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.geekcert.com/ccfa-200.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You are beginning the rollout of the Falcon Sensor for the first time side-by-side with your existing security solution. You need to configure the Machine Learning levels of the Prevention Policy so it does not interfere with existing solutions

during the testing phase.

What settings do you choose?

A. Detection slider: Extra Aggressive Prevention slider: Cautious

B. Detection slider: Moderate Prevention slider: Disabled

C. Detection slider: Cautious Prevention slider: Cautious

D. Detection slider: Disabled Prevention slider: Disabled

Correct Answer: C

The best settings to configure the Machine Learning levels of the Prevention Policy so it does not interfere with existing solutions during the testing phase are Cautious for both Detection and Prevention sliders. This setting will enable the sensor to detect and prevent only high-confidence malicious events, while allowing low-confidence events to run without interference. This setting will also generate less noise and false positives than higher settings, such as Moderate or Extra Aggressive1. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 2

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: A

The type of information that is found in the Linux Sensors Dashboard is Hosts by Kernel Version, Shells spawned by Root, Wget/Curl Usage. The Linux Sensors Dashboard is a dashboard that provides an overview of the Linux hosts in your environment that have Falcon sensors installed. You can use this dashboard to monitor the health and activity of your Linux hosts, such as their kernel versions, root shell usage, network communication, detections, and preventions. References: How to Become a CrowdStrike Certified Falcon Administrator

QUESTION 3

You want to create a detection-only policy. How do you set this up in your policy\\'s settings?

A. Enable the detection sliders and disable the prevention sliders. Then ensure that Next Gen Antivirus is enabled so it will disable Windows Defender.

B. Select the "Detect-Only" template. Disable hash blocking and exclusions.

C. You can\\'t create a policy that detects but does not prevent. Use Custom IOA rules to detect.

D. Set the Next-Gen Antivirus detection settings to the desired detection level and all the prevention sliders to disabled. Do not activate any of the other blocking or malware prevention options.

Correct Answer: D

The administrator can create a detection-only policy by setting the Next-Gen Antivirus detection settings to the desired detection level and all the prevention sliders to disabled in the policy\\'s settings. This will allow Falcon to detect but not prevent threats on the hosts using this policy. Do not activate any of the other blocking or malware prevention options, as they will enable prevention actions. The other options are either incorrect or not related to creating a detection-only policy. Reference: [CrowdStrike Falcon User Guide], page 35.

QUESTION 4

While a host is Network contained, you need to allow the host to access internal network resources on specific IP addresses to perform patching and remediation. Which configuration would you choose?

A. Configure a Real Time Response policy allowlist with the specific IP addresses

B. Configure a Containment Policy with the specific IP addresses

C. Configure a Containment Policy with the entire internal IP CIDR block

D. Configure the Host firewall to allowlist the specific IP addresses

Correct Answer: B

While a host is Network contained, the administrator can allow the host to access internal network resources on specific IP addresses to perform patching and remediation by configuring a Containment Policy with the specific IP addresses. 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 5

What must an admin do to reset a user\\'s password?

A. From User Management, open the account details for the affected user and select "Generate New Password"

B. From User Management, select "Reset Password" from the three dot menu for the affected user account

C. From User Management, select "Update Account" and manually create a new password for the affected user account

D. From User Management, the administrator must rebuild the account as the certificate for user specific private/public key generation is no longer valid

Correct Answer: B

The administrator can reset a user\\'s password by selecting "Reset Password" from the three dot menu for the affected user account in the User Management page. This will generate a new password and send it to the user\\'s email address. The other options are either incorrect or not available. Reference: CrowdStrike Falcon User Guide, page 25.