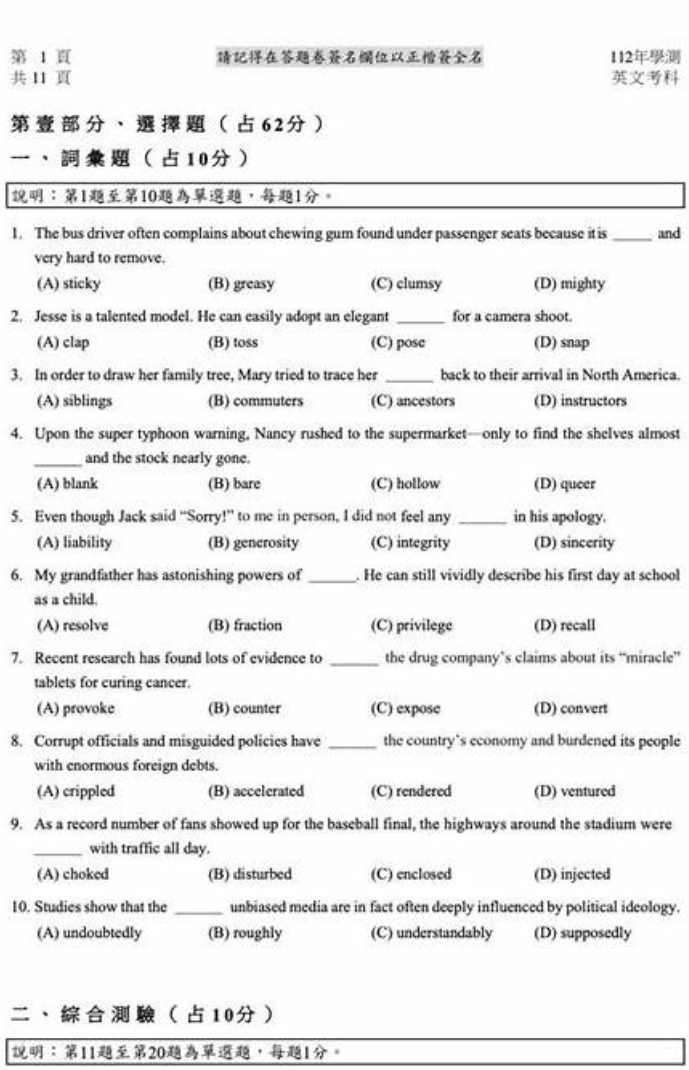
高質量的CCFR-201b題庫和資格考試中的領先供應平臺＆有效的CCFR-201b：CrowdStrike Certified Falcon Responder



第 1 頁 共 11 頁　請記得在答題卷簽名欄位以正楷簽全名　112年學測 英文考科

第壹部分、選擇題（占62分）

一、詞彙題（占10分）

說明：第1題至第10題為單選題，每題1分。

1. The bus driver often complains about chewing gum found under passenger seats because it is _____ and very hard to remove.
(A) sticky (B) greasy (C) clumsy (D) mighty

2. Jesse is a talented model. He can easily adopt an elegant _____ for a camera shoot.
(A) clap (B) toss (C) pose (D) snap

3. In order to draw her family tree, Mary tried to trace her _____ back to their arrival in North America.
(A) siblings (B) commuters (C) ancestors (D) instructors

4. Upon the super typhoon warning, Nancy rushed to the supermarket—only to find the shelves almost _____ and the stock nearly gone.
(A) blank (B) bare (C) hollow (D) queer

5. Even though Jack said "Sorry!" to me in person, I did not feel any _____ in his apology.
(A) liability (B) generosity (C) integrity (D) sincerity

6. My grandfather has astonishing powers of _____. He can still vividly describe his first day at school as a child.
(A) resolve (B) fraction (C) privilege (D) recall

7. Recent research has found lots of evidence to _____ the drug company's claims about its "miracle" tablets for curing cancer.
(A) provoke (B) counter (C) expose (D) convert

8. Corrupt officials and misguided policies have _____ the country's economy and burdened its people with enormous foreign debts.
(A) crippled (B) accelerated (C) rendered (D) ventured

9. As a record number of fans showed up for the baseball final, the highways around the stadium were _____ with traffic all day.
(A) choked (B) disturbed (C) enclosed (D) injected

10. Studies show that the _____ unbiased media are in fact often deeply influenced by political ideology.
(A) undoubtedly (B) roughly (C) understandably (D) supposedly

二、綜合測驗（占10分）

說明：第11題至第20題為單選題，每題1分。

BONUS!!! 免費下載Fast2test CCFR-201b考試題庫的完整版：https://drive.google.com/open?id=15yLkIsXRAdBph_ttoNDkSVpmRnY9XgtJ

Fast2test擁有CrowdStrike CCFR-201b 認證考試的特殊培訓工具，能使你不用花費大量的時間和金錢就可以短時間獲得很多IT技術知識來提升你的技術，很快就能在IT行業中證明你的專業知識和技術。Fast2test的培訓課程是Fast2test的專家團隊利用自己的知識和經驗為CrowdStrike CCFR-201b 認證考試而研究出來的。

CrowdStrike CCFR-201b 考試大綱：

主題	簡介
主題 1	• 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.
主題 2	• Event Search: This domain focuses on performing advanced event searches from detections, refining searches using event actions, and distinguishing between commonly used event types.

主題 3	• Search Tools: This domain covers utilizing User Search, IP Search, Hash Search, Host Search, and Bulk Domain Search to gather intelligence during investigations.

>> CCFR-201b題庫 <<

CCFR-201b題庫和最新的CrowdStrike認證培訓 - CrowdStrike CrowdStrike Certified Falcon Responder

要在今日競爭的工作市場上成功，無論是尋找新的機會或是在您目前的職位上獲得升遷，都需要建立與展現您的技術專業和技能。CCFR-201b 認證能夠滿足考生在激烈的職場生涯中脫穎而出，衆多國際知名認證廠商都在招聘與 CrowdStrike 技能相關職位時首先看中 CCFR-201b 的認證證書，可見 CCFR-201b 認證的含金量很高。

最新的 CrowdStrike CCFR CCFR-201b 免費考試真題 (Q180-Q185):

問題 #180
During the configuration of a new IOA rule, the administrator must decide what action the sensor should take.
Which of the following is NOT a valid IOA rule action?

- A. Block
- B. No Action
- C. Monitor
- D. Kill Process

答案：B

問題 #181
A list of managed and unmanaged neighbors for an endpoint can be found:

- A. only by searching event data using Event Search
- B. under "Audit" by running Sensor Visibility Exclusions Audit
- C. by using Hosts page in the Investigate tool
- D. by reviewing "Groups" in Host Management under the Hosts page

答案：C

問題 #182
In the full detection tree view, icons provide visual cues about the telemetry. What does the specific icon representing a 'Falcon' (blue bird) indicate to the responder?

- A. The host is currently undergoing a remote live response session.
- B. There is related Intelligence (Intel) data available for this detection.
- C. The file has been successfully quarantined by the sensor.
- D. The process has been identified as a legitimate system file.

答案：B

問題 #183
A responder is focused on a specific malicious script and wants to see everything that the script's process did.
Which timeline is the best tool for this task?

- A. Host Timeline
- B. User Timeline
- C. Process Timeline

- D. Administrative Timeline

答案：C

問題 #184
The Falcon sensor can automatically upload quarantined files to the CrowdStrike Cloud for further analysis.
What is the maximum size allowed for a quarantined file to be uploaded?

- A. 128MB
- B. 10MB
- C. 32MB
- D. 64MB

答案：C

問題 #185
.....