Free Questions for CCFA-200 by dumpssheet

Shared by Nixon on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

How are user permissions set in Falcon?

Options:

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

Answer:

B

Explanation:

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.

Question 2

Question Type: MultipleChoice

What is the primary purpose of using glob syntax in an exclusion?

Options:

A- To specify a Domain be excluded from detections

B- To specify exclusion patterns to easily exclude files and folders and extensions from detections

C- To specify exclusion patterns to easily add files and folders and extensions to be prevented

D- To specify a network share be excluded from detections

Answer:

B

Explanation:

Glob syntax is used to specify exclusion patterns to easily exclude files and folders and extensions from detections. Glob syntax allows you to use wildcards (*) and ranges ([a-z]) to match multiple characters or values in a file path or name.For example, you can use glob syntax to exclude all files with .exe extension in a folder by using C:\Folder*.exe as an exclusion pattern2.

Question 3

Question Type: MultipleChoice

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

Options:

A- Hostname

B- Username

C- Group

D- OS Version

Answer:

B

Explanation:

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.

Question 4

Question Type: MultipleChoice

You have an existing workflow that is triggered on a critical detection that sends an email to the escalation team. Your CISO has asked to also be notified via email with a customized message. What is the best way to update the workflow?

Options:

A- Clone the workflow and replace the existing email with your CISO's email

B- Add a sequential action to send a custom email to your CISO

C- Add a parallel action to send a custom email to your CISO

D- Add the CISO's email to the existing action

Answer:

C

Explanation:

The best way to update the workflow is to add a parallel action to send a custom email to your CISO. A parallel action allows you to perform multiple actions simultaneously when a workflow is triggered, without affecting the order or outcome of other actions. A sequential action, on the other hand, requires one action to complete before another action can start.By adding a parallel action, you can ensure that both the escalation team and your CISO receive an email notification as soon as possible1.

Question 5

Question Type: MultipleChoice

An analyst has reported they are not receiving workflow triggered notifications in the past few days. Where should you first check for potential failures?

Options:

A- Custom Alert History

B- Workflow Execution log

C- Workflow Audit log

D- Falcon UI Audit Trail

Answer:

B

Explanation:

The Workflow Execution log in the Workflow Management option allows you to view the status and results of workflow executions triggered by detection events. You can filter the log by workflow name, status, start and end time, and detection ID. You can also view the details of each execution, including the actions performed, the output received, and any errors encountered.This log can help you troubleshoot potential failures or issues with your workflows1.

Question 6

Question Type: MultipleChoice

The Logon Activities Report includes all of the following information for a particular user EXCEPT _____.

Options:

A- the account type for the user (e.g. Domain Administrator, Local User)

B- all hosts the user logged into

C- the logon type (e.g. interactive, service)

D- the last time the user's password was set

Answer:

B

Explanation:

Checked in console, it returns only the last machine where the user logged on, so it will not return all the machines that the user was logged on in the desired search

Question 7

Question Type: MultipleChoice

Why is the ability to disable detections helpful?

Options:

A- It gives users the ability to set up hosts to test detections and later remove them from the console

B- It gives users the ability to uninstall the sensor from a host

C- It gives users the ability to allowlist a false positive detection

D- It gives users the ability to remove all data from hosts that have been uninstalled

Answer:

A

Explanation:

'Disable Detections. This is helpful for users who want to set up hosts to test detections in the Falcon console and who later want to remove those old test detections from the'

Question 8

Question Type: MultipleChoice

Which report can assist in determining the appropriate Machine Learning levels to set in a Prevention Policy?

Options:

A- Sensor Report

B- Machine Learning Prevention Monitoring

C- Falcon UI Audit Trail

D- Machine Learning Debug

Answer:

B

Explanation:

The Machine Learning Prevention Monitoring report in the Prevention Policy Management option allows you to monitor the impact of machine learning (ML) prevention settings on your environment. You can view the number of ML detections and preventions by severity, policy, and host group. You can also drill down into specific events and hosts to see more details.This report can help you determine the appropriate ML levels to set in a prevention policy based on your risk tolerance and security posture1.

Question 9

Question Type: MultipleChoice

How do you find a list of inactive sensors?

Options:

A- The Falcon platform does not provide reporting for inactive sensors

B- A sensor is always considered active until removed by an Administrator

C- Run the Inactive Sensor Report in the Host setup and management option

D- Run the Sensor Aging Report within the Investigate option

Answer:

C

Explanation:

The Inactive Sensor Report in the Host setup and management option allows you to view a list of hosts that have not communicated with the Falcon platform for a specified period of time. You can filter the report by sensor version, OS, and last seen date.This report can help you identify hosts that may have connectivity issues or need sensor updates1.

Question 10

Question Type: MultipleChoice

Which of the following options is a feature found ONLY with the Sensor-based Machine Learning (ML)?

Options:

A- Next-Gen Antivirus (NGAV) protection

B- Adware and Potentially Unwanted Program detection and prevention

C- Real-time offline protection

D- Identification and analysis of unknown executables

Answer:

D

Explanation:

According to documentation (documentation/detections/technique/sensor-based-ml-cst0007): CrowdStrike sensor-based machine learning (ML) identifies and analyzes unknown executables as they run on hosts. This technique is triggered by files and file attributes associated with known malware. This is similar to the [Cloud-based ML](/support/documentation/detections/technique/cloud-based-ml) technique. Cloud-based ML is informed by global analysis of executables that classifies and identifies malware. The key difference is that it doesn't run on hosts when they're offline.