CCFH-202考試指南 -您最好的助力CrowdStrike Certified Falcon Hunter更新

P.S. VCESoft在Google Drive上分享了免費的、最新的CCFH-202考試題庫：https://drive.google.com/open?id=1t9HggzugIAAqicXVP7KlvS8GK1bm-QWL

通過CrowdStrike CCFH-202的考試是不簡單的，選擇合適的培訓是你成功的第一步，選擇好的資訊來源是你成功的保障，而VCESoft的產品是有很好的資訊來源保障。如果你選擇了VCESoft的產品不僅可以100%保證你通過CrowdStrike CCFH-202認證考試，還可以為你提供長達一年的免費更新。

VCESoft的CCFH-202考古題和實際的認證考試一樣，不僅包含了實際考試中的所有問題，而且考古題的軟體版完全類比了真實考試的氛圍。使用了VCESoft的考古題，你在參加考試時完全可以應付自如，輕鬆地獲得高分。

>> CCFH-202考試指南 <<

CCFH-202考試指南和認證成功保證，簡便的培訓方式和CrowdStrike CrowdStrike Certified Falcon Hunter

VCESoft 的 CCFH-202 考古題包括了PDF電子檔和軟體考題形式，全新的收錄了CrowdStrike 認證考試的所有試題，並根據真實的考題變化而不斷變化，參考考試指南編訂，而且適合全球考生適用。該 CCFH-202 考古題是考試原題的完美組合，覆蓋率95%以上，答案由多位專業資深講師原版破解得出，正確率100%。你還可以點擊我們網站下載 CCFH-202 考古題的demo，你會明白這才是你想要的。

CrowdStrike CCFH-202 考試大綱：

主題	簡介
主題 1	• Identify the vulnerability exploited from an initial attack vector • Explain what information is in the Events Data Dictionary
主題 2	• Utilize the MITRE ATT&CK Framework to model threat actor behaviors • Explain what information a bulk (Destination) IP search provides
主題 3	• Explain what information a Mac Sensor Report will provide • Conduct hypothesis and hunting lead generation to prove them out using Falcon tools

主題 4	• Convert and format Unix times to UTC-readable time • Evaluate information for reliability, validity and relevance for use in the process of elimination
主題 5	• Explain what information a Hash Execution Search provides • Explain what information a Bulk Domain Search provides
主題 6	• Locate built-in Hunting reports and explain what they provide • Identify alternative analytical interpretations to minimize and reduce false positives
主題 7	• From the Statistics tab, use the left click filters to refine your search • Explain what the “join” command does and how it can be used to join disparate queries
主題 8	• Explain what information a Source IP Search provides • Explain what the “table” command does and demonstrate how it can be used for formatting output
主題 9	• Demonstrate how to get a Process Timeline • Analyze and recognize suspicious overt malicious behaviors

最新的 CrowdStrike Certified Falcon Hunter CCFH-202 免費考試真題 (Q28-Q33):

問題 #28
How do you rename fields while using transforming commands such as table, chart, and stats?

- A. By using the "renamed" keyword after the field name eg "stats count renamed totalcount by ComputerName"
- B. By specifying the desired name after the field name eg "stats count totalcount by ComputerName"
- C. By renaming the fields with the "rename" command after the transforming command e.g. "stats count by ComputerName | rename count AS total_count"
- D. You cannot rename fields as it would affect sub-queries and statistical analysis

答案：C

解題說明：
The rename command is used to rename fields while using transforming commands such as table, chart, and stats. It can be used after the transforming command and specify the old and new field names with the AS keyword. You can rename fields as it would not affect sub-queries and statistical analysis, as long as you use the correct field names in your queries. The renamed keyword and the desired name after the field name are not valid ways to rename fields.

問題 #29
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. Event stream APIs
- B. Streaming API Event Dictionary
- C. Hunting and Investigation
- D. Events Data Dictionary

答案：D

解題說明：
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.

問題 #30
In the Powershell Hunt report, what does the "score" signify?

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

答案：D

解題說明：
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.

問題 #31
Which SPL (Splunk) field name can be used to automatically convert Unix times (Epoch) to UTC readable time within the Flacon Event Search?

- A. time
- B. conv_time
- C. _time
- D. utc_time

答案：C

解題說明：
_time is the SPL (Splunk) field name that can be used to automatically convert Unix times (Epoch) to UTC readable time within the Falcon Event Search. It is a default field that shows the timestamp of each event in a human-readable format. utc_time, conv_time, and time are not valid SPL field names for converting Unix times to UTC readable time.

問題 #32
What kind of activity does a User Search help you investigate?

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

答案：B

解題說明：
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.

問題 #33
.....

- CCFH-202證照指南 □ CCFH-202資訊 □ CCFH-202認證考試解析 □ ▷ www.kaoguti.com ◁上搜索 ➡ CCFH-202 □□□輕鬆獲取免費下載CCFH-202考古題
- CCFH-202題庫 □ CCFH-202認證考試解析 ⤵ CCFH-202題庫資訊 □ "www.newdumpspdf.com"最新✔ CCFH-202 □✔□問題集合CCFH-202考題資源
- 高質量的CCFH-202考試指南，最有效的學習資料幫助妳快速通過CCFH-202考試 □ 開啟[www.newdumpspdf.com]輸入➡ CCFH-202 □□□並獲取免費下載CCFH-202題庫
- CCFH-202題庫 □ CCFH-202考試資訊 □ CCFH-202考古題 □ 免費下載{ CCFH-202 }只需在□ www.newdumpspdf.com □上搜索CCFH-202考試備考經驗
- 高質量的CCFH-202考試指南，最有效的學習資料幫助妳快速通過CCFH-202考試 □ 打開➠ tw.fast2test.com □搜尋【 CCFH-202 】以免費下載考試資料CCFH-202考古題
- CCFH-202資料 □ CCFH-202資料 □ CCFH-202認證考試解析 □ 「 www.newdumpspdf.com 」上的免費下載[CCFH-202]頁面立即打開CCFH-202考試大綱
- 完美的CCFH-202考試指南和認證考試的領導者材料和完整的CCFH-202更新 □ 打開▶ www.pdfexamdumps.com ◀搜尋（ CCFH-202 ）以免費下載考試資料CCFH-202考試備考經驗
- 完美的CCFH-202考試指南和認證考試的領導者材料和完整的CCFH-202更新 □ ➠ www.newdumpspdf.com □ □上搜索□ CCFH-202 □輕鬆獲取免費下載CCFH-202考試備考經驗
- CCFH-202考試指南：CrowdStrike Certified Falcon Hunter確定通過考試，CrowdStrike CCFH-202更新 □ 在□ www.newdumpspdf.com □網站上免費搜索□ CCFH-202 □題庫CCFH-202資訊
- 使用保證通過的CrowdStrike CCFH-202考試指南高效率地學習您的CrowdStrike CCFH-202考試 □ 複製網址（ www.newdumpspdf.com ）打開並搜索{ CCFH-202 }免費下載CCFH-202套裝
- CCFH-202題庫資訊 □ CCFH-202套裝 □ CCFH-202權威考題 □ 進入▷ www.newdumpspdf.com ◁搜尋➥ CCFH-202 □免費下載CCFH-202考題資源
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

P.S. VCESoft在Google Drive上分享了免費的、最新的CCFH-202考試題庫：https://drive.google.com/open?id=1t9Hggzug1AAqicXVP7KlvS8GK1bm-QWL