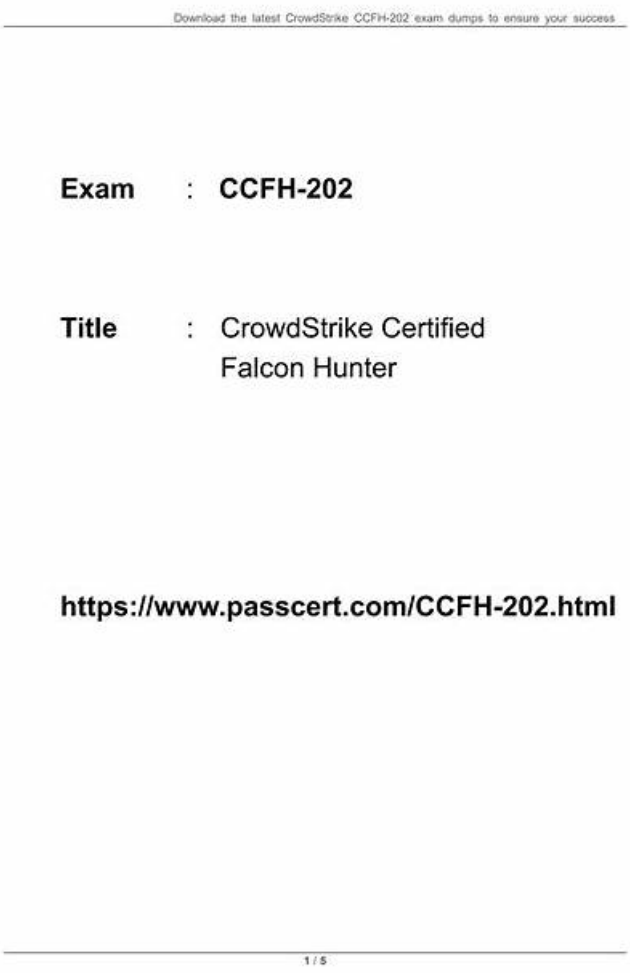
Latest CCFH-202b Test Dumps | Reliable CCFH-202b Exam Camp



Nowadays, online learning is very popular among students. Most candidates have chosen our CCFH-202b learning engine to help them pass the exam. Our company has accumulated many experiences after ten years' development. We never stop researching and developing the new version of the CCFH-202b practice materials. With our CCFH-202b study questions, you can easily get your expected certification as well as a brighter future.

CrowdStrike CCFH-202b Exam Syllabus Topics:

Topic	Details
Topic 1	• Reports and References: This domain covers using built-in Hunt and Visibility reports and leveraging Events Full Reference documentation for event information.
Topic 2	• Search and Investigation Tools: This domain covers analyzing file and process metadata, using Investigate Module tools, performing various searches, and interpreting dashboard results.
Topic 3	• Detection Analysis: This domain focuses on analyzing Host and Process Timelines in Falcon to understand events and detections, and pivoting to additional investigative tools.

Topic 4	• 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.

>> Latest CCFH-202b Test Dumps <<

Reliable CCFH-202b Exam Camp - CCFH-202b Useful Dumps

We Lead2Passed are growing faster and faster owing to our high-quality latest CCFH-202b certification guide materials with high pass rate. Based on our past data, our pass rate of CCFH-202b training guide is high up to 99% to 100% recently years. Many customer will become regular customer and think of us once they have exams to clear after choosing our CCFH-202b Exam Guide one time. So we have no need to spend much spirits to advertise but only put most into researching and after-sale service. As long as you study with our CCFH-202b learning questions, you will find that it is a right choice.

CrowdStrike Certified Falcon Hunter Sample Questions (Q33-Q38):

NEW QUESTION # 33
Which field should you reference in order to find the system time of a *FileWritten event?

- A. timestamp
- B. ContextTimeStamp_decimal
- C. ProcessStartTime_decimal
- D. FileTimeStamp_decimal

Answer: B

Explanation:
ContextTimeStamp_decimal is the field that shows the system time of the event that triggered the sensor to send data to the cloud. In this case, it would be the time when the file was written. FileTimeStamp_decimal is the field that shows the last modified time of the file, which may not be the same as the time when the file was written. ProcessStartTime_decimal is the field that shows the start time of the process that performed the file write operation, which may not be the same as the time when the file was written. Timestamp is the field that shows the time when the sensor data was received by the cloud, which may not be the same as the time when the file was written.

NEW QUESTION # 34
In which of the following stages of the Cyber Kill Chain does the actor not interact with the victim endpoint(s)?

- A. Exploitation
- B. Command & control
- C. Installation
- D. Weaponization

Answer: D

Explanation:
Weaponization is the stage of the Cyber Kill Chain where the actor does not interact with the victim endpoint(s). Weaponization is where the actor prepares or packages the exploit or payload that will be used to compromise the target. This stage does not involve any communication or interaction with the victim endpoint(s), as it is done by the actor before delivering the weaponized content. Exploitation, Command & Control, and Installation are all stages where the actor interacts with the victim endpoint(s), either by executing code, establishing communication, or installing malware.

NEW QUESTION # 35
SPL (Splunk) eval statements can be used to convert Unix times (Epoch) into UTC readable time Which eval function is correct