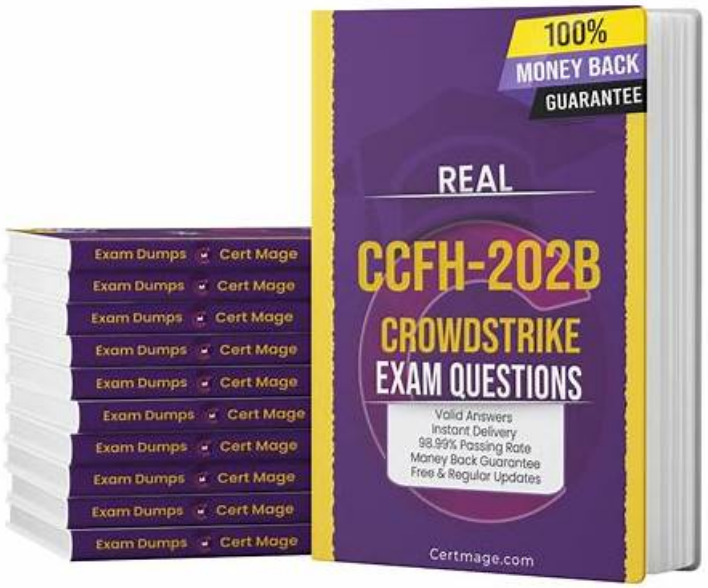
Trustworthy CCFH-202b Valid Test Vce Free & Leader in Qualification Exams & Valid CCFH-202b: CrowdStrike Certified Falcon Hunter



Are you tired of feeling overwhelmed and unsure about how to prepare for the CCFH-202b exam? Are you ready to take control of your future and get the CrowdStrike Certified Falcon Hunter (CCFH-202b) certification you need to accelerate your career? If so, it's time to visit VCETorrent and download real CrowdStrike CCFH-202b Exam Dumps. Our team of experts has designed a CCFH-202b Exam study material that has already helped thousands of students just like you achieve their goals. We offer a comprehensive CrowdStrike Certified Falcon Hunter (CCFH-202b) practice exam material that is according to the content of the CCFH-202b test.

Working in IT field, you definitely want to prove your ability by passing IT certification test. Moreover, the colleagues and the friends with IT certificate have been growing. In this case, if you have none, you will not be able to catch up with the others. For example like CrowdStrike CCFH-202b Certification Exam, it is a very valuable examination, which must help you realize your wishes.

>> CCFH-202b Valid Test Vce Free <<

Latest CrowdStrike Certified Falcon Hunter exam dumps & CCFH-202b braindumps2go vce

CCFH-202b study dumps always managed to build an excellent relationship with our users through the mutual respect and attention we provide to everyone. We sincerely hope our CCFH-202b study dumps will help you to pass the CCFH-202b Exam in a shortest time, we aimed to help you save more time. Once you purchase our CCFH-202b study dumps, we will send to your mailbox within 5-10 minutes, if there are some problem, please contact with us.

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

NEW QUESTION # 56
Which of the following is a suspicious process behavior?

- A. An Internet browser (eg, Internet Explorer) performing multiple DNS requests

- B. PowerShell launching a PowerShell script
- C. PowerShell running an execution policy of RemoteSigned
- D. Non-network processes (eg, notepad exe) making an outbound network connection

Answer: D

Explanation:
Non-network processes are processes that are not expected to communicate over the network, such as notepad.exe. If they make an outbound network connection, it could indicate that they are compromised or maliciously used by an adversary. PowerShell running an execution policy of RemoteSigned is a default setting that allows local scripts to run without digital signatures. An Internet browser performing multiple DNS requests is a normal behavior for web browsing. PowerShell launching a PowerShell script is also a common behavior for legitimate tasks.

NEW QUESTION # 57
What topics are presented in the Hunting and Investigation Guide?

- A. Detailed tutorial on writing advanced queries such as sub-searches and joins
- B. Detailed summary of event names, descriptions, and some key data fields for hunting and investigation
- C. Recommended platform configurations and prevention settings to ensure detections are generated for hunting leads
- D. Sample hunting queries, select walkthroughs and best practices for hunting with Falcon

Answer: D

Explanation:
This is the correct answer for the same reason as above. The Hunting and Investigation guide provides sample hunting queries, select walkthroughs, and best practices for hunting with Falcon. It does not provide a detailed tutorial on writing advanced queries, a detailed summary of event names and descriptions, or recommended platform configurations and prevention settings.

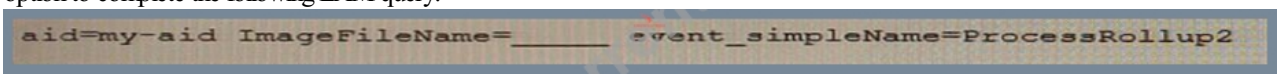
NEW QUESTION # 58
Which of the following does the Hunting and Investigation Guide contain?

- A. Example Event Search queries useful for Falcon platform configuration
- B. A list of all event types specifically used for hunting and their syntax
- C. A list of all event types and their syntax
- D. Example Event Search queries useful for threat hunting

Answer: D

Explanation:
The Hunting and Investigation guide contains example Event Search queries useful for threat hunting. These queries are based on common threat hunting use cases and scenarios, such as finding suspicious processes, network connections, registry activity, etc. The guide also explains how to customize and modify the queries to suit different needs and environments. The guide does not contain a list of all event types and their syntax, as that information is provided in the Events Data Dictionary. The guide also does not contain example Event Search queries useful for Falcon platform configuration, as that is not the focus of the guide.

NEW QUESTION # 59
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. *$Recycle Bin*
- B. *$Recycle Bin