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

CrowdStrike Certified Falcon Administrator

Pass CrowdStrike CCFA-200 Exam with 100% Guarantee

QUESTION 1

What may prevent a user from logging into Falcon via single sign-on (SSO)?

A. The SSO username doesn\\'t match their email address in Falcon

B. The maintenance token has expired

C. Falcon is in reduced functionality mode

D. The user never configured their security questions

Correct Answer: A

The option that may prevent a user from logging into Falcon via single sign- on (SSO) is that the SSO username doesn\\'t match their email address in Falcon. SSO is a feature that allows you to use an external identity provider (IdP) to

authenticate and authorize users to access the Falcon platform. SSO simplifies and streamlines the login process, as users only need to remember one set of credentials for multiple applications. However, SSO requires that the username in

the IdP matches the email address in Falcon for each user. If there is a mismatch between the username and the email address, the user will not be able to log into Falcon via SSO.

References: : [Cybersecurity Resources | CrowdStrike]

QUESTION 2

What is likely the reason your Windows host would be in Reduced Functionality Mode (RFM)?

A. Microsoft updates altering the kernel

B. The host lost internet connectivity

C. A misconfiguration in your prevention policy for the host

D. A Sensor Update Policy was misconfigured

Correct Answer: B

The likely reason your Windows host would be in Reduced Functionality Mode (RFM) is that the host lost internet connectivity. RFM is a mode that limits the sensor\\'s functionality due to license expiration, network connectivity loss, or certificate validation failure. When a Windows sensor is in RFM, it will only provide basic prevention capabilities, such as blocking known malware hashes and preventing script execution from the %TEMP% directory. The sensor will not send any telemetry or detection events to the Falcon platform, and will not receive any policy or update changes from the Falcon cloud1. Losing internet connectivity is a common cause of RFM, as it prevents the sensor from communicating with the Falcon cloud. A misconfiguration in your prevention policy or sensor update policy will not cause RFM, as these policies are applied by the Falcon cloud and do not affect the sensor\\'s license, network, or certificate status. Microsoft updates altering the kernel may cause compatibility issues with the sensor, but not RFM3. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike 3: How to Become a CrowdStrike Certified Falcon Administrator

QUESTION 3

What best describes what happens to detections in the console after clicking "Disable Detections" for a host from within the Host Management page?

A. The detections for the host are removed from the console immediately and no new detections will display in the console going forward

B. You cannot disable detections for a host

C. Existing detections for the host remain, but no new detections will display in the console going forward

D. Preventions will be disabled for the host

Correct Answer: A

The option that best describes what happens to detections in the console after clicking "Disable Detections" for a host from within the Host Management page is that the detections for the host are removed from the console immediately and no new detections will display in the console going forward. The "Disable Detections" 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 4

Which of the following is NOT an available filter on the Hosts Management page?

A. Hostname

B. Username

C. Group

D. OS Version

Correct Answer: B

Username is not an available filter on the Hosts Management page. The Hosts Management page allows you to view and manage all the hosts in your environment that have Falcon sensors installed. You can filter the hosts by hostname, group, OS version, sensor version, last seen date, health events, detections, and preventions. You can also perform actions such as assigning hosts to groups, updating sensor policies, uninstalling sensors, or isolating hosts1. References: 1: Falcon Administrator Learning Path | Infographic | CrowdStrike

QUESTION 5

How are user permissions set in Falcon?

A. Permissions are assigned to a User Group and then users are assigned to that group, thereby inheriting those permissions

B. Pre-defined permissions are assigned to sets called roles. Users can be assigned multiple roles based on job function and they assume a cumulative set of permissions based on those assignments

C. An administrator selects individual granular permissions from the Falcon Permissions List during user creation

D. Permissions are token-based. Users request access to a defined set of permissions and an administrator adds their token to the set of permissions

Correct Answer: B

User permissions are set in Falcon by assigning pre-defined permissions to sets called roles. Users can be assigned multiple roles based on job function and they assume a cumulative set of permissions based on those assignments. Roles are collections of permissions that define what users can see and do in Falcon. Permissions are granular actions that allow users to access specific features or functions in Falcon. For example, a user who is assigned both the Falcon Administrator role and the Falcon Investigator role will have all the permissions from both roles2. References: 2: Cybersecurity Resources | CrowdStrike