CCFH-202b認證考試，免費下載CCFH-202b考題

P.S. Testpdf在Google Drive上分享了免費的、最新的CCFH-202b考試題庫：https://drive.google.com/open?id=10w9ldU-yqRNY8PPYXGcHnhwd8aGzDMRq

Testpdf提供的產品有很高的品質和可靠性。你可以先在網上免費下載部分Testpdf提供的關於CrowdStrike CCFH-202b 認證考試的練習題和答案作為嘗試。在你使用之後，相信你會很滿意我們的產品的。這麼好的一個能幫助你順利通過考試的產品，你還在猶豫什麼，快將Testpdf的產品加入您的購物車吧。

CrowdStrike CCFH-202b 考試大綱：

主題	簡介
主題 1	• Hunting Analytics: This domain focuses on recognizing malicious behaviors, evaluating information reliability, decoding command line activity, identifying infection patterns, distinguishing legitimate from adversary activity, and identifying exploited vulnerabilities.
主題 2	• 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.
主題 3	• Search and Investigation Tools: This domain covers analyzing file and process metadata, using Investigate Module tools, performing various searches, and interpreting dashboard results.
主題 4	• 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.
主題 5	• Hunting Methodology: This domain covers conducting active hunts, performing outlier analysis, testing hunting hypotheses, constructing queries, and investigating process trees.

>> CCFH-202b認證考試 <<

免費下載CCFH-202b考題，CCFH-202b最新題庫

如果你選擇了Testpdf，Testpdf可以確保你100%通過CrowdStrike CCFH-202b 認證考試，如果考試失敗，Testpdf將全額退款給你。

最新的 CrowdStrike Falcon Certification Program CCFH-202b 免費考試真題 (Q50-Q55):

問題 #50
What is the main purpose of the Mac Sensor report?

- A. To provide vulnerability assessment for Mac Operating Systems
- B. To identify endpoints that are in Reduced Functionality Mode
- C. To provide a summary view of selected activities on Mac hosts
- D. To provide a dashboard for Mac related detections

答案：C

解題說明：
The Mac Sensor report is a pre-defined report that provides a summary view of selected activities on Mac hosts. It shows information such as process execution events, network connection events, file write events, etc. that occurred on Mac hosts within a specified time range. The Mac Sensor report does not identify endpoints that are in Reduced Functionality Mode, provide vulnerability assessment for Mac Operating Systems, or provide a dashboard for Mac related detections.

問題 #51
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 renaming the fields with the "rename" command after the transforming command e.g. "stats count by ComputerName | rename count AS total_count"
- C. By specifying the desired name after the field name eg "stats count totalcount by ComputerName"
- D. You cannot rename fields as it would affect sub-queries and statistical analysis

答案：B

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 #52
Which threat framework allows a threat hunter to explore and model specific adversary tactics and techniques, with links to intelligence and case studies?

- A. MITRE ATT&CK
- B. NIST 800-171 Cyber Threat Framework
- C. Lockheed Martin Cyber Kill Chain
- D. Director of National Intelligence Cyber Threat Framework

答案：A

解題說明：
MITRE ATT&CK is a threat framework that allows a threat hunter to explore and model specific adversary tactics and techniques, with links to intelligence and case studies. It is a knowledge base of adversary behaviors and tactics that covers various platforms, domains, and scenarios. It provides a common language and structure for threat hunters to understand and analyze threats, as well as to share findings and recommendations.

問題 #53
A benefit of using a threat hunting framework is that it:

- A. Provides actionable, repeatable steps to conduct threat hunting
- B. Provides high fidelity threat actor attribution
- C. Eliminates false positives
- D. Automatically generates incident reports

答案：A

解題說明：
A threat hunting framework is a methodology that guides threat hunters in planning, executing, and improving their threat hunting activities. A benefit of using a threat hunting framework is that it provides actionable, repeatable steps to conduct threat hunting in a consistent and efficient manner. A threat hunting framework does not automatically generate incident reports, eliminate false positives, or provide high fidelity threat actor attribution, as these are dependent on other factors such as data sources, tools, and analysis skills.

問題 #54
Which Falcon documentation guide should you reference to hunt for anomalies related to scheduled tasks and other Windows related artifacts?

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

答案：A

解題說明：
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.

問題 #55
.....

- 完整的CCFH-202b認證考試擁有模擬真實考試環境與場境的軟件VCE版本＆高通過率的免費下載CCFH-202b考題 □ 到□ www.newdumpspdf.com □搜索【 CCFH-202b 】輕鬆取得免費下載CCFH-202b權威考題
- CCFH-202b題庫分享 □ CCFH-202b證照信息 □ CCFH-202b證照信息 □ 在（ www.vcesoft.com ）網站上免費搜索➤ CCFH-202b □題庫CCFH-202b套裝
- 最新版的CCFH-202b認證考試，CrowdStrike CrowdStrike Falcon Certification Program認證CCFH-202b考試題庫提供免費下載 □ 在✔ www.newdumpspdf.com □✔□網站上免費搜索□ CCFH-202b □題庫CCFH-202b題庫資訊
- 免費下載CCFH-202b考題 □ CCFH-202b權威考題 □ CCFH-202b證照信息 □ 在《 www.kaoguti.com 》上搜索➤ CCFH-202b □並獲取免費下載新版CCFH-202b題庫
- rebeccasmmy684033.mdkblog.com, companyspage.com, www.stes.tyc.edu.tw, gretappdd225657.blog-mall.com, tornadosocial.com, 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, bookmark-share.com, 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, madesocials.com, Disposable vapes

從Google Drive中免費下載最新的Testpdf CCFH-202b PDF版考試題庫：https://drive.google.com/open?id=10w9ldU-yqRNY8PPYXGcHnhwd8aGzDMRq