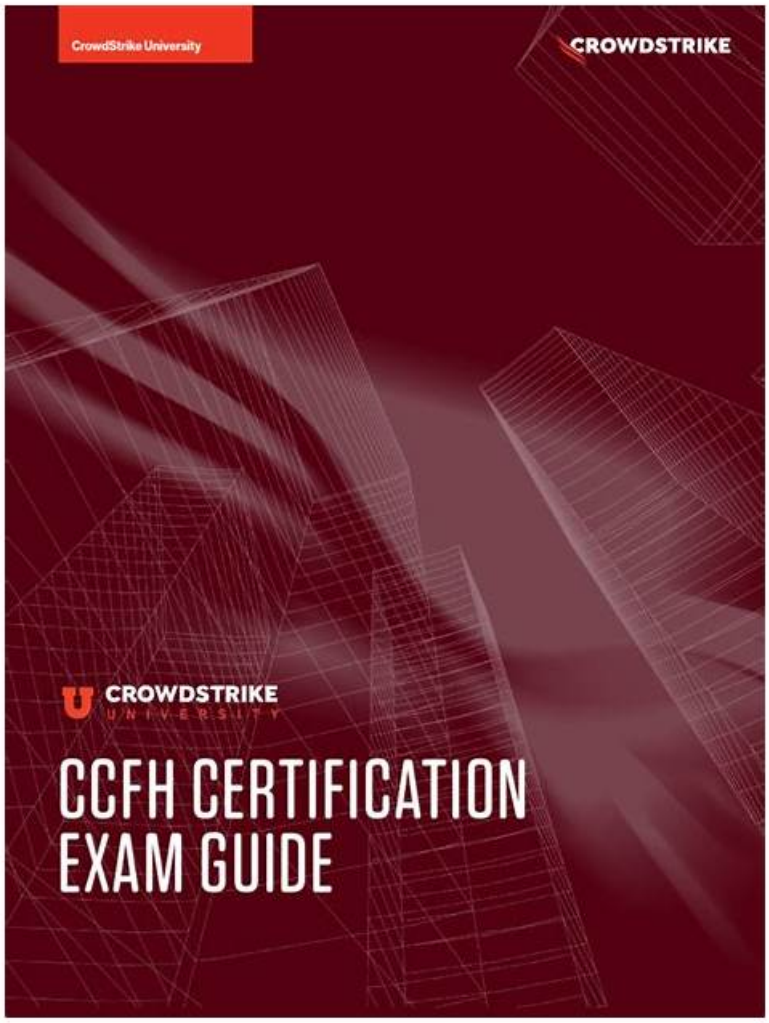
Valid CCFH-202b Exam Tips - Practice CCFH-202b Exam



The three versions of our CCFH-202b training materials each have its own advantage. On the one hand, the software version can simulate the real CCFH-202b examination for all of the users in windows operation system. By actually simulating the real test environment. On the other hand, if you choose to use the software version, you can download our CCFH-202b Exam Prep only for Windows system. We strongly believe that the software version of our CCFH-202b study materials will be of great importance for you to prepare for the exam and all of the employees in our company wish you early success.

We strongly recommend using our CrowdStrike CCFH-202b exam dumps to prepare for the CrowdStrike CCFH-202b certification. It is the best way to ensure success. With our CrowdStrike CCFH-202b practice questions, you can get the most out of your studying and maximize your chances of passing your CrowdStrike CCFH-202b Exam. Pass4sures CrowdStrike CCFH-202b practice test software is the answer if you want to score higher in the CrowdStrike CCFH-202b exam and achieve your academic goals.

>> Valid CCFH-202b Exam Tips <<

Practice CCFH-202b Exam, Certification CCFH-202b Exam Dumps

Our company has authoritative experts and experienced team in related industry. To give the customer the best service, all of our company's CCFH-202b learning materials are designed by experienced experts from various field, so our CCFH-202b Learning materials will help to better absorb the test sites. One of the great advantages of buying our product is that can help you master the core knowledge in the shortest time. At the same time, our CCFH-202b Learning Materials discard the most traditional rote memorization methods and impart the key points of the qualifying exam in a way that best suits the user's learning interests, this is the

highest level of experience that our most authoritative think tank brings to our CCFH-202b learning materials users.

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	• Reports and References: This domain covers using built-in Hunt and Visibility reports and leveraging Events Full Reference documentation for event information.
Topic 3	• Search and Investigation Tools: This domain covers analyzing file and process metadata, using Investigate Module tools, performing various searches, and interpreting dashboard results.

CrowdStrike Certified Falcon Hunter Sample Questions (Q19-Q24):

NEW QUESTION # 19
Refer to Exhibit.
Falcon detected the above file attempting to execute. At initial glance; what indicators can we use to provide an initial analysis of the file?

- A. File name, path, Local and Global prevalence within the environment
- B. VirusTotal, Hybrid Analysis, and Google pivot indicator lights enabled
- C. Local prevalence, IOC Management action, and Event Search
- D. File path, hard disk volume number, and IOC Management action

Answer: A

Explanation:
The file name, path, Local and Global prevalence are indicators that can provide an initial analysis of the file without relying on external sources or tools. The file name can indicate the purpose or origin of the file, such as if it is a legitimate application or a malicious payload. The file path can indicate where the file was located or executed from, such as if it was in a temporary or system directory. The Local and Global prevalence can indicate how common or rare the file is within the environment or across all Falcon customers, which can help assess the risk or impact of the file.

NEW QUESTION # 20
Which Falcon documentation guide should you reference to hunt for anomalies related to scheduled tasks and other Windows related artifacts?

- A. MITRE-Based Falcon Detections Framework
- B. Events Data Dictionary
- C. Customizable Dashboards
- D. Hunting and Investigation

Answer: D

Explanation:
The Hunting and Investigation guide is the Falcon documentation guide that you should reference to hunt for anomalies related to scheduled tasks and other Windows related artifacts. The Hunting and Investigation guide provides sample hunting queries, select walkthroughs, and best practices for hunting with Falcon. It covers various topics such as process execution, network connections, registry activity, scheduled tasks, and more.

NEW QUESTION # 21
You need details about key data fields and sensor events which you may expect to find from Hosts running the Falcon sensor.
Which documentation should you access?

- A. Hunting and Investigation
- B. Streaming API Event Dictionary
- C. Event stream APIs
- D. Events Data Dictionary

Answer: D

Explanation:
The Events Data Dictionary found in the Falcon documentation is useful for writing hunting queries because it provides a reference of information about the events found in the Investigate > Event Search page of the Falcon Console. The Events Data Dictionary describes each event type, field name, data type, description, and example value that can be used to query and analyze event data. The Streaming API Event Dictionary, Hunting and Investigation, and Event stream APIs are not documentation that provide details about key data fields and sensor events.

NEW QUESTION # 22
To view Files Written to Removable Media within a specified timeframe on a host within the Host Search page, expand and refer to the _____dashboard panel.

- A. Command Line and Admin Tools
- B. Suspicious File Activity
- C. Registry, Tasks, and Firewall
- D. Processes and Services

Answer: B

Explanation:
To view Files Written to Removable Media within a specified timeframe on a host within the Host Search page, you need to expand and refer to the Suspicious File Activity dashboard panel. The Suspicious File Activity dashboard panel shows information such as files written to removable media, files written to system directories by non-system processes, files written to startup folders, etc. The other dashboard panels do not show files written to removable media.

NEW QUESTION # 23
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.