MA0-107^{Q&As}

MA0-107^{Q&As}

McAfee Certified Product Specialist - ENS

Pass McAfee MA0-107 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/ma0-107.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by McAfee Official Exam Center

QUESTION 1

An administrator is running new software, and a file is detected by the On-Access scanner as a Potentially Unwanted Program. In which of the following ways can the administrator prevent the file from being detected?

A. Adding the process name within standard process settings

B. Excluding by detection name

C. Adding to Potentially Unwanted Program Detections.

D. Configuring low-risk settings and low risk the software

Correct Answer: C

QUESTION 2

In which of the following ways would ATP determine the reputation information if Adaptive Threat Protection (ATP) is deployed and neither a TIE server nor an Internet connection is available?

A. ATP will use information from the local system.

B. ATP will query other systems in the environment.

C. ATP will do nothing and auto-disable itself.

D. ATP will prompt the user for manual input.

Correct Answer: B

QUESTION 3

An ePO administrator needs to add exclusions for a folder. The folder has been created in several locations, including C:\Program Files\Custom\Acme or C:\Program Files\Acme, but the folder could be located in other subfolders in the Program Files folder.

Which of the following is the correct way to write an exclusion for the Acme folder?

A. \Program Files\?\Acme

B. \Program Files**\Acme

C. \Program Files*\Acme

D. \Program Files\??\Acme

Correct Answer: C

QUESTION 4

The ePO administrators have already tuned and configured dynamic application containment rules within the policy. In which of the following ways will dynamic application containment protect against malware once enforcement is enabled?

A. The scan engine will learn the behavior of the application and send up to GT1 for analysis, and then receive an action to block all actions from the application\\'s process.

B. If an application\\'s reputation is below the threshold while triggering a block rule and is not an excluded application, malicious behavior of the application will be contained.

C. The ENS client will receive the reputation as "highly suspicious" from either the McAfee GTI or TIE server, and then immediately uninstall the application on the system.

D. The adaptive threat protection scanner will send the file automatically to a preconfigured "Sandbox" folder and analyze the application for malicious features before use.

Correct Answer: B

QUESTION 5

Joe, an administrator, runs a policy-based, on-demand scan on a system and notices that after the scan, a threat event was created for what appears to be a false positive. Joe wants to submit the file for analysis to McAfee Labs; but every time he accesses the file, it is detected.

In which of the following default locations can Joe find the backups of the detected files?

A. %ProgramData%\McAfee\Common Framework\AgentEvents

B. C:\Quarantine

C. C:\Windows\Temp\Quarantine

D. %deflogfir%\Quarantine

Correct Answer: A