DirectCertify

Unlock Your Potential, Certify Your Success

CrowdStrike

CCFR-201b Exam

CrowdStrike Falcon Responder

Exam Latest Version: 6.0

DEMO Version

Full Version Features:

• 90 Days Free Updates

• 30 Days Money Back Guarantee

• Instant Download Once Purchased

• 24 Hours Live Chat Support

Full version is available at link below with affordable price.

https://www.directcertify.com/crowdstrike/ccfr-201b

Question 1. (Single Select)

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

Correct Answer: C

Question 2. (Multi Select)

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

Correct Answer: A, C

Question 3. (Single Select)

What can the "File Hash" filter help you identify in Falcon Search?

A: File access times

B: Specific files associated with incidents
C: User activity history
D: Process execution order

Correct Answer: B

Question 4. (Single Select)

Which Falcon tool allows viewing multiple related processes in a table format?

A: View as Process Table
B: Host Timeline
C: Event Search Summary
D: File Activity Tracker

Correct Answer: A

Question 5. (Multi Select)

You're investigating suspicious behavior linked to a user.

Which key indicators should you examine in the User Search view to assess the threat context? (Choose two)

A: Number of failed login attempts
B: User’s IP subnet
C: Number of hosts the user has accessed
D: Number of detections associated with the user

Correct Answer: C, D

DirectCertify

Unlock Your Potential, Certify Your Success

Full version is available at link below with affordable price.

https://www.directcertify.com/crowdstrike/ccfr-201b

30% Discount Coupon Code: LimitedTime2025