CrowdStrike CCFA-200b Practice Questions

Shared by Fitzgerald on 22-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

How do you disable all detections for a host?

Options:

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

Answer:

D

Explanation:

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 2

Question Type: MultipleChoice

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

Options:

A- Script-based Execution Monitoring
B- Interpreter-Only
C- Additional User Mode Data
D- Engine (Full Visibility)

Answer:

A

Explanation:

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.

Question 3

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 4

Question Type: MultipleChoice

Which Real Time Response role will allow you to see all analyst session details?

Options:

A- Real Time Response - Read-Only Analyst
B- None of the Real Time Response roles allows this
C- Real Time Response -Active Responder
D- Real Time Response -Administrator

Answer:

D

Explanation:

The Real Time Response role that will allow you to see all analyst session details is Real Time Response -Administrator. A Real Time Response -Administrator is a role that has full access and control over the Real Time Response feature in Falcon, which allows you to remotely access and investigate hosts in real time. A Real Time Response -Administrator can view all analyst session details, such as session ID, host name, start and end time, commands executed, and output received.A Real Time Response -Administrator can also create, modify, delete, and assign scripts and commands to other analysts2.

Question 5

Question Type: MultipleChoice

What three things does a workflow condition consist of?

Options:

A- A parameter, an operator, and a value
B- A beginning, a middle, and an end
C- Triggers, actions, and alerts
D- Notifications, alerts, and API's

Answer:

A

Explanation:

A workflow condition consists of a parameter, an operator, and a value. A workflow condition is a rule that defines when a workflow should be triggered based on certain criteria or filters. A parameter is a variable or attribute that can be used to filter or match detection events, such as severity, tactic, or host group. An operator is a symbol or word that specifies how to compare or evaluate the parameter and the value, such as equals, contains, or greater than.A value is a constant or expression that provides the expected or desired result for the parameter, such as high, credential dumping, or default group1.

Question 6

Question Type: MultipleChoice

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

Options:

A- Configuration module
B- Intelligence module
C- Support module
D- Discover module

Answer:

C

Explanation:

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 7

Question Type: MultipleChoice

Custom IOA rules are defined using which syntax?

Options:

A- Glob
B- PowerShell
C- Yara
D- Regex

Answer:

D

Explanation:

Regex guidelines
https://falcon.crowdstrike.com/documentation/68/detection-and-prevention-policies#regex

To Get Premium Files for CCFA-200b Visit

https://www.p2pexams.com/products/ccfa-200b

For More Free Questions Visit

https://www.p2pexams.com/crowdstrike/pdf/ccfa-200b

