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

CrowdStrike Certified Falcon Administrator

Pass CrowdStrike CCFA-200 Exam with 100% Guarantee

QUESTION 1

Why is it important to know your company\\'s event data retention limits in the Falcon platform?

A. This is not necessary; you simply select "All Time" in your query to search all data

B. You will not be able to search event data into the past beyond your retention period

C. Data such as process records are kept for a shorter time than event data

D. Your query will require you to specify the data pool associated with the date you wish to search

Correct Answer: B

It is important to know your company\\'s event data retention limits in the Falcon platform because you will not be able to search event data into the past beyond your retention period. The retention period is the amount of time that event data is stored in the Falcon Cloud, and it may vary depending on your subscription plan and settings. The other options are either incorrect or not related to knowing your retention limits. Reference: CrowdStrike Falcon User Guide, page 48.

QUESTION 2

Why is the ability to disable detections helpful?

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

Correct Answer: A

"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 3

You need to have the ability to monitor suspicious VBA macros. Which Sensor Visibility setting should be turned on within the Prevention policy settings?

A. Script-based Execution Monitoring

B. Interpreter-Only

C. Additional User Mode Data

D. Engine (Full Visibility)

Correct Answer: A

Turn on the Script-Based Execution Monitoring prevention policy setting to enable the "Falcon sensor to monitor the contents of scripts and shells that are popular mechanisms for executing malicious code on hosts. This setting does not kill or block scripts." Scripting languages: Excel 4.0 macros JScript VBA Macros VBScript The Sensor Visibility setting that should be turned on within the Prevention policy settings to monitor suspicious VBA macros is Script-based Execution Monitoring. Script-based Execution Monitoring is a feature that enables the Falcon sensor to monitor and prevent malicious script execution on Windows systems. The feature uses machine learning and behavioral analysis to detect suspicious scripts or commands executed by various script interpreters, such as PowerShell, WScript, CScript, or Bash. VBA (Visual Basic for Applications) is a scripting language that can be embedded in Microsoft Office documents, such as Word or Excel. VBA macros can be used to automate tasks or perform actions within the documents, but they can also be abused by attackers to deliver malware or execute malicious code. Script-based Execution Monitoring can help detect and prevent such attacks by monitoring the contents of VBA macros for execution of malicious content. References: : [Falcon Administrator Learning Path | Infographic | CrowdStrike]

QUESTION 4

What is the purpose of precedence with respect to the Sensor Update policy?

A. Precedence applies to the Prevention policy and not to the Sensor Update policy

B. Hosts assigned to multiple policies will assume the highest ranked policy in the list (policy with the lowest number)

C. Hosts assigned to multiple policies will assume the lowest ranked policy in the list (policy with the highest number)

D. Precedence ensures that conflicting policy settings are not set in the same policy

Correct Answer: B

The purpose of precedence with respect to the Sensor Update policy is that hosts assigned to multiple policies will assume the highest ranked policy in the list (policy with the lowest number). This means that if a host belongs to more than one group that has different Sensor Update policies assigned, it will use the policy that has the highest precedence (lowest number) among them. The other options are either incorrect or not related to precedence. Reference: CrowdStrike Falcon User Guide, page 38.

QUESTION 5

How can you find a list of hosts that have not communicated with the CrowdStrike Cloud in the last 30 days?

A. Under Dashboards and reports, choose the Sensor Report. Set the "Last Seen" dropdown to 30 days and reference the Inactive Sensors widget

B. Under Host setup and management, choose the Host Management page. Set the group filter to "Inactive Sensors"

C. Under Host setup and management > Managed endpoints > Inactive Sensors. Change the time range to 30 days

D. Under Host setup and management, choose the Disabled Sensors Report. Change the time range to 30 days

Correct Answer: C

The administrator can find a list of hosts that have not communicated with the CrowdStrike Cloud in the last 30 days by going to Host setup and management > Managed endpoints > Inactive Sensors. Then, change the time range to 30 days. This will show the host name, last seen date, sensor version and group name for each inactive host. The other options are either incorrect or not available. Reference: [CrowdStrike Falcon User Guide], page 31.