

# ***KillTest***

높은 품질, 더 나은 서비스



## 연습 문제

<https://www.killtest.kr>

1년간 무료 업데이트 제공

**Exam : CCFR-201b**

**Title : CrowdStrike Certified  
Falcon Responder - 2024  
Version**

**Version : DEMO**

1.In the MITRE ATT&CK® framework, which of the following is a valid technique under the Credential Dumping category?

- A. Application Layer Protocol
- B. Acquire Credentials
- C. LSASS Memory
- D. Data from Information Repositories

**Answer: C**

2.Which FQL search parameter is used to filter events by a specific user account?

- A. UserName
- B. file\_hash
- C. process\_name
- D. event\_type

**Answer: A**

3.What role does machine learning play in detection analysis?

- A. It replaces human analysts completely
- B. It generates financial reports
- C. It improves the accuracy of threat detection
- D. It simplifies software installation

**Answer: C**

4.When executing a command within Falcon RTR, what is the expected behavior for long-running processes?

- A. They will timeout immediately
- B. They will continue running until the endpoint is rebooted
- C. They will be interrupted
- D. The command will run in the background

**Answer: D**

5.Which two exclusions can be configured to minimize false positives in Falcon detections? (Choose two)

- A. Sensor visibility exclusions
- B. DNS blocklists
- C. Machine learning exclusions
- D. IP allowlists

**Answer: AC**