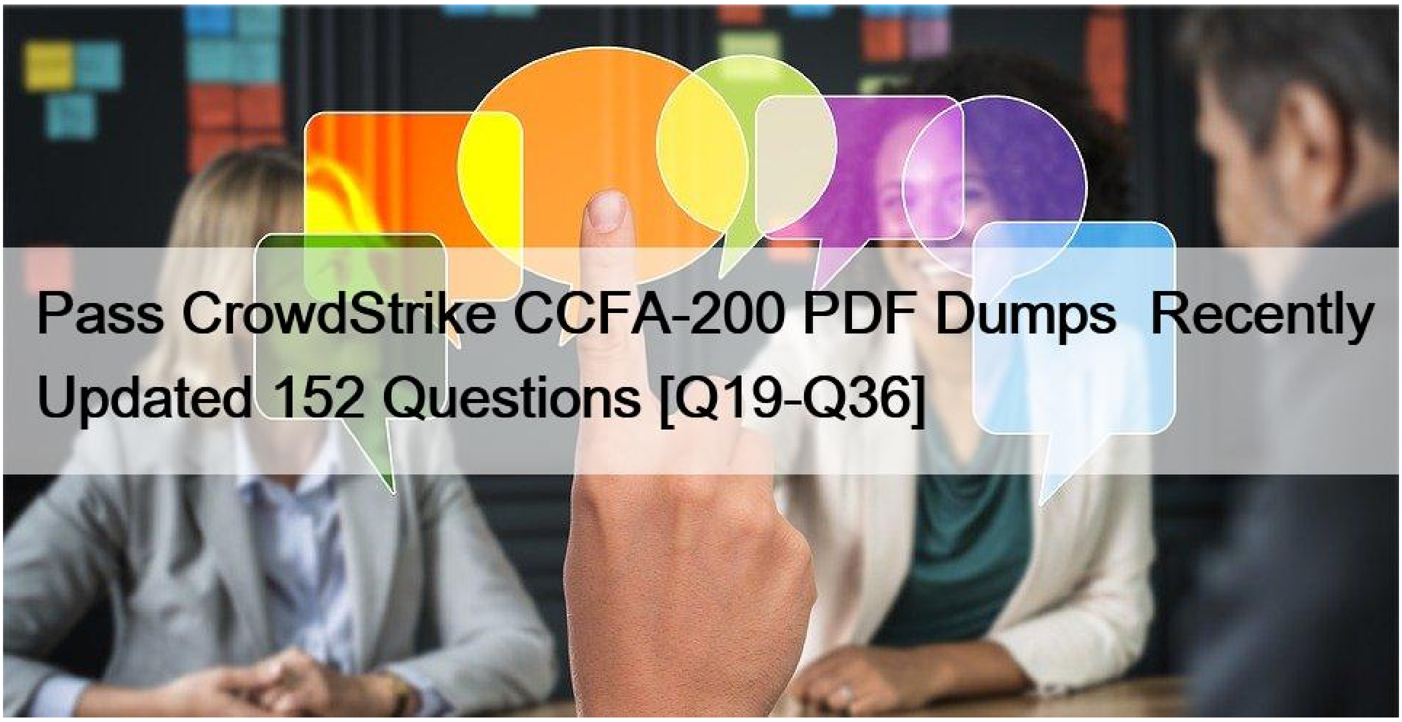
Pass CrowdStrike CCFA-200 PDF Dumps Recently Updated 152 Questions [Q19-Q36



Pass CrowdStrike CCFA-200 PDF Dumps | Recently Updated 152 Questions
Updated Test Engine to Practice CCFA-200 Dumps & Practice Exam

The CCFA-200 exam is a valuable certification for cybersecurity professionals who are looking to advance their careers. It demonstrates the candidate's expertise in one of the leading endpoint protection platforms and provides a competitive advantage in the job market. CrowdStrike Certified Falcon Administrator certification also provides access to CrowdStrike's community of certified professionals, which offers networking opportunities and access to exclusive resources.

CrowdStrike CCFA-200 (CrowdStrike Certified Falcon Administrator) Certification Exam is a rigorous certification program that is designed to test the knowledge and skills of IT professionals in the field of cybersecurity. CrowdStrike Certified Falcon Administrator certification is aimed at individuals who are responsible for the administration and management of the CrowdStrike Falcon platform, which is a cloud-based endpoint protection solution that provides advanced threat protection to organizations of all sizes.

QUESTION 19

When the Notify End Users policy setting is turned on, which of the following is TRUE?
* End users will not be notified as we would not want to notify a malicious actor of a detection. This setting does not exist
* End users will be immediately notified via a pop-up that their machine is in-network isolation
* End-users receive a pop-up notification when a prevention action occurs

* End users will receive a pop-up allowing them to confirm or refuse a pending quarantine

QUESTION 20

The Falcon sensor uses certificate pinning to defend against man-in-the-middle attacks. Which statement is TRUE concerning Falcon sensor certificate validation?
* SSL inspection should be configured to occur on all Falcon traffic
* Some network configurations, such as deep packet inspection, interfere with certificate validation
* HTTPS interception should be enabled to proceed with certificate validation
* Common sources of interference with certificate pinning include protocol race conditions and resource contention
Explanation

The statement that some network configurations, such as deep packet inspection, interfere with certificate validation is true concerning Falcon sensor certificate validation. The Falcon sensor uses certificate pinning to defend against man-in-the-middle attacks, which means that it verifies that the server certificate presented by the Falcon cloud matches a hard-coded certificate embedded in the sensor. Some network configurations, such as deep packet inspection, SSL inspection, or HTTPS interception, may attempt to modify or replace the server certificate, which will cause the sensor to reject the connection and generate an error3.

References: 3: How to Become a CrowdStrike Certified Falcon Administrator

QUESTION 21

What should be disabled on firewalls so that the sensor&#8217;s man-in-the-middle attack protection works properly?
* Deep packet inspection
* Linux Sub-System
* PowerShell
* Windows Proxy
Explanation

The option that should be disabled on firewalls so that the sensor&#8217;s man-in-the-middle attack protection works properly is deep packet inspection. Deep packet inspection is a network configuration that inspects and modifies the data packets that pass through a firewall. Deep packet inspection may interfere with the sensor&#8217;s certificate validation, which is a feature that verifies that the server certificate presented by the Falcon cloud matches a hard-coded certificate embedded in the sensor. If the certificate validation fails, the sensor will reject the connection and generate an error3.

References: 3: How to Become a CrowdStrike Certified Falcon Administrator

QUESTION 22

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

QUESTION 23

Which of the following applies to Custom Blocking Prevention Policy settings?
* Hashes must be entered on the Prevention Hashes page before they can be blocked via this policy

* Blocklisting applies to hashes, IP addresses, and domains
* Executions blocked via hash blocklist may have partially executed prior to hash calculation process remediation may be necessary
* You can only blocklist hashes via the API

QUESTION 24

Which port and protocol does the sensor use to communicate with the CrowdStrike Cloud?
* TCP port 22 (SSH)
* TCP port 443 (HTTPS)
* TCP port 80 (HTTP)
* TCP UDP port 53 (DNS)
Explanation

The sensor uses TCP port 443 (HTTPS) to communicate with the CrowdStrike Cloud. This port and protocol are used to securely send and receive data between the sensor and the cloud, such as detections, policies, updates, commands, etc. The other options are either incorrect or not used by the sensor.

Reference: CrowdStrike Falcon User Guide, page 28.

QUESTION 25

Under which scenario can Sensor Tags be assigned?
* While triaging a detection
* While managing hosts in the Falcon console
* While updating a sensor in the Falcon console
* While installing a sensor

QUESTION 26

What will happen to a host if it is not assigned a Sensor Update policy?
* The host will uninstall the Sensor and provide an alert to the installation team
* The host will automatically update to the newest sensor version and auto-update to future release
* The host will automatically create a custom Sensor Update policy
* The host will use the Default Sensor Update policy
Explanation

The option that describes what will happen to a host if it is not assigned a Sensor Update policy is that the host will use the Default Sensor Update policy. A Sensor Update policy is a policy that controls how and when the Falcon sensor is updated on a host. You can create and assign custom Sensor Update policies to different hosts or groups in your environment. However, if a host is not assigned to a specific Sensor Update policy, it will inherit the settings from the Default Sensor Update policy. The Default Sensor Update policy is a &#8220;catch-all&#8221; policy that is enabled by default and has the &#8220;Uninstall and Maintenance Protection&#8221; feature turned on. You can modify the settings of the Default Sensor Update policy, but you cannot delete or disable it1.

References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 27

How can you find a list of hosts that have not communicated with the CrowdStrike Cloud in the last 30 days?
* Under Dashboards and reports, choose the Sensor Report. Set the &#8220;Last Seen&#8221; dropdown to 30 days and reference

the Inactive Sensors widget

* Under Host setup and management, choose the Host Management page. Set the group filter to &#8220;Inactive Sensors&#8221;
* Under Host setup and management > Managed endpoints > Inactive Sensors. Change the time range to 30 days
* Under Host setup and management, choose the Disabled Sensors Report. Change the time range to 30 days

QUESTION 28

Which role will allow someone to manage quarantine files?

* Falcon Security Lead
* Detections Exceptions Manager
* Falcon Analyst &#8211; Read Only
* Endpoint Manager

QUESTION 29

Why do Sensor Update policies need to be configured for each OS (Windows, Mac, Linux)?

* To bundle the Sensor and Prevention policies together into a deployment package
* Sensor Update policies are OS dependent
* To assist with auditing and change management
* This is false. One policy can be applied to all Operating Systems

Explanation

Sensor Update policies need to be configured for each OS (Windows, Mac, Linux) because Sensor Update policies are OS dependent. A Sensor Update policy is a policy that controls how and when the Falcon sensor is updated on a host. Sensor Update policies are specific to each operating system type, as different operating systems have different sensor versions, features, and requirements. Therefore, you need to create and assign separate Sensor Update policies for each operating system type in your environment1.

References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 30

Where can you modify settings to permit certain traffic during a containment period?

* Prevention Policy
* Host Settings
* Containment Policy
* Firewall Settings

Explanation

The administrator can modify settings to permit certain traffic during a containment period by creating or editing a Containment Policy. This policy allows users to specify which ports, protocols and IP addresses are allowed or blocked during network containment. The other options are either incorrect or not related to network containment. Reference: [CrowdStrike Falcon User Guide], page 40.

QUESTION 31

Why is it critical to have separate sensor update policies for Windows/Mac/*nix?

* There may be special considerations for each OS
* To assist with testing and tracking sensor rollouts
* The network protocols are different for each host OS

* It is an auditing requirement

QUESTION 32

The Logon Activities Report includes all of the following information for a particular user EXCEPT __________.
* the account type for the user (e.g. Domain Administrator, Local User)
* all hosts the user logged into
* the logon type (e.g. interactive, service)
* the last time the user&#8217;s password was set

QUESTION 33

You have created a Sensor Update Policy for the Mac platform. Which other operating system(s) will this policy manage?
* *nix
* Windows
* Both Windows and *nix
* Only Mac

QUESTION 34

What best describes what happens to detections in the console after clicking &#8220;Enable Detections&#8221; for a host which previously had its detections disabled?
* Enables custom detections for the host
* New detections will start appearing in the console, and all retroactive stored detections will be restored to the console for that host
* New detections will start appearing in the console immediately. Previous detections will not be restored to the console for that host
* Preventions will be enabled for the host
Explanation

The option that best describes what happens to detections in the console after clicking &#8220;Enable Detections&#8221; for a host which previously had its detections disabled is that new detections will start appearing in the console immediately. Previous detections will not be restored to the console for that host. The &#8220;Enable Detections&#8221; feature allows you to enable or disable the detection and prevention capabilities of the Falcon sensor on a specific host. When you disable detections for a host, the sensor will stop sending any detection or prevention events to the Falcon console, and any existing events for that host will be removed from the console. When you enable detections for a host, the sensor will resume sending any new detection or prevention events to the Falcon console, but any previous events for that host will not be restored to the console1.

References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 35

When creating new IOCs in IOC management, which of the following fields must be configured?
* Hash, Description, Filename
* Hash, Action and Expiry Date
* Filename, Severity and Expiry Date
* Hash, Platform and Action

QUESTION 36

With Custom Alerts, it is possible to __________.

* schedule the alert to run at any interval
* receive an alert in an email
* configure prevention actions for alerting
* be alerted to activity in real-time

CrowdStrike CCFA-200 Dumps Cover Real Exam Questions: https://www.vceprep.com/CCFA-200-latest-vce-prep.html]