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

Where in the Falcon console can information about supported operating system versions be found?

A. Configuration module

B. Intelligence module

C. Support module

D. Discover module

Correct Answer: C

Information about supported operating system versions can be found in the Support module in the Falcon console. This module provides access to various support resources, such as documentation, downloads, FAQs, release notes and system status. One of the documents available in this module is the CrowdStrike Sensor Compatibility List, which lists the supported operating system versions for each sensor type and platform. The other options are either incorrect or not related to finding information about supported operating system versions. Reference: CrowdStrike Falcon User Guide, page 26.

QUESTION 2

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

A. To bundle the Sensor and Prevention policies together into a deployment package

B. Sensor Update policies are OS dependent

C. To assist with auditing and change management

D. This is false. One policy can be applied to all Operating Systems

Correct Answer: B

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 3

After agent installation, an agent opens a permanent___connection over port 443 and keeps that connection open until the endpoint is turned off or the network connection is terminated.

A. SSH

B. TLS

C. HTTP

D. TCP

Correct Answer: B

After agent installation, an agent opens a permanent TLS connection over port 443 and keeps that connection open until the endpoint is turned off or the network connection is terminated. TLS (Transport Layer Security) is a protocol that

provides secure and encrypted communication between the agent and the Falcon cloud. Port 443 is the standard port for HTTPS (Hypertext Transfer Protocol Secure) traffic. The agent uses this connection to send and receive data,

commands, policies, and updates from the Falcon cloud2.

References: 2: Cybersecurity Resources | CrowdStrike

QUESTION 4

Which of the following is a valid step when troubleshooting sensor installation failure?

A. Confirm all required services are running on the system

B. Enable the Windows firewall

C. Disable SSL and TLS on the host

D. Delete any available application crash log files

Correct Answer: A

A valid step when troubleshooting sensor installation failure is to confirm all required services are running on the system. This can help identify if there are any issues with the sensor service, the Windows Management Instrumentation service, or the Windows Remote Management service, which are required for the sensor to function properly. The other options are either incorrect or not helpful for troubleshooting sensor installation failure. Reference: CrowdStrike Falcon User Guide, page 29.

QUESTION 5

When creating a Host Group for all Workstations in an environment, what is the best method to ensure all workstation hosts are added to the group?

A. Create a Dynamic Group with Type=Workstation Assignment

B. Create a Dynamic Group and Import All Workstations

C. Create a Static Group and Import all Workstations

D. Create a Static Group with Type=Workstation Assignment

Correct Answer: A

The best method to ensure all workstation hosts are added to the group is to create a Dynamic Group with Type=Workstation Assignment. A Dynamic Group is a group that automatically updates its membership based on certain criteria or filters. A Type=Workstation Assignment filter will match all hosts that have the workstation type assigned in their Active Directory domain. This way, any new or existing workstation hosts will be added to the group without manual intervention1. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 6

How do you disable all detections for a host?

A. Create an exclusion rule and apply it to the machine or group of machines

B. Contact support and provide them with the Agent ID (AID) for the machine and they will put it on the Disabled Hosts list in your Customer ID (CID)

C. You cannot disable all detections on individual hosts as it would put them at risk

D. In Host Management, select the host and then choose the option to Disable Detections

Correct Answer: D

The administrator can disable all detections for a host by selecting the host and then choosing the option to Disable Detections in the Host Management page. This will prevent the host from sending any detection events to the Falcon Cloud. The other options are either incorrect or not available. Reference: [CrowdStrike Falcon User Guide], page 32.

QUESTION 7

What can the Quarantine Manager role do?

A. Manage and change prevention settings

B. Manage quarantined files to release and download

C. Manage detection settings

D. Manage roles and users

Correct Answer: B

The Quarantine Manager role can manage quarantined files to release and download. This role allows users to view and search quarantined files, as well as release them from quarantine or download them for further analysis. The other roles do not have this capability. Reference: [CrowdStrike Falcon User Guide], page 19.

QUESTION 8

You have determined that you have numerous Machine Learning detections in your environment that are false positives. They are caused by a single binary that was custom written by a vendor for you and that binary is running on many endpoints. What is the best way to prevent these in the future?

A. Contact support and request that they modify the Machine Learning settings to no longer include this detection

B. Using IOC Management, add the hash of the binary in question and set the action to "Allow"

C. Using IOC Management, add the hash of the binary in question and set the action to "Block, hide detection"

D. Using IOC Management, add the hash of the binary in question and set the action to "No Action"

Correct Answer: B

to match any number of characters including none while not matching beyond path separators (\ or /) and double asterisks are used to recursively match zero or more directories that fall under the current directory.

QUESTION 9

When editing an existing IOA exclusion, what can NOT be edited?

A. The IOA name

B. All parts of the exclusion can be changed

C. The exclusion name

D. The hosts groups

Correct Answer: A

When editing an existing IOA exclusion, the IOA name cannot be edited. An IOA (indicator of attack) exclusion allows you to define custom rules for excluding suspicious behavior from detection or prevention based on process execution, file write, network connection, or registry events. The IOA name is a predefined name that identifies the type of IOA behavior that you want to exclude, such as "Suspicious Process Execution

- Script Interpreter Executing File". The IOA name cannot be changed when editing an existing IOA exclusion, as it is linked to a specific IOA rule in the Falcon platform. However, you can edit other parts of the IOA exclusion, such as the exclusion name, the hosts groups, and the filter criteria2. References: 2: Cybersecurity Resources | CrowdStrike

QUESTION 10

Which of the follow should be used with extreme caution because it may introduce additional security risks such as malware or other attacks which would not be recorded, detected, or prevented based on the exclusion syntax?

A. Sensor Visibility Exclusion

B. Machine Learning Exclusions

C. IOC Exclusions

D. IOA Exclusions

Correct Answer: D

The option that should be used with extreme caution because it may introduce additional security risks such as malware or other attacks which would not be recorded, detected, or prevented based on the exclusion syntax is IOA Exclusions.

An IOA (indicator of attack) exclusion allows you to define custom rules for excluding suspicious behavior from detection or prevention based on process execution, file write, network connection, or registry events. However, using IOA exclusions may reduce the visibility and protection of the Falcon sensor, as it may allow malicious activity to bypass the sensor\\'s detection and prevention capabilities. Therefore, you should use IOA exclusions with extreme caution and only when necessary2. References: 2: Cybersecurity Resources | CrowdStrike

QUESTION 11

When performing targeted filtering for a host on the Host Management Page, which filter bar attribute is NOT case-sensitive?

A. Username

B. Model

C. Domain

D. Hostname

Correct Answer: D

When performing targeted filtering for a host on the Host Management Page, the filter bar attribute that is not case-sensitive is Hostname. The Hostname attribute allows you to filter hosts by their computer name or DNS name. The Hostname filter is not case- sensitive, meaning that it will match hosts regardless of the capitalization of their names. For example, filtering by hostname=DESKTOP-1234 will match hosts with names such as DESKTOP-1234, desktop-1234, or Desktop12342. References: 2: Cybersecurity Resources | CrowdStrike

QUESTION 12

Which of the following scenarios best describes when you would add IP addresses to the containment policy?

A. You want to automate the Network Containment process based on the IP address of a host

B. Your organization has additional IP addresses that need to be able to access the Falcon console

C. A new group of analysts need to be able to place hosts under Network Containment

D. Your organization has resources that need to be accessible when hosts are network contained

Correct Answer: D

The scenario that best describes when you would add IP addresses to the containment policy is that your organization has resources that need to be accessible when hosts are network contained. As explained in the previous question,

adding IP addresses to the containment policy allows you to create an allowlist of trusted IP addresses that can communicate with your contained hosts. This can be useful when you need to isolate a host from the network due to a potential

compromise or investigation, but still want to allow it to access certain resources or services that are essential for your organization\\'s operations or security2.

References: 2: Cybersecurity Resources | CrowdStrike

QUESTION 13

What is the goal of a Network Containment Policy?

A. Increase the aggressiveness of the assigned prevention policy

B. Limit the impact of a compromised host on the network

C. Gain more visibility into network activities

D. Partition a network for privacy

Correct Answer: B

The goal of a Network Containment Policy is to limit the impact of a compromised host on the network. This policy allows users to isolate a host from the network, while still allowing it to communicate with the Falcon Cloud and other essential

services. This can help prevent further damage or data exfiltration from a compromised host. The other options are either incorrect or not related to the policy. Reference:

[CrowdStrike Falcon User Guide], page 40.

QUESTION 14

What is the purpose of the Machine-Learning Prevention Monitoring Report?

A. It is designed to give an administrator a quick overview of machine-learning aggressiveness settings as well as the numbers of items actually quarantined

B. It is the dashboard used by an analyst to view all items quarantined and to release any items deemed non-malicious

C. It is the dashboard used to see machine-learning preventions, and it is used to identify spikes in activity and possible targeted attacks

D. It is designed to show malware that would have been blocked in your environment based on different Machine-Learning Prevention settings

Correct Answer: D

Machine-Learning Prevention Monitoring dashboard: Use this dashboard to view malware that would have been blocked in your environment over the selected timeframe based on different Machine Learning Prevention settings (Cautious, Moderate, Aggressive or Extra Aggressive).

QUESTION 15

Which role is required to manage groups and policies in Falcon?

A. Falcon Host Analyst

B. Falcon Host Administrator

C. Prevention Hashes Manager

D. Falcon Host Security Lead

Correct Answer: B

The Falcon Host Administrator role is required to manage groups and policies in Falcon. This role allows users to create, edit and delete groups and policies, as well as assign them to hosts. The other roles do not have this capability.

Reference:

[CrowdStrike Falcon User Guide], page 17.