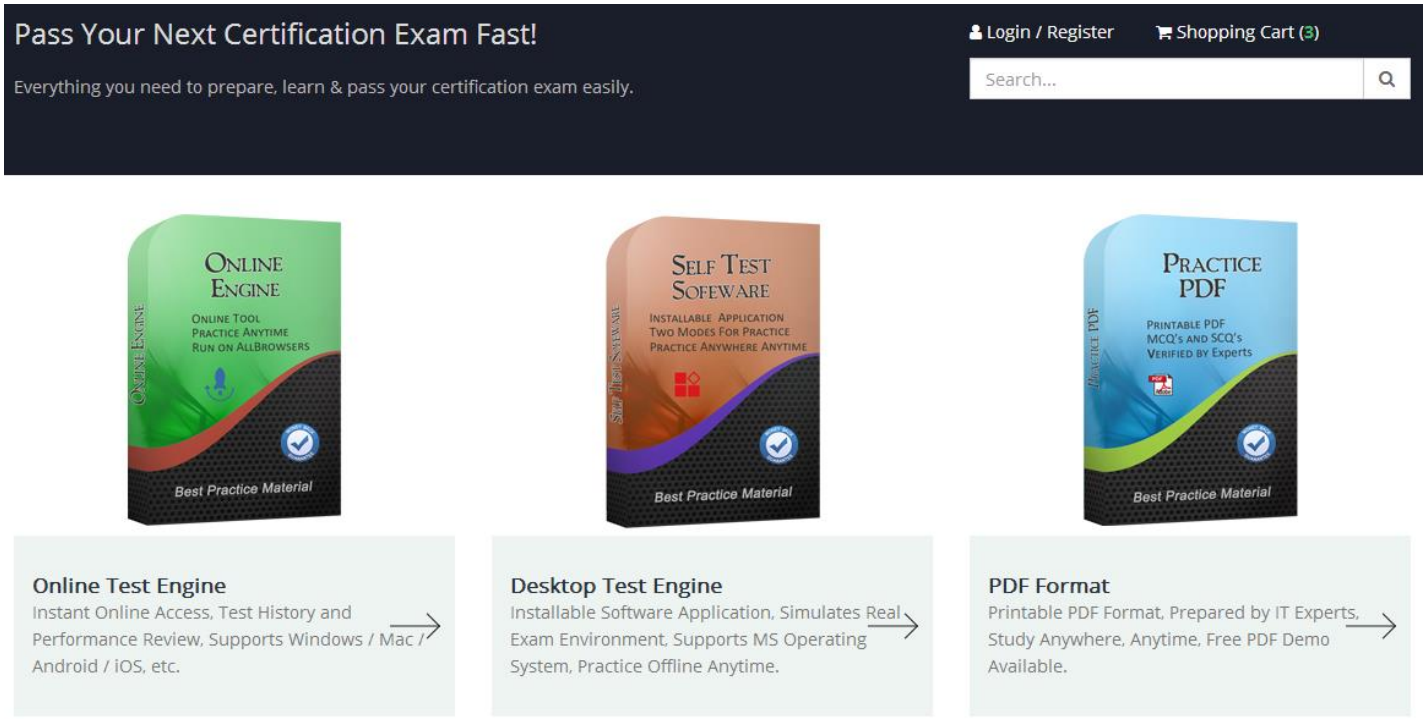
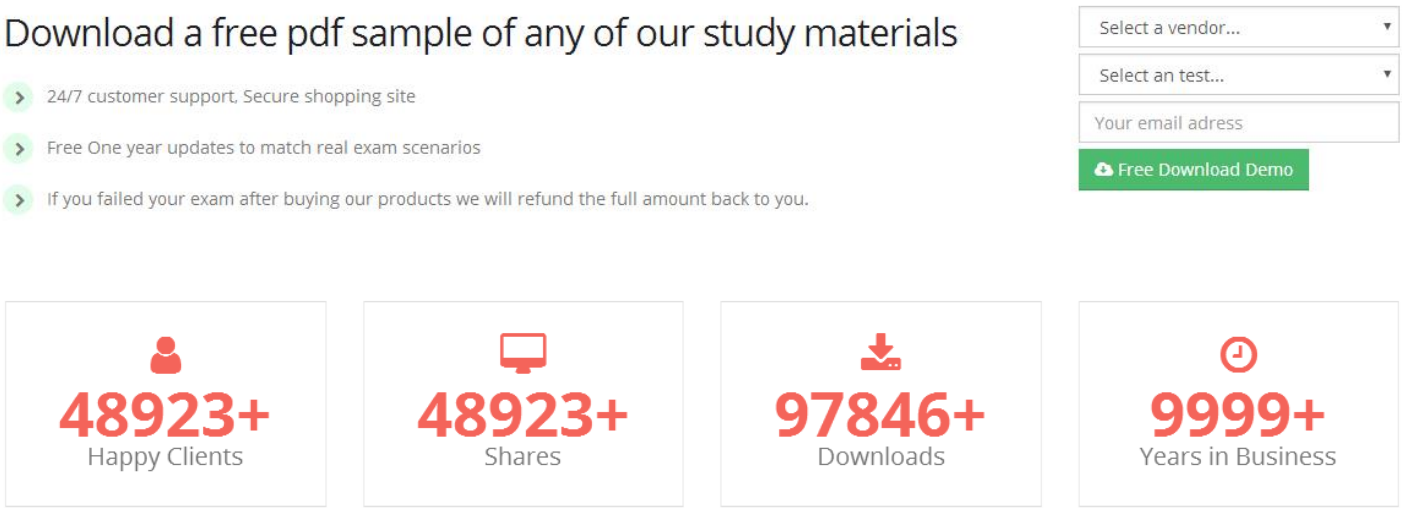
ExamcollectionPass





http://www.examcollectionpass.com/

Everything you need to prepare, learn & pass your certification exam easily.

Exam : **CCFA-200b**

Title : CrowdStrike Certified Falcon Administrator - 2024 Version

Vendor : CrowdStrike

Version : DEMO

NO.1 In order to prevent duplicate Agent IDs, what install parameter should be used on VMs to be used as persistent clones?

A. ProvNoWait=1

B. VDI=true

C. NO_START=1

D. VM=True

Answer: B

Explanation:

The correct parameter is VDI=true. In virtual desktop or cloned virtual machine scenarios, Falcon must avoid duplicate Agent IDs across clones. Persistent clone workflows require sensor installation to be performed with the correct VDI parameter so that each cloned endpoint registers properly and receives a unique identity.

ProvNoWait=1 is used for provisioning-timeout behavior and does not address duplicate Agent IDs.

NO_START=1 is used in some deployment contexts to delay sensor start but is not the VDI identity control.

VM=True is not the documented Falcon parameter. CCFA sensor deployment guidance treats VDI and golden-image preparation as a distinct deployment pattern because cloning a sensor incorrectly can duplicate identity and corrupt host tracking, policy assignment, and detection attribution.

NO.2 What prevention policy setting prevents sensor-related files, folders, and registry objects from being renamed or deleted?

A. Host Modification Protection

B. System Configuration Protection

C. Sensor Tampering Protection

D. Sensor Modification Protection

Answer: C

Explanation:

Sensor Tampering Protection is the prevention policy setting that blocks attempts to interfere with core Falcon sensor components. The official prevention policy guidance states that when this setting is enabled, it "blocks attempts to tamper with the sensor" and protects "sensor-related files, folders and registry objects from renaming or deletion." If disabled, Falcon may still create detections for tampering attempts, but it will not block the activity. This distinction is important because attackers commonly attempt to disable or corrupt endpoint security tooling before establishing persistence, evading detection, or executing payloads. Host Modification Protection, System Configuration Protection, and Sensor Modification Protection are not the named Falcon prevention setting for this control. The correct CCFA topic alignment is Policy Application, specifically Prevention Policy Settings > Sensor Capabilities > Sensor Tampering Protection.

NO.3 An inactive host that does not contact the Falcon cloud will be automatically removed from the Host Management and Trash pages after how many days?

A. 75 Days

B. 60 Days

C. 90 Days

D. 45 Days

Answer: D
Explanation:
The correct retention period is 45 days . In Falcon Host Management, a host becomes inactive when its sensor no longer sends heartbeat communication back to the CrowdStrike cloud. Inactive status is identified by the host's Last Seen timestamp, allowing administrators to determine when the endpoint last communicated.
Falcon automatically removes hosts that remain inactive for more than 45 days from both the Host Management page and the Trash page. This behavior prevents stale endpoint records from remaining indefinitely in the operational console while still giving administrators time to review, delete, restore, or investigate host records before they age out. The 60-day, 75-day, and 90-day options do not match the documented Falcon host lifecycle. This topic belongs to Host Management and Setup, specifically inactive host cleanup, deleted host handling, Trash retention, and endpoint lifecycle management.

NO.4 What page provides a count of new Reduced Functionality Mode (RFM) sensors by day?
A. Hosts Overview
B. Sensor Health
C. Activity Overview
D. Support and resources
Answer: B
Explanation:
The correct page is Sensor Health . The Sensor Health dashboard is designed to show Falcon sensor operational status across the environment and help administrators identify hosts running unsupported sensor versions, unsupported operating system versions, incorrect configurations, connectivity problems, and RFM conditions. The official guidance states that the Sensor Health dashboard includes information about "hosts that entered RFM each day" and clarifies that this shows hosts newly entering Reduced Functionality Mode, not the total number of hosts currently in RFM. This distinction matters because Sensor Health is used to track newly emerging sensor health issues over time, while Host Management can be used to filter for the current list of hosts in RFM. Hosts Overview and Activity Overview do not provide this specific daily RFM count. Support and resources is a navigation area, not the sensor health reporting dashboard. Reference topics: Dashboards and Reports, Sensor Health Dashboard, Reduced Functionality Mode, Sensor Operational Status.

NO.5 What type of information is provided in sensor health report?
A. User login history
B. Local performance metrics
C. Current operational status
D. Network traffic patterns
Answer: C
Explanation:
Sensor health reporting provides current operational status of sensors. Its purpose is to help administrators identify whether sensors are online, offline, in reduced functionality, properly reporting, or otherwise in a state requiring attention. User login history belongs to account or identity-related telemetry, not sensor health.
Local performance metrics may be relevant during troubleshooting but are not the primary sensor

health report objective. Network traffic patterns are investigated through event search, network telemetry, or other dashboards, not basic sensor health. CCFA dashboards and reports topics emphasize using sensor health and sensor reports to monitor deployment status, operational readiness, sensor connectivity, and coverage across the environment so that administrators can quickly locate hosts requiring remediation.

NO.6 What are the three required parts of a Fusion SOAR workflow condition?

A. Operator, value, and source

B. Alert, action, and schedule

C. Trigger, parameter, and alert

D. Parameter, operator, and value

Answer: D

Explanation:

A Fusion SOAR workflow condition is built from a parameter , an operator , and a value . The parameter is the field being evaluated, such as severity, hostname, platform, status, or detection type. The operator defines the comparison, such as equals, contains, is in, or is greater than. The value is the target value used in the comparison. This structure allows a workflow to start from a broad event trigger and then narrow execution to only the events that match the desired criteria. Alert, action, schedule, trigger, and source are workflow concepts, but they are not the three required components of a condition. The CCFA workflow model uses conditions to refine and control automation safely.

NO.7 What is true about the Default Sensor Policy?

A. It tests the sensor configuration settings before deployment

B. It is applied automatically if no other Sensor Policies are applied

C. It can be used to reset all sensor settings to Default

D. It is a mechanism to deploy the oldest supported version of the Falcon Sensor

Answer: B

Explanation:

The Default Sensor Policy is the fallback policy that applies when a host is not matched to another assigned sensor policy. Falcon policy assignment is driven by host group membership and policy precedence. If a host belongs to a group that has an assigned policy, Falcon applies the highest-precedence applicable policy. If the host is not part of any group, or if its groups do not have a policy assigned, Falcon automatically applies the default policy. This ensures every sensor has an update policy path and avoids unmanaged update behavior.

The default policy is not a test mechanism, does not reset all settings, and is not intended to deploy the oldest supported sensor version. The course guide states that the default policy may appear as platform_default and is applied to hosts that do not have an assigned policy. Reference topics: Sensor Deployment, Sensor Update Policies, Default Policy, Host Group Policy Assignment.

NO.8 What update policy does a sensor receive when it does not have a group assignment?

A. Top precedence policy

B. Default policy

C. Auto N-1 policy

Answer: B

Explanation:
A sensor with no applicable custom host group assignment receives the Default policy . Sensor update policies follow the same basic host group and precedence pattern used throughout Falcon policy management.
If a host is included in a group assigned to a higher-precedence sensor update policy, that policy applies. If it does not match any assigned custom policy, Falcon falls back to the default sensor update policy. The top- precedence policy only applies when the host belongs to a host group assigned to that policy. Auto N-1 is a possible version-selection strategy within a policy, not the automatic fallback policy assignment. This is why the course emphasizes reviewing default policy settings carefully before broad deployment.

NO.9 What prevention policy settings must be enabled to quarantine files on the host?

A. Quarantine Files; Windows Anti-Malware Execution Blocking

B. Malware Protection; Custom Execution Blocking

C. Next-Gen Antivirus Prevention sliders; Quarantine & Security Center Registration

D. Advanced Remediation Actions; Quarantine level set to Aggressive

Answer: C

Explanation:
To quarantine files, Falcon requires the relevant Next-Gen Antivirus prevention capability and the quarantine setting. The correct pairing is Next-Gen Antivirus Prevention sliders with Quarantine & Security Center Registration . Quarantine does not operate independently; Falcon must first prevent the file through NGAV- related controls such as cloud or sensor machine-learning prevention. Once prevention occurs, the quarantine setting governs whether the prevented executable is quarantined on the host. Custom Execution Blocking is related to IOC-based blocking, not the general NGAV quarantine requirement. "Advanced Remediation Actions" and an "Aggressive quarantine level" are not the documented configuration pair. The course guide identifies quarantine under Next-Gen Antivirus and ties it to prevention-level configuration and Security Center registration.

NO.10 Your organization has determined that your cybersecurity architect needs to be notified via email whenever Falcon generates detections of a medium severity or higher. Additionally, the architect should be notified about any incidents with a CrowdScore of 1.0 or higher. What can the Falcon Administrator do to ensure the architect is properly alerted?

A. Create a new Falcon user for the architect then create and assign a custom Falcon user role so they are automatically notified for the new detections and emails

B. Create a custom Fusion SOAR workflow to send an email every time a new detection or incident is created

C. Add the architect's email address to the manage list for detection and incident emails from the General settings menu

D. Create a new Falcon user for the architect and assign the Detections and Exceptions Manager role so they are automatically notified for the new detections and incidents

Answer: C

Explanation:
The correct administrative action is to add the architect's email address to the managed recipient list for standard incident and detection notification emails in General settings. Falcon standard notification behavior already matches the stated requirement: CrowdStrike sends email notifications

for detections with severity of medium or higher and sends incident notifications when a new incident reaches a CrowdScore of 1.0 or higher. The recipient list is managed from Support and resources > Resource and tools > General settings under "Manage list for detection and incident emails." Creating a Falcon user or assigning a custom role does not automatically subscribe the architect to these standard email notifications. A Fusion SOAR workflow could send email, but it is unnecessary because the native notification mechanism already exists and is designed for this use case. The Detections and Exceptions Manager role controls exception management, not notification enrollment. CCFA reference topics: Falcon Notifications, General Settings, Standard Incident and Detection Notification Emails, Dashboards and Reports.