Web-Based CrowdStrike CCFR-201b Practice Test - Compatible with All Major

The CrowdStrike CCFR-201b exam is one of the top-rated career advancement certifications in the market. With the CrowdStrike Certified Falcon Responder CCFR-201b certification exam everyone can validate their skills and knowledge after passing the CCFR-201b exam. The CrowdStrike CCFR-201b certification exam will recognize your expertise and knowledge in the market. You will get solid proof of your proven skill set. There are other countless benefits that you can gain after passing the CrowdStrike Certified Falcon Responder CCFR-201b Certification Exam. But the problem is how to pass the CrowdStrike CCFR-201b exam. The CrowdStrike CCFR-201b certification exam is not an easy exam. It is a challenging exam that gives taught time to candidates. However, with the assistance of CrowdStrike CCFR-201b PDF Questions and practice tests you can pass the CCFR-201b exam easily.

CrowdStrike CCFR-201b Exam Syllabus Topics:

Topic	Details
Topic 1	• Event Search: This domain focuses on performing advanced event searches from detections, refining searches using event actions, and distinguishing between commonly used event types.
Topic 2	• Search Tools: This domain covers utilizing User Search, IP Search, Hash Search, Host Search, and Bulk Domain Search to gather intelligence during investigations.
Topic 3	• Detection Analysis: This domain covers analyzing and triaging detections in Falcon, including interpreting dashboards, endpoint detections, contextual data, process views, prevalence, IOCs, and implementing hash management actions like blocking, allowlisting, and exclusions.

Topic 4	• Real Time Response (RTR): This domain covers RTR technical capabilities, administrative settings, connecting to hosts, using RTR commands for remediation, utilizing custom scripts, setting up workflows, and reviewing audit logs.
Topic 5	• ATT&CK Frameworks: This domain covers understanding the MITRE ATT&CK framework and applying its tactics and techniques within Falcon to provide context to detections.

>> CCFR-201b Exam Overviews <<

Practice CCFR-201b Questions - Test CCFR-201b Dates

Candidates can benefit a lot if they can get the certificate of the exam: they can get a better job in a big company, and the wage will also promote. Our CCFR-201b Training Material will help you to get the certificate easily by provide you the answers and questions. The questions and answers of the practicing materials is correct and the updated one, we will also update the version for you regularly, therefore, you can know the latest changes for the exam.

CrowdStrike Certified Falcon Responder Sample Questions (Q151-Q156):

NEW QUESTION # 151
Which of the following statements about the 'Detection Activity' report is FALSE?

- A. Clicking on a ProcessID value within the report pivots to a pre-populated Event Search.
- B. The report can be exported to a CSV file.
- C. It provides a summary of all alerts over a selected time period.
- D. It can be filtered by host name or severity.

Answer: A

NEW QUESTION # 152
The Activity Dashboard is a core feature for security teams. What is the primary purpose of this dashboard?

- A. To view the raw telemetry of every event happening on the network.
- B. To provide a summary of the current threat state and active detections in the environment.
- C. To manage the installation and update of Falcon sensors.
- D. To audit the changes made by other Falcon administrators.

Answer: B

NEW QUESTION # 153
Which of the following sentences best describes the technical visibility provided by the 'Host Timeline' view?

- A. A log of every time the Falcon sensor was updated or restarted.
- B. Every host-relevant event (Process, File, Registry, Network) recorded in a given timeframe.
- C. A history of every hardware change or driver update on the endpoint.
- D. A list of every time a user has logged in or out of the machine.

Answer: B

NEW QUESTION # 154
When a responder chooses to 'Release' a file from quarantine because it was determined to be a false positive, what type of allowlist is automatically created in the background?

- A. Path-based allowlist
- B. Filename-based allowlist

- C. Command-line allowlist
- D. Hash-based allowlist

Answer: D

NEW QUESTION # 155
The Falcon sensor is designed to provide deep visibility into endpoint activity, yet it is not omniscient.
According to the Cyber Kill Chain model, which of the following stages does the Falcon sensor typically NOT have visibility over?

- A. Delivery of a malicious document via an encrypted email attachment
- B. Exploitation of a memory-resident vulnerability
- C. Weaponization of a malicious payload on the adversary's infrastructure
- D. Installation of a persistent backdoor

Answer: C

NEW QUESTION # 156
.....

Choosing our CCFR-201b learning guide is not only an enrichment of learning content, but also an opportunity to improve our own discovery space. Our CCFR-201b study dumps could bring huge impact to your personal development, because in the process of we are looking for a job, hold a certificate you have more advantage than your competitors, the company will be a greater probability of you. After using our CCFR-201b Study Dumps, users can devote more time and energy to focus on their major and makes themselves more and more prominent in the professional field. Therefore, our CCFR-201b exam materials can help you achieve multiple returns in the future, provide you with more opportunities to pursue higher life goals, and create a higher quality of life.