh