CCFA-200$^{Q\&As}$

CrowdStrike Certified Falcon Administrator

QUESTION 1

The Falcon sensor uses certificate pinning to defend against man-in-the-middle attacks. Which statement is TRUE concerning Falcon sensor certificate validation?

A. SSL inspection should be configured to occur on all Falcon traffic

B. Some network configurations, such as deep packet inspection, interfere with certificate validation

C. HTTPS interception should be enabled to proceed with certificate validation

D. Common sources of interference with certificate pinning include protocol race conditions and resource contention

Correct Answer: B

QUESTION 2

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

Correct Answer: B

QUESTION 3

Which is the correct order for manually installing a Falcon Package on a macOS system?

A. Install the Falcon package, then register the Falcon Sensor via the registration package

B. Install the Falcon package, then register the Falcon Sensor via command line

C. Register the Falcon Sensor via command line, then install the Falcon package

D. Register the Falcon Sensor via the registration package, then install the Falcon package

Correct Answer: C

QUESTION 4

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

Correct Answer: D

QUESTION 5

Once an exclusion is saved, what can be edited in the future?

A. All parts of the exclusion can be changed

B. Only the selected groups and hosts to which the exclusion is applied can be changed

C. Only the options to "Detect/Block" and/or "File Extraction" can be changed

D. The exclusion pattern cannot be changed

Correct Answer: B