



Free Questions for CCFA-200 by ebraindumps

Shared by Bentley on 19-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Why would you assign hosts to a static group instead of a dynamic group?

Options:

- A- You do not want the group membership to change automatically
- B- You are managing more than 1000 hosts
- C- You need hosts to be automatically assigned to a group
- D- You want the group to contain hosts from multiple operating systems

Answer:

A

Question 2

Question Type: MultipleChoice

What type of information is found in the Linux Sensors Dashboard?

Options:

- 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

Answer:

C

Question 3

Question Type: MultipleChoice

Which of the following Machine Learning (ML) sliders will only detect or prevent high confidence malicious items?

Options:

A- Aggressive

B- Cautious

C- Minimal

D- Moderate

Answer:

C

Question 4

Question Type: MultipleChoice

You have created a Sensor Update Policy for the Mac platform. Which other operating system(s) will this policy manage?

Options:

A- *nix

B- Windows

C- Both Windows and *nix

D- Only Mac

Answer:

C

Question 5

Question Type: MultipleChoice

Under the "Next-Gen Antivirus: Cloud Machine Learning" setting there are two categories, one of them is "Cloud Anti-Malware" and the other is:

Options:

A- Adware & PUP

B- Advanced Machine Learning

C- Sensor Anti-Malware

D- Execution Blocking

Answer:

B

Question 6

Question Type: MultipleChoice

Which of the following best describes the Default Sensor Update policy?

Options:

- A-** The Default Sensor Update policy does not have the 'Uninstall and maintenance protection' feature
- B-** The Default Sensor Update policy is only used for testing sensor updates
- C-** The Default Sensor Update policy is a 'catch-all' policy
- D-** The Default Sensor Update policy is disabled by default

Answer:

C

Question 7

Question Type: MultipleChoice

If a user wanted to install an older version of the Falcon sensor, how would they find the older installer file?

Options:

- A- Older versions of the sensor are not available for download
- B- By emailing CrowdStrike support at support@crowdstrike.com
- C- By installing the current sensor and clicking the 'downgrade' button during the install
- D- By clicking on 'Older versions' links under the Host setup and management > Deploy > Sensor downloads

Answer:

D

Question 8

Question Type: MultipleChoice

Which of the following best describes the Default Sensor Update policy?

Options:

- A-** The Default Sensor Update policy does not have the 'Uninstall and maintenance protection' feature
- B-** The Default Sensor Update policy is only used for testing sensor updates
- C-** The Default Sensor Update policy is a 'catch-all' policy
- D-** The Default Sensor Update policy is disabled by default

Answer:

C

Question 9

Question Type: MultipleChoice

If a user wanted to install an older version of the Falcon sensor, how would they find the older installer file?

Options:

- A- Older versions of the sensor are not available for download
- B- By emailing CrowdStrike support at support@crowdstrike.com
- C- By installing the current sensor and clicking the 'downgrade' button during the install
- D- By clicking on 'Older versions' links under the Host setup and management > Deploy > Sensor downloads

Answer:

D

To Get Premium Files for CCFA-200 Visit

<https://www.p2pexams.com/products/ccfa-200>

For More Free Questions Visit

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

