CrowdStrike CCFH-202b試験問題集、CCFH-202b無料試験

さらに、PassTest CCFH-202bダンプの一部が現在無料で提供されています：https://drive.google.com/open?id=1mMyVtLuBS_8jN7Lhn2tjK7PuPrDkB_s7

これらの2つの特性により、CCFH-202bガイドトレントを使用するほぼすべての候補者が一度にテストに合格できることがわかります。これは自己決定ではありません。統計によると、当社のCCFH-202bガイドトレントは98％〜99％の高い合格率を達成しており、これは他のすべてをかなり上回る程度です。同時に、CCFH-202bテストトレントが毎日更新されるかどうかを確認する専門スタッフがいます。メールでお問い合わせいただく場合でも、オンラインでお問い合わせいただく場合でも、できるだけ早く問題を解決できるようサポートいたします。心配する必要はまったくありません。

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	• Search and Investigation Tools: This domain covers analyzing file and process metadata, using Investigate Module tools, performing various searches, and interpreting dashboard results.
トピック 2	• Hunting Methodology: This domain covers conducting active hunts, performing outlier analysis, testing hunting hypotheses, constructing queries, and investigating process trees.
トピック 3	• 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.

CCFH-202b無料試験、CCFH-202b模試エンジン

PassTestは長い歴史を持っているCrowdStrikeのCCFH-202bトレーニング資料が提供されるサイトです。IT領域で長い時間に存在していますから、現在のよく知られていて、知名度が高い状況になりました。これは受験生の皆様を助けた結果です。PassTestが提供したCrowdStrikeのCCFH-202bトレーニング資料は問題と解答に含まれていて、IT技術専門家たちによって開発されたものです。CrowdStrikeのCCFH-202b認定試験を受けたいのなら、PassTestを選ぶのは疑いないことです。

CrowdStrike Certified Falcon Hunter 認定 CCFH-202b 試験問題 (Q47-Q52):

質問 # 47
Which of the following Event Search queries would only find the DNS lookups to the domain: www randomdomain com?

- A. event_simpleName=DnsRequest DomainName=www randomdomain com
- B. event_simpleName=DnsRequest DomainName=randomdomain com ComputerName=localhost
- C. ComputerName=localhost DnsRequest "randomdomain com"
- D. Dns=randomdomain com

正解：A

解説：
This Event Search query would only find the DNS lookups to the domain www randomdomain com, as it specifies the exact event type and domain name to match. The other queries would either find other events or domains that are not relevant to the question.

質問 # 48
While you're reviewing Unresolved Detections in the Host Search page, you notice the User Name column contains "hostnameS " What does this User Name indicate?

- A. The User Name is not relevant for the dashboard
- B. There is no User Name associated with the event
- C. The User Name is a System User
- D. The Falcon sensor could not determine the User Name

正解：B

解説：
When you see "hostnameS" in the User Name column in the Host Search page, it means that there is no User Name associated with the event. This can happen when the event is related to a system process or service that does not have a user context. It does not mean that the User Name is a System User, that the User Name is not relevant for the dashboard, or that the Falcon sensor could not determine the User Name.

質問 # 49
When exporting the results of the following event search, what data is saved in the exported file (assuming Verbose Mode)?
event_simpleName=*Written | stats count by ComputerName

- A. The results of the Statistics tab
- B. No data Results can only be exported when the "table" command is used
- C. All events in the Events tab
- D. The text of the query

正解：A

解説：
When exporting the results of an event search, the data that is saved in the exported file depends on the mode and the tab that is

selected. In this case, the mode is Verbose and the tab is Statistics, as indicated by the stats command. Therefore, the data that is saved in the exported file is the results of the Statistics tab, which shows the count of events by ComputerName. The text of the query, all events in the Events tab, and no data are not correct answers.

質問 # 50
SPL (Splunk) eval statements can be used to convert Unix times (Epoch) into UTC readable time Which eval function is correct