CCFH-202b Technical Training & Exam CCFH-202b Quizzes

PrepAwayPDF is also offering one year free CCFH-202b updates. You can update your CCFH-202b study material for 90 days from the date of purchase. The CrowdStrike Certified Falcon Hunter updated package will include all the past questions from the past papers. You can pass the CCFH-202b exam easily with the help of the PDF dumps included in the package. It will have all the questions that you should cover for the CrowdStrike CCFH-202b Exam. If you are facing any issues with the products you have, then you can always contact our 24/7 support to get assistance.

The pressure is not terrible, and what is terrible is that you choose to evade it. You clearly have seen your own shortcomings, and you know that you really should change. Then, be determined to act! Buying our CCFH-202b exam questions is the first step you need to take. And as long as you study with our CCFH-202b Practice Guide, you will find that the exam is just a piece of cake and the certification is easy to get. With the certification, you will find your future is much brighter.

>> CCFH-202b Technical Training <<

Quiz Authoritative CrowdStrike - CCFH-202b - CrowdStrike Certified Falcon Hunter Technical Training

Many ambitious IT professionals want to make further improvements in the IT industry and be closer from the IT peak. They would choose this difficult CrowdStrike certification CCFH-202b exam to get certification and gain recognition in IT area. CrowdStrike CCFH-202b is very difficult and passing rate is relatively low. But enrolling in the CrowdStrike Certification CCFH-202b Exam is a wise choice, because in today's competitive IT industry, we should constantly upgrade ourselves. However, you can choose many ways to help you pass the exam.

CrowdStrike Certified Falcon Hunter Sample Questions (Q23-Q28):

NEW QUESTION # 23
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 count of failed user logon activity
- D. A list of process activity executed by the specified user account

Answer: D

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 # 24
Which of the following queries will return the parent processes responsible for launching badprogram.exe?

- A. event_simpleName=processrollup2 [search event_simpleName=processrollup2 FileName=badprogram.exe | rename TargetProcessId_decimal AS ParentProcessId_decimal | fields aid TargetProcessId_decimal] | stats count by FileName _time
- B. [search (ParentProcess) where name=badprogranrexe] | table ParentProcessName _time
- C. [search (ProcessList) where Name=badprogram.exe] | search ParentProcessName | table ParentProcessName _time
- D. event_simpleName=processrollup2 [search event_simpleName=processrollup2 FileName=badprogram.exe | rename ParentProcessId_decimal AS TargetProcessId_decimal | fields aid TargetProcessId_decimal] | stats count by FileName _time

Answer: A

Explanation:
This query will return the parent processes responsible for launching badprogram.exe by using a subsearch to find the processrollup2 events where FileName is badprogram.exe, then renaming the TargetProcessId_decimal field to ParentProcessId_decimal and using it as a filter for the main search, then using stats to count the occurrences of each FileName by _time. The other queries will either not return the parent processes or use incorrect field names or syntax.

NEW QUESTION # 25
The help desk is reporting an increase in calls related to user accounts being locked out over the last few days. You suspect that this could be an attack by an adversary against your organization. Select the best hunting hypothesis from the following:

- A. A zero-day vulnerability is being exploited on a Microsoft Exchange server
- B. Users are locking their accounts out because they recently changed their passwords
- C. A password guessing attack is being executed against remote access mechanisms such as VPN
- D. A publicly available web application has been hacked and is causing the lockouts

Answer: C

Explanation:
A hunting hypothesis is a statement that describes a possible malicious activity that can be tested with data and analysis. A good hunting hypothesis should be specific, testable, and relevant to the problem or goal. In this case, the best hunting hypothesis from the following is that a password guessing attack is being executed against remote access mechanisms such as VPN, as it explains the possible cause and method of the user account lockouts in a specific and testable way. A zero-day vulnerability on a Microsoft Exchange server is too vague and does not explain how it relates to the lockouts. A hacked web application is also too vague and does not specify how it causes the lockouts. Users locking their accounts out because they recently changed their passwords is not a malicious activity and does not account for the increase in calls.

NEW QUESTION # 26
In the Powershell Hunt report, what does the "score" signify?

- A. A cumulative score of the various potential command line switches
- B. Maliciousness score determined by NGAV
- C. Number of hosts that ran the PowerShell script
- D. How recently the PowerShell script executed

Answer: A

Explanation:
In the Powershell Hunt report, the score signifies a cumulative score of the various potential command line switches that were used in the PowerShell script execution. The score is based on a weighted system that assigns different values to different switches based on their potential maliciousness or usefulness for threat hunting. For example, -EncodedCommand has a higher value than -NoProfile.

The score does not signify the number of hosts that ran the PowerShell script, how recently the PowerShell script executed, or the maliciousness score determined by NGAV.

NEW QUESTION # 27
Event Search data is recorded with which time zone?

- A. GMT
- B. EST
- C. PST
- D. UTC

Answer: D

Explanation:
Event Search data is recorded with UTC (Coordinated Universal Time) time zone. UTC is a standard time zone that is used as a reference point for other time zones. PST (Pacific Standard Time), GMT (Greenwich Mean Time), and EST (Eastern Standard Time) are not the time zones that Event Search data is recorded with.

NEW QUESTION # 28
.....

One of the main unique qualities of the PrepAwayPDF Google Exam Questions is its ease of use. Our practice exam simulators are user and beginner friendly. You can use CrowdStrike PDF dumps and Web-based software without installation. CrowdStrike Certified Falcon Hunter (CCFH-202b) PDF questions work on all the devices like smartphones, Macs, tablets, Windows, etc. We know that it is hard to stay and study for the CrowdStrike CCFH-202b exam dumps in one place for a long time.

Exam CCFH-202b Quizzes: https://www.prepawaypdf.com/CrowdStrike/CCFH-202b-practice-exam-dumps.html

PrepAwayPDF's top CCFH-202b dumps are meant to deliver you the best knowledge on CrowdStrike Falcon Certification Program certification syllabus contents, It is very popular among the IT personals because it brings great convenience in your practice of CCFH-202b free demo, Do you want to pass the CCFH-202b real test with ease, CrowdStrike CCFH-202b Technical Training Choosing Free4Dump, choosing success.

To his surprise, one of the foundational solutions CCFH-202b offered was industrial design, No one could tell me, to my satisfaction, why I should getrid of the moss, PrepAwayPDF's Top CCFH-202b Dumps are meant to deliver you the best knowledge on CrowdStrike Falcon Certification Program certification syllabus contents.

Your Investment with PrepAwayPDF CCFH-202b CrowdStrike Certified Falcon Hunter Practice Test is Secured

It is very popular among the IT personals because it brings great convenience in your practice of CCFH-202b free demo, Do you want to pass the CCFH-202b real test with ease?

Choosing Free4Dump, choosing success, People are very busy nowadays, so they want to make good use of their lunch time for preparing for their CCFH-202b exam.

- Get Ready for CCFH-202b with CrowdStrike's Updated Dumps and Stay Current with Free Updates for 1 Year □ Open website ⇒ www.prepawaypdf.com ⇐ and search for ➠ CCFH-202b □ for free download □New CCFH-202b Cram Materials
- New CCFH-202b Exam Test □ CCFH-202b Test Testking □ Official CCFH-202b Practice Test □ Search for □ CCFH-202b □ and download exam materials for free through ▹ www.pdfvce.com ◃ □Official CCFH-202b Practice Test
- Latest CCFH-202b Technical Training - Find Shortcut to Pass CCFH-202b Exam □ Enter 「 www.troytecdumps.com 」 and search for 「 CCFH-202b 」 to download for free □CCFH-202b Test Testking
- CCFH-202b Exam Practice □ Test CCFH-202b Score Report □ CCFH-202b Exam Practice □ Open website { www.pdfvce.com } and search for ➤ CCFH-202b □ for free download □Latest CCFH-202b Exam Camp
- CCFH-202b Discount □ Free CCFH-202b Download □ CCFH-202b Cert □ Search for ☀ CCFH-202b □☀□ and download it for free on □ www.vceengine.com □ website ↴Test CCFH-202b Score Report
- Pdf CCFH-202b Free □ Official CCFH-202b Practice Test □ CCFH-202b Test Testking □ Go to website 《 www.pdfvce.com 》 open and search for ☀ CCFH-202b □☀□ to download for free □Test CCFH-202b Score Report

- Test CCFH-202b Tutorials □ Exam CCFH-202b Pass4sure □ Reliable CCFH-202b Dumps Free ♥ Search for ▹ CCFH-202b ◃ and obtain a free download on ➠ www.dumpsmaterials.com □ □Free CCFH-202b Download
- CCFH-202b Test Testking □ Exam CCFH-202b Pass4sure □ New CCFH-202b Exam Test □ Open " www.pdfvce.com " and search for 《 CCFH-202b 》 to download exam materials for free □CCFH-202b Discount
- Pdf CCFH-202b Free □ CCFH-202b Exam Practice □ New CCFH-202b Exam Test □ Search for " CCFH-202b " and download it for free immediately on ➤ www.vceengine.com □ □Test CCFH-202b Score Report
- Latest CCFH-202b Technical Training - Find Shortcut to Pass CCFH-202b Exam □ Simply search for 《 CCFH-202b 》 for free download on 「 www.pdfvce.com 」 □CCFH-202b Test Testking
- Get Ready for CCFH-202b with CrowdStrike's Updated Dumps and Stay Current with Free Updates for 1 Year □ Easily obtain 《 CCFH-202b 》 for free download through （ www.examcollectionpass.com ） □New CCFH-202b Exam Test
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, letterboxd.com, www.stes.tyc.edu.tw, bbs.t-firefly.com, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, giphy.com, Disposable vapes