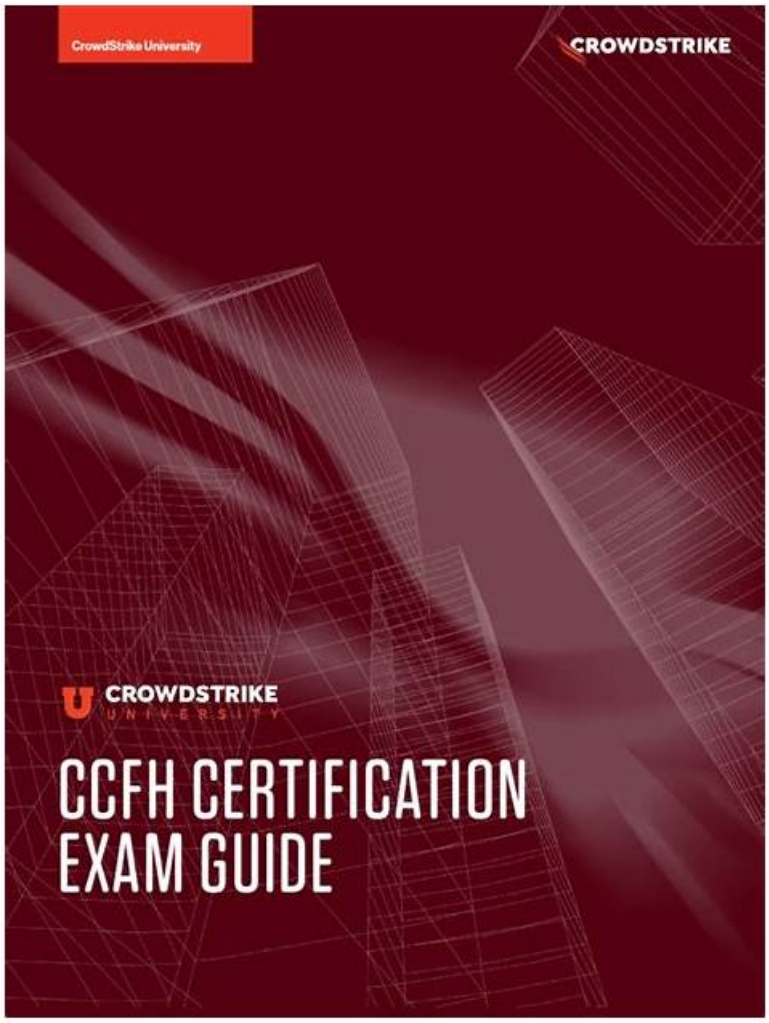
CCFH-202b Exam Preview, CCFH-202b Test Study Guide



What's more, part of that Lead1Pass CCFH-202b dumps now are free: https://drive.google.com/open?id=14MD-SRsLkUs6XWhkl0a3On5TWJEDnC88

We can provide absolutely high quality guarantee for our CCFH-202b practice materials, for all of our CrowdStrike CCFH-202b learning materials are finalized after being approved by industry experts. Without doubt, you will get what you expect to achieve, no matter your satisfied scores or according CCFH-202bcertification file. As long as you choose our CrowdStrike Certified Falcon Hunter exam questions, you will get the most awarded.

CrowdStrike CCFH-202b Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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.

>> CCFH-202b Exam Preview <<

CCFH-202b Test Study Guide, Test CCFH-202b Study Guide

Lead1Pass addresses this issue by offering real CrowdStrike CCFH-202b Questions. Lead1Pass's team of professionals worked tirelessly to create the CCFH-202b questions, ensuring that applicants have access to the most recent and genuine CCFH-202b Exam Questions. With Lead1Pass's help, you can pass the CCFH-202b exam on your first attempt or claim a refund according to certain terms and conditions.

CrowdStrike Certified Falcon Hunter Sample Questions (Q52-Q57):

NEW QUESTION # 52
The Events Data Dictionary found in the Falcon documentation is useful for writing hunting queries because:

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

Answer: A

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 # 53
What kind of activity does a User Search help you investigate?

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

Answer: A

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 # 54
Where would an analyst find information about shells spawned by root, Kernel Module loads, and wget/curl usage?

- A. Sensor Health report
- B. Mac Sensor report
- C. Linux Sensor report
- D. Sensor Policy Daily report

Answer: C

Explanation:
The Linux Sensor report is where an analyst would find information about shells spawned by root, Kernel Module loads, and wget/curl usage. The Linux Sensor report is a pre-defined report that provides a summary view of selected activities on Linux hosts. It shows information such as process execution events, network connection events, file write events, etc. that occurred on Linux

hosts within a specified time range. The Sensor Health report, the Sensor Policy Daily report, and the Mac Sensor report do not provide the same information.

NEW QUESTION # 55
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. Events Data Dictionary
- B. Hunting and Investigation
- C. Event stream APIs
- D. Streaming API Event Dictionary

Answer: A

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 # 56
With Custom Alerts you are able to configure email alerts using predefined templates so you're notified about specific activity in your environment. Which of the following outlines the steps required to properly create a custom alert rule?

- A. Create the query for the alert, setup the email template for the alert, and then set the schedule for the alert
- B. Choose the template you would like to configure, setup how often you would like the alert to run, and then schedule the alert
- C. Create a new custom template, configure the email template, and then create the custom query for the alert
- D. Choose the template you would like to configure, preview the search results, and then schedule the alert

Answer: D

Explanation:
These are the steps required to properly create a custom alert rule. Custom Alerts are a feature that allows you to configure email alerts using predefined templates so you're notified about specific activity in your environment. You can choose from various templates that cover different use cases, such as suspicious PowerShell activity, network connections to risky countries, etc. You can also preview the search results of the template before scheduling the alert. You do not need to create the query for the alert, setup the email template for the alert, or create a new custom template, as these are already provided by the predefined templates.

NEW QUESTION # 57
.....

- CCFH-202b Practice Test: CrowdStrike Certified Falcon Hunter - CCFH-202b Exam Preparation - CCFH-202b Study Guide □ Copy URL ⇛ www.pdfvce.com ⇚ open and search for ➤ CCFH-202b □ to download for free □CCFH-202b Test Certification Cost
- Free PDF Quiz Useful CrowdStrike - CCFH-202b - CrowdStrike Certified Falcon Hunter Exam Preview □ Open website ▸ www.easy4engine.com ◂ and search for [CCFH-202b] for free download □CCFH-202b Passleader Review
- Get High Hit Rate CCFH-202b Exam Preview and Pass Exam in First Attempt □ Search for ➥ CCFH-202b □ on 【 www.pdfvce.com 】 immediately to obtain a free download □Review CCFH-202b Guide
- CCFH-202b Hot Spot Questions □ CCFH-202b Test Quiz ❣ Reliable CCFH-202b Test Prep □ Download ▸ CCFH-202b ◂ for free by simply searching on （ www.prep4sures.top ） □CCFH-202b Hot Spot Questions
- Free PDF The Best CrowdStrike - CCFH-202b Exam Preview □ Open website ▸ www.pdfvce.com ◂ and search for 「 CCFH-202b 」 for free download □Valuable CCFH-202b Feedback
- Vce CCFH-202b Test Simulator □ Study CCFH-202b Center □ CCFH-202b Latest Exam Format □ Go to website ⇛ www.dumpsquestion.com ⇚ open and search for ➽ CCFH-202b □ to download for free □CCFH-202b Valid Test Duration
- Exam CCFH-202b Success □ CCFH-202b Test Quiz □ Valuable CCFH-202b Feedback □ Easily obtain ➥ CCFH-202b □ for free download through ☀ www.pdfvce.com □☀□ □Review CCFH-202b Guide
- Get High Hit Rate CCFH-202b Exam Preview and Pass Exam in First Attempt □ Search on “ www.vceengine.com ” for ➡ CCFH-202b □□□ to obtain exam materials for free download □CCFH-202b Passleader Review
- oisiuwjo137847.bloggerbags.com, mirrorbookmarks.com, tedbpty969522.blog-eye.com, prestonnacz833910.lotrlegendswiki.com, socialnetworkadsinfo.com, wanderlog.com, loriidii017957.webdesign96.com, nevekewz317863.snack-blog.com, nannieltwu482668.wikidank.com, bookmarkshq.com, Disposable vapes

P.S. Free 2026 CrowdStrike CCFH-202b dumps are available on Google Drive shared by Lead1Pass: https://drive.google.com/open?id=14MD-SRsLkUs6XWhkl0a3On5TWJEDnC88