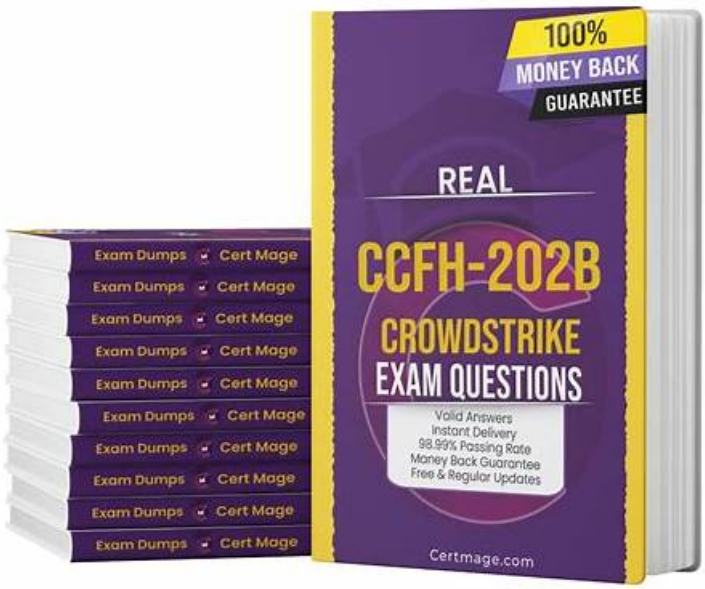
Valid CCFH-202b Exam Answers - Valid CCFH-202b Test Materials



Before you decide to buy PrepAwayETE of CrowdStrike CCFH-202b exam questions, you will have a free part of the questions and answers as a trial. So that you will know the quality of the PrepAwayETE of CrowdStrike CCFH-202b Exam Training materials. The CrowdStrike CCFH-202b exam of PrepAwayETE is the best choice for you.

CrowdStrike CCFH-202b Exam Syllabus Topics:

Topic	Details
Topic 1	• Search and Investigation Tools: This domain covers analyzing file and process metadata, using Investigate Module tools, performing various searches, and interpreting dashboard results.
Topic 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.
Topic 3	• Hunting Methodology: This domain covers conducting active hunts, performing outlier analysis, testing hunting hypotheses, constructing queries, and investigating process trees.
Topic 4	• Detection Analysis: This domain focuses on analyzing Host and Process Timelines in Falcon to understand events and detections, and pivoting to additional investigative tools.

>> Valid CCFH-202b Exam Answers <<

Valid CrowdStrike CCFH-202b Test Materials & Test CCFH-202b Sample Questions

If you are sure you have learnt all the CCFH-202b exam questions, you have every reason to believe it. PrepAwayETE's CCFH-202b exam dumps have the best track record of awarding exam success and a number of candidates have already obtained their

targeted CCFH-202b Certification relying on them. They provide you the real exam scenario and by doing them repeatedly you enhance your confidence to CCFH-202b questions answers without any hesitation.

CrowdStrike Certified Falcon Hunter Sample Questions (Q38-Q43):

NEW QUESTION # 38
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. Hunting and Investigation
- B. Streaming API Event Dictionary
- C. Events Data Dictionary
- D. Event stream APIs

Answer: C

Explanation:
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.

NEW QUESTION # 39
Lateral movement through a victim environment is an example of which stage of the Cyber Kill Chain?

- A. Actions on Objectives
- B. Delivery
- C. Exploitation
- D. Command & Control

Answer: D

Explanation:
Lateral movement through a victim environment is an example of the Command & Control stage of the Cyber Kill Chain. The Cyber Kill Chain is a model that describes the phases of a cyber attack, from reconnaissance to actions on objectives. The Command & Control stage is where the adversary establishes and maintains communication with the compromised systems and moves laterally to expand their access and control.

NEW QUESTION # 40
What Search page would help a threat hunter differentiate testing, DevOPs, or general user activity from adversary behavior?

- A. IP Search
- B. User Search
- C. Domain Search
- D. Hash Search

Answer: B

Explanation:
User Search is a search page that allows a threat hunter to search for user activity across endpoints and correlate it with other events. This can help differentiate testing, DevOPs, or general user activity from adversary behavior by identifying anomalous or suspicious user actions, such as logging into multiple systems, running unusual commands, or accessing sensitive files.

NEW QUESTION # 41
When performing a raw event search via the Events search page, what are Event Actions?

- A. Event Actions contains an audit information log of actions an analyst took in regards to a specific detection

- 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 is the field name that contains the event name defined in the Events Data Dictionary such as ProcessRollup, SyntheticProcessRollup, DNS request, etc
- D. Event Actions are pivotable workflows including connecting to a host, pre-made event searches and pivots to other investigatory pages such as host search

Answer: D

Explanation:
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.

NEW QUESTION # 42
Which structured analytic technique contrasts different hypotheses to determine which is the best leading (prioritized) hypothesis?

- A. Competitive analysis
- B. Analysis of competing hypotheses
- C. Key assumptions check
- D. Model hunting framework

Answer: B

Explanation:
Analysis of competing hypotheses is a structured analytic technique that contrasts different hypotheses to determine which is the best leading (prioritized) hypothesis. It involves listing all the possible hypotheses, identifying the evidence and assumptions for each hypothesis, evaluating the consistency and reliability of the evidence and assumptions, and rating the likelihood of each hypothesis based on the evidence and assumptions.

NEW QUESTION # 43
.....

There are a lot of the functions on our CCFH-202b exam questions to help our candidates to reach the best condition befor they take part in the real exam. I love the statistics report function and the timing function most. The statistics report function helps the learners find the weak links and improve them accordingly. The timing function of our CCFH-202b training quiz helps the learners to adjust their speed to answer the questions and keep alert and our CCFH-202b study materials have set the timer.

CCFH-202b □□□ for free download □CCFH-202b Valid Test Vce Free

- CCFH-202b Valid Exam Cost □ Test CCFH-202b Answers □ CCFH-202b Test Centres □ Copy URL （ www.prep4away.com ） open and search for [CCFH-202b] to download for free □CCFH-202b Test Centres
- 100% Pass Quiz CrowdStrike - CCFH-202b –High Pass-Rate Valid Exam Answers □ Easily obtain free download of 《 CCFH-202b 》 by searching on ➽ www.pdfvce.com □ □Free CCFH-202b Exam Dumps
- Latest Released CrowdStrike Valid CCFH-202b Exam Answers: CrowdStrike Certified Falcon Hunter □ Download ➤ CCFH-202b □ for free by simply entering 《 www.prep4sures.top 》 website □CCFH-202b Valid Test Vce Free
- 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, maryam6409708.blogspot.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes