

Boost up Your Certification Score

CrowdStrike

CCFA-200b

CrowdStrike Falcon Administrator



For More Information – Visit link below:

<https://www.examsboost.com/>

Product Version

- ✓ Up to Date products, reliable and verified.
- ✓ Questions and Answers in PDF Format.

Visit us at: <https://www.examsboost.com/test/ccfa-200b>

Latest Version: 6.1

Question: 1

Which use cases are appropriate for configuring a Falcon workflow?
(Choose two)

- A. Forwarding detection data to a SIEM system
- B. Updating endpoint hostnames
- C. Modifying policy priorities
- D. Alerting a SOC team when high-severity detections

Answer: A,D

Question: 2

Which benefits are provided by assigning endpoints to properly structured host groups?
(Choose two)

- A. Faster login performance
- B. Easier reporting and filtering
- C. Consistent policy enforcement
- D. Automatic malware removal

Answer: B,C

Question: 3

Which component of a prevention policy controls whether potentially unwanted programs (PUPs) are blocked or allowed?

- A. PUP handling
- B. Machine learning sensitivity
- C. Exploit protection
- D. Application control

Answer: A

Question: 4

To ensure rules apply globally across all endpoints in a customer account, administrators must enable _____ management in the General Settings.

- A. Regional
- B. CID-wide
- C. Device group
- D. Host-based

Answer: B

Question: 5

Which considerations should be made when applying a new prevention policy?
(Choose two)

- A. Restarting all endpoints
- B. Uninstalling existing sensors
- C. Policy testing on a pilot group
- D. Reviewing host group priorities

Answer: C,D

Question: 6

When creating a new user role in Falcon, which of the following permissions is required to enable the user to generate API keys?

- A. Activity App
- B. Hosts Management
- C. API Clients and Keys
- D. Real Time Response

Answer: C

Question: 7

Which Falcon platform features assist in locating hosts that may have Reduced Functionality Mode enabled?

(Choose two)

- A. Host Management filters using RFM

- B. Detection Summary Report
- C. Real Time Response session logs
- D. RFM column in Host Management table view

Answer: A,D

Question: 8

Which audit logs are available in the Falcon console for administrative and forensic tracking?
(Choose two)

- A. Sensor Kernel Log
- B. RTR Audit log
- C. Activity Audit Log
- D. Application Control Log

Answer: B,C

Question: 9

Which considerations should be made when applying a new prevention policy?
(Choose two)

- A. Policy testing on a pilot group
- B. Restarting all endpoints
- C. Uninstalling existing sensors
- D. Reviewing host group priorities

Answer: A,D

Question: 10

What does the "Sensor Operational" filter indicate when set in Host Management?

- A. Displays only active detections
- B. Shows only hosts not in RFM or inactive
- C. Groups sensors by policy
- D. Filters by sensor version

Answer: B

Thank You for Trying Our Product

For More Information – **Visit link below:**

<https://www.examsboost.com/>

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**



Visit us at: <https://www.examsboost.com/test/ccfa-200b>