TestHorse

Certified IT practice exam authority

Accurate study guides, High passing rate!
Testhorse provides update free of charge in one year!

http://www.testhorse.com

Exam: **CCFA-200**

Title: CrowdStrike Certified Falcon Administrator

Version: DEMO

1.An analyst has reported they are not receiving workflow triggered notifications in the past few days. Where should you first check for potential failures?
A. Custom Alert History
B. Workflow Execution log
C. Workflow Audit log
D. Falcon UI Audit Trail
Answer: B

2.How are user permissions set in Falcon?
A. Permissions are assigned to a User Group and then users are assigned to that group, thereby inheriting those permissions
B. Pre-defined permissions are assigned to sets called roles. Users can be assigned multiple roles based on job function and they assume a cumulative set of permissions based on those assignments
C. An administrator selects individual granular permissions from the Falcon Permissions List during user creation
D. Permissions are token-based. Users request access to a defined set of permissions and an administrator adds their token to the set of permissions
Answer: B

3.When creating new IOCs in IOC management, which of the following fields must be configured?
A. Hash, Description, Filename
B. Hash, Action and Expiry Date
C. Filename, Severity and Expiry Date
D. Hash, Platform and Action
Answer: D

4.Your organization has a set of servers that are not allowed to be accessed remotely, including via Real Time Response (RTR). You already have these servers in their own Falcon host group.
What is the next step to disable RTR only on these hosts?
A. Edit the Default Response Policy, toggle the "Real Time Response" switch off and assign the policy to the host group
B. Edit the Default Response Policy and add the host group to the exceptions list under "Real Time Functionality"
C. Create a new Response Policy, toggle the "Real Time Response" switch off and assign the policy to the host group
D. Create a new Response Policy and add the host name to the exceptions list under "Real Time Functionality"
Answer: C

5.Which exclusion pattern will prevent detections on a file at C:\Program Files\My Program\My Files\program.exe?
A. \Program Files\My Program\My Files*
B. \Program Files\My Program*
C. **

D. *\Program Files\My Program*\
Answer: A