CCFA-200 Q&As

CrowdStrike Certified Falcon Administrator

Pass CrowdStrike CCFA-200 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/ccfa-200.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CrowdStrike Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What type of information is found in the Linux Sensors Dashboard?

A. Hosts by Kernel Version, Shells spawned by Root, Wget/Curl Usage

B. Hidden File execution, Execution of file from the trash, Versions Running with Computer Names

C. Versions running, Directory Made Invisible to Spotlight, Logging/Auditing Referenced, Viewed, or Modified

D. Private Information Accessed, Archiving Tools ?Exfil, Files Made Executable

Correct Answer: C

QUESTION 2

When would the No Action option be assigned to a hash in IOC Management?

A. When you want to save the indicator for later action, but do not want to block or allow it at this time

B. Add the indicator to your allowlist and do not detect it

C. There is no such option as No Action available in the Falcon console

D. Add the indicator to your blocklist and show it as a detection

Correct Answer: A

QUESTION 3

What is the purpose of using groups with Sensor Update policies in CrowdStrike Falcon?

A. To group hosts with others in the same business unit

B. To group hosts according to the order in which Falcon was installed, so that updates are installed in the same order every time

C. To prioritize the order in which Falcon updates are installed, so that updates are not installed all at once leading to network congestion

D. To allow the controlled assignment of sensor versions onto specific hosts

Correct Answer: D

QUESTION 4

An administrator creating an exclusion is limited to applying a rule to how many groups of hosts?

A. File exclusions are not aligned to groups or hosts

B. There is a limit of three groups of hosts applied to any exclusion

C. There is no limit and exclusions can be applied to any or all groups

D. Each exclusion can be aligned to only one group of hosts

Correct Answer: B

QUESTION 5

What is the purpose of a containment policy?

A. To define which Falcon analysts can contain endpoints

B. To define the duration of Network Containment

C. To define the trigger under which a machine is put in Network Containment (e.g. a critical detection)

D. To define allowed IP addresses over which your hosts will communicate when contained

Correct Answer: C