高パスレートCCFH-202問題無料 &資格試験のリーダー &現実的CrowdStrike CrowdStrike Certified Falcon Hunter

まずCCFH-202問題集を使って試験の知識点を理解します。

通読段階は、初めて本を読む時：

1 本を通読して、記憶しなくてもいいです。目的は前に習った内容をもう一度知ることです。

2 同時に、前の本に書いたポイントに注目して、自分が知っている新しいポイントをマークします。

このステップは、CCFH-202問題集における実際の試験問題に関する研究と結合して行うことができます。CCFH-202試験の題型と範囲、及び知識点の考察方法を研究します。

もうちょっと詳しく話し、私達の普段の習慣は直接に上述の勉強と知識点を区別しないです。でも、今はGOWUKAKUは逆にCCFH-202問題集の中の本当の問題を研究して、テストでカバーされているすべての知識点を調べます。

本を読み、要点をマークし、実際の質問を理解します。3つのステップが同時に実行されます。知識のポイントに従って、CCFH-202問題集で関連する質問と回答を見つけ出す。教科書のどのページに回答があるかをマークします（問題の回答の下にソースがある質問もあります）。

これは最初のレビューですが、暗記する必要はなく、理解するのみなので、実際には非常に簡単です。

CCFH-202問題集を使用して知識ポイントを覚えるのに役立てる

そして第二ステップに進みます

BONUS！！！ CertShiken CCFH-202ダンプの一部を無料でダウンロード：https://drive.google.com/open?id=14NV7cOs5mlsEd7eSJZDRvmVIXEnPsk2w

「私はだめです。」という話を永遠に言わないでください。これは皆さんのためのアドバイスです。難しいCrowdStrikeのCCFH-202認定試験に合格する能力を持たないと思っても、あなたは効率的な骨の折れないトレーニングツールを選んで試験に合格させることができます。CertShikenのCrowdStrikeのCCFH-202試験トレーニング資料はとても良いトレーニングツールで、１００パーセントの合格率を保証します。それに、資料の値段は手頃です。CertShikenを利用したらあなたはきっと大いに利益を得ることができます。ですから、「私はだめです。」という話を言わないでください。諦めないのなら、希望が現れています。あなたの希望はCertShikenのCrowdStrikeのCCFH-202試験トレーニング資料にありますから、速く掴みましょう。

CrowdStrike CCFH-202 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• 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
トピック 2	• Utilize the MITRE ATT&CK Framework to model threat actor behaviors • Explain what information a bulk (Destination) IP search provides
トピック 3	• Explain what information a Mac Sensor Report will provide • Conduct hypothesis and hunting lead generation to prove them out using Falcon tools
トピック 4	• Locate built-in Hunting reports and explain what they provide • Identify alternative analytical interpretations to minimize and reduce false positives
トピック 5	• Demonstrate how to get a Process Timeline • Analyze and recognize suspicious overt malicious behaviors
トピック 6	• Explain what information is in the Hunting & Investigation Guide • Differentiate testing, DevOps or general user activity from adversary behavior
トピック 7	• Explain what information a Source IP Search provides • Explain what the “table” command does and demonstrate how it can be used for formatting output
トピック 8	• Identify the vulnerability exploited from an initial attack vector • Explain what information is in the Events Data Dictionary

>> CCFH-202問題無料 <<

正確的CCFH-202｜最高のCCFH-202問題無料試験｜試験の準備方法CrowdStrike Certified Falcon Hunter専門試験

CertShikenは実環境であなたの本当のCrowdStrike CCFH-202試験に準備するプロセスを見つけられます。もしあなたが初心者だったら、または自分の知識や専門的なスキルを高めたいのなら、CertShikenのCrowdStrikeのCCFH-202問題集があなたを助けることができ、一歩一歩でその念願を実現することにヘルプを差し上げます。CertShikenのCrowdStrikeのCCFH-202は試験に関する全ての質問が解決して差し上げられます。それに一年間の無料更新サービスを提供しますから、CertShikenのウェブサイトをご覧ください。

CrowdStrike Certified Falcon Hunter 認定 CCFH-202 試験問題 (Q21-Q26):

質問 # 21
When performing a raw event search via the Events search page, what are Event Actions?

- A. Event Actions are pivotable workflows including connecting to a host, pre-made event searches and pivots to other investigatory pages such as host search
- B. Event Actions contains the summary of actions taken by the Falcon sensor such as quarantining a file, prevent a process from executing or taking no actions and creating a detection only
- C. Event Actions contains an audit information log of actions an analyst took in regards to a specific detection
- D. Event Actions is the field name that contains the event name defined in the Events Data Dictionary such as ProcessRollup, SyntheticProcessRollup, DNS request, etc

正解：A

解説：
When performing a raw event search via the Events search page, Event Actions are pivotable workflows that allow you to perform various tasks related to the event or the host. For example, you can connect to a host using Real Time Response, run pre-made event searches based on the event type or name, or pivot to other investigatory pages such as host search, hash search, etc. Event Actions do not contain audit information log, summary of actions taken by the Falcon sensor, or the event name defined in the Events Data Dictionary.

質問 # 22
Event Search data is recorded with which time zone?

- A. UTC
- B. GMT
- C. EST
- D. PST

正解：A

解説：
Event Search data is recorded with UTC (Coordinated Universal Time) time zone. UTC is a standard time zone that is used as a reference point for other time zones. PST (Pacific Standard Time), GMT (Greenwich Mean Time), and EST (Eastern Standard Time) are not the time zones that Event Search data is recorded with.

質問 # 23
Which tool allows a threat hunter to populate and colorize all known adversary techniques in a single view?

- A. MITRE ATT&CK Navigator
- B. OWASP Threat Dragon
- C. MISP
- D. OpenXDR

正解：A

解説：
MITRE ATT&CK Navigator is a tool that allows a threat hunter to populate and colorize all known adversary techniques in a single view. It is based on the MITRE ATT&CK framework, which is a knowledge base of adversary behaviors and tactics. The tool enables threat hunters to create custom matrices, layers, annotations, and filters to explore and model specific adversary techniques, with links to intelligence and case studies.

質問 # 24
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. You cannot rename fields as it would affect sub-queries and statistical analysis
- D. By renaming the fields with the "rename" command after the transforming command e.g. "stats count by ComputerName | rename count AS total_count"

正解：D

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 # 25
SPL (Splunk) eval statements can be used to convert Unix times (Epoch) into UTC readable time Which eval function is correct