CCFH-202b専門試験、CCFH-202b関連資料

CCFH-202b準備資料のガイダンスの下で、さまざまな学生に合わせた試験の焦点を提供し、例と図およびIT専門家を追加することで長くて退屈な参考書を簡素化できるため、より生産的かつ効率的になることができます変更できない問題を回避するために、CCFH-202bガイドトレントを毎日更新します。そして、あなたはあなたの日常生活の中で自分自身のために時刻表やto-soリストを設定する方法についてCCFH-202b研究急流を勉強することができます。したがって、CCFH-202b学習教材の学習過程で喜びを見つけます。

CCFH-202b試験に合格すると多くのメリットが得られることは誰もが知っていますが、CrowdStrikeすべての受験者がそれを達成するのは容易ではありません。 CCFH-202bガイド急流は、すべての受験者が試験に合格するのを支援することを目的としたツールです。 私たちの試験資料は、コンピュータと人の量に制限なしでインストールおよびダウンロードできます。 弊社が提供するCCFH-202b学習資料が有用であり、テストに合格するのに役立つことを保証します。 製品を購入すると、便利な方法を使用して、いつでもどこでもCCFH-202b試験トレントを学習できます。 そのため、購入の前後に安心して、CCFH-202b学習教材にウイルスがないことを信頼してください。 CrowdStrike Certified Falcon Hunter当社の製品Topexamに慣れるために、CCFH-202b学習教材の機能と利点を次のようにリストします。

>> CCFH-202b専門試験 <<

更新するCCFH-202b専門試験 & 合格スムーズCCFH-202b関連資料 | 有難いCCFH-202b参考書内容

CCFH-202b最新の試験トレントは、資格試験ごとに分類が異なるため、ユーザーはユーザーの実際のニーズに応じて独自の学習モードを選択できます。 CCFH-202b試験の質問は、ユーザーが選択できるさまざまな学習モードを提供します。これは、コンピューターや携帯電話の複数のクライアントがオンラインで勉強したり、オフライン統合のためにデータを印刷したりするために使用できます。手頃な価格と実践を完璧にサポートする最新のCCFH-202b試験のトレントは、CCFH-202b試験の質問のみを気に入っています。

CrowdStrike Certified Falcon Hunter 認定 CCFH-202b 試験問題 (Q33-Q38):

質問 # 33
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. time

- C. conv_time
- D. utc_time

正解：A

解説：
_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.

質問 # 34
Refer to Exhibit.
Falcon detected the above file attempting to execute. At initial glance; what indicators can we use to provide an initial analysis of the file?

- A. File name, path, Local and Global prevalence within the environment
- B. Local prevalence, IOC Management action, and Event Search
- C. VirusTotal, Hybrid Analysis, and Google pivot indicator lights enabled
- D. File path, hard disk volume number, and IOC Management action

正解：A

解説：
The file name, path, Local and Global prevalence are indicators that can provide an initial analysis of the file without relying on external sources or tools. The file name can indicate the purpose or origin of the file, such as if it is a legitimate application or a malicious payload. The file path can indicate where the file was located or executed from, such as if it was in a temporary or system directory. The Local and Global prevalence can indicate how common or rare the file is within the environment or across all Falcon customers, which can help assess the risk or impact of the file.

質問 # 35
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 publicly available web application has been hacked and is causing the lockouts
- B. Users are locking their accounts out because they recently changed their passwords
- C. A zero-day vulnerability is being exploited on a Microsoft Exchange server
- D. A password guessing attack is being executed against remote access mechanisms such as VPN

正解：D

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 # 36
What information is provided when using IP Search to look up an IP address?

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

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 # 37
You would like to search for ANY process execution that used a file stored in the Recycle Bin on a Windows host. Select the option to complete the following EAM query.

- A. *$Recycle Bin