# 試験の準備方法-真実的なCCFH-202b難易度受験料試験-効果的なCCFH-202b日本語復習赤本


無料でクラウドストレージから最新のPassTest CCFH-202b PDFダンプをダウンロードする：https://drive.google.com/open?id=19QFwE9NPQ5_3xeLqF-f-2HrJIAh8pVxU

CrowdStrike Certified Falcon Hunter CCFH-202bは、技術的な精度の最高水準を高め、認定された主題と専門家のみを使用します。最新の正確なCCFH-202b試験トレントをクライアントに提供し、提供する質問と回答は実際の試験に基づいています。合格率が高く、約98%-100%であることをお約束します。また、CCFH-202bテストブレインダンプは高いヒット率を高め、試験を刺激してCCFH-202b試験の準備を整えることができます。あなたの成功は、CCFH-202b試験問題に縛られています。

## CrowdStrike CCFH-202b 認定試験の出題範囲：

| トピック | 出題範囲 |
|---|---|
| トピック 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. |
| トピック 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. |

| | |
|---|---|
| トピック 3 | • Hunting Methodology: This domain covers conducting active hunts, performing outlier analysis, testing hunting hypotheses, constructing queries, and investigating process trees. |
| トピック 4 | • 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. |
| トピック 5 | • 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. |
| トピック 6 | • Search and Investigation Tools: This domain covers analyzing file and process metadata, using Investigate Module tools, performing various searches, and interpreting dashboard results. |



## 高品質なCCFH-202b難易度受験料一回合格-真実的なCCFH-202b日本語復習赤本

弊社のCCFH-202b問題集は大好評を博しました。専門家たちの整理と分析を通して、問題集の質量はよくなりました。だから、お客様は我々のCCFH-202b問題集を安心で利用することができます。弊社の商品の質量に疑問がありましたら、我々のサイトで無料のCCFH-202bデモをダウンロードして見ることができます。

## CrowdStrike Certified Falcon Hunter 認定 CCFH-202b 試験問題 (Q37-Q42):

**質問 # 37**
What information is provided when using IP Search to look up an IP address?

- A. Suspicious IP addresses
- B. External IPs only
- C. Both internal and external IPs
- D. Internal IPs only

**正解：B**

解説：
IP Search is an Investigate tool that allows you to look up information about external IPs only. It shows information such as geolocation, network connection events, detection history, etc. for each external IP address that has communicated with your hosts. It does not show information about internal IPs, suspicious IPs, or both internal and external IPs.

**質問 # 38**
Which Falcon documentation guide should you reference to hunt for anomalies related to scheduled tasks and other Windows related artifacts?

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

**正解：C**

解説：
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.

**質問 # 39**
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. Hunting and Investigation
- C. Streaming API Event Dictionary
- D. Events Data Dictionary

**正解：D**

解説：
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.

**質問 # 40**
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. A password guessing attack is being executed against remote access mechanisms such as VPN
- C. Users are locking their accounts out because they recently changed their passwords
- D. A publicly available web application has been hacked and is causing the lockouts

**正解：B**

解説：
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.

**質問 # 41**
How do you rename fields while using transforming commands such as table, chart, and stats?

- A. You cannot rename fields as it would affect sub-queries and statistical analysis
- 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. By using the "renamed" keyword after the field name eg "stats count renamed totalcount by ComputerName"

**正解：B**

解説：
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.

**質問 # 42**
.....

常にCrowdStrike　CCFH-202b試験に参加する予定があるお客様は「こちらの問題集には、全部で何問位、掲載されておりますか？」といった質問を提出しました。心配なくて我々PassTestのCrowdStrike　CCFH-202b試験問題集は実際試験のすべての問題種類をカバーします。70%の問題は解説がありますし、試験の内容を理解しやすいと助けます。

**CCFH-202b日本語復習赤本**: https://www.passtest.jp/CrowdStrike/CCFH-202b-shiken.html

- CCFH-202b真実試験 □ CCFH-202b日本語版受験参考書 □ CCFH-202b合格資料 □ ➥ www.shikenpass.com □は、➠ CCFH-202b □を無料でダウンロードするのに最適なサイトですCCFH-202b真実試験
- CCFH-202bテストガイド、CrowdStrike CCFH-202b試験問題集、CCFH-202bトレーニング資料 □ ➡ www.goshiken.com □□□で《 CCFH-202b 》を検索し、無料でダウンロードしてくださいCCFH-202b過去問題
- 高品質なCCFH-202b難易度受験料 - 合格スムーズCCFH-202b日本語復習赤本 | 効果的なCCFH-202b勉強の資料 □ （ CCFH-202b ）を無料でダウンロード[ jp.fast2test.com ]で検索するだけCCFH-202b受験資料更新版
- CCFH-202b合格資料 □ CCFH-202b専門トレーリング □ CCFH-202b日本語資格取得 □ [ CCFH-202b ]を無料でダウンロード➽ www.goshiken.com □ウェブサイトを入力するだけCCFH-202b模擬資料
- 試験の準備方法-一番優秀なCCFH-202b難易度受験料試験-権威のあるCCFH-202b日本語復習赤本 □ ⇒ CCFH-202b ⇐を無料でダウンロード▹ www.goshiken.com ◃ウェブサイトを入力するだけCCFH-202b最新テスト
- タイトル：CrowdStrike Certified Falcon Hunter試験テストエンジン、CCFH-202b予備資料、CrowdStrike Certified Falcon Hunter模擬試験 □ ➤ www.goshiken.com □から▹ CCFH-202b ◃を検索して、試験資料を無料でダウンロードしてくださいCCFH-202b真実試験
- CCFH-202b過去問題 □ CCFH-202b受験料 □ CCFH-202b模擬資料 □ { www.mogiexam.com }に移動し、➠ CCFH-202b □を検索して無料でダウンロードしてくださいCCFH-202bミシュレーション問題
- CCFH-202b真実試験 □ CCFH-202b真実試験 □ CCFH-202b難易度 □ ✔ www.goshiken.com □✔□に移動し、□ CCFH-202b □を検索して、無料でダウンロード可能な試験資料を探しますCCFH-202b合格資料
- CCFH-202b試験の準備方法｜有難いCCFH-202b難易度受験料試験｜便利なCrowdStrike Certified Falcon Hunter日本語復習赤本 □ ⇛ www.mogiexam.com ⇚サイトにて（ CCFH-202b ）問題集を無料で使おうCCFH-202b模擬資料
- CCFH-202b合格資料 □ CCFH-202b合格資料 □ CCFH-202b受験料 □ ☀ CCFH-202b □☀□を無料でダウンロード《 www.goshiken.com 》ウェブサイトを入力するだけCCFH-202b模擬問題
- CCFH-202b最新テスト □ CCFH-202b真実試験 □ CCFH-202b日本語版受験参考書 □ 《 www.topexam.jp 》から簡単に（ CCFH-202b ）を無料でダウンロードできますCCFH-202b受験資料更新版
- scalar.usc.edu, youemerge.com, network.crcna.org, www.longisland.com, www.slideshare.net, 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, telegra.ph, scalar.usc.edu, writeablog.net, www.stes.tyc.edu.tw, Disposable vapes

BONUS！！！ PassTest CCFH-202bダンプの一部を無料でダウンロード：https://drive.google.com/open?id=19QFwE9NPQ5_3xeLqF-f-2HrJIAh8pVxU