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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A new ENS policy has been created and deployed, and a user contacts the help desk stating that a particular site is no longer accessible. Which of the following ENS Web Control policy categories is the culprit?

A. Options

B. Content Actions

C. Browser Control

D. Enforcement Messaging

Correct Answer: D

QUESTION 2

The ENS administrator wants to monitor remotely the modification of files, but BigFix.exe is generating many false positives. Which of the following should the ENS administrator do?

A. Exclude the file under Threat Prevention / Access Protection / Remotely creating or modifying Files or Folders.

B. Add the file as a High Risk Process under Threat Prevention / On Access Scan / Process settings.

C. Exclude the file under Common Options / Self Protection.

D. Add the file under Threat Prevention / Options/ Exclusions by detection name.

Correct Answer: C

QUESTION 3

Which of the following fields can an ePO administrator use when creating exclusions for Dynamic Application Containment?

A. Certificate

B. Rule

C. File version

D. MD5 hash

Correct Answer: D

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

A hospital in another county just received a new variant of ransom ware that infected 70% of its systems. After learning the characteristics of this ransom ware, the security team wants to implement a protection policy to stop certain files from being modified and new registry keys from being created that are relevant to the ransom ware. Which of the following policies meets this requirement?

A. Exploit prevention policy

B. Block and allow list policy

C. Access protection policy

D. Firewall rules policy

Correct Answer: C

QUESTION 6

An ePO administrator wants to enable script scanning in the environment; however, the administrator wants to exclude several custom scripts from being scanned. Which of the following is the BEST practice for script scan exclusions?

A. Ensure wildcard characters are fully supported.

B. Use fully qualified domain names and NetBIOS names.

C. Include port numbers if they are part of the address.

D. Keep the URL short.

Correct Answer: B

QUESTION 7

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 8

An ePO administrator is experiencing issues installing an ENS module on a client machine and decides to investigate by analyzing the install log. In which of the following locations will the administrator find the install log, assuming it is in its default location on the endpoint?

A. %programdata%\mcafee\datreputation\logs

B. **\program files\mcafee\

C. %temp%\mcafeelogs

D. %programdata%\mcafee\Agent\logs

Correct Answer: D

QUESTION 9

Dynamic Application Containment uses which of the following attributes of an executable to provide advanced protection?

A. File behavior

B. File name

C. File size

D. File source

Correct Answer: C

QUESTION 10

A security technician is configuring the exploit prevention policy. Based on best practices for critical servers, which of the following severity levels should the technician configure signatures to block after a requisite period of tuning?

A. Low

B. High

C. Informational

D. Medium

Correct Answer: B

QUESTION 11

An administrator wants to prevent incoming packets until the system reboots fully. Which of the following features should be configured to allow this?

A. Treat McAfee GTI Match as an Intrusion

B. Allow Bridged Traffic

C. Allow Only Outgoing Traffic Until Firewall Services Have Started

D. Block All Untrusted Executables

Correct Answer: C

QUESTION 12

The security team wants to schedule an on-demand scan to run at noon every day for all workstations. However, the team would like to ensure system performance is not impacted because users may be working. Which of the following is a system utilization setting that meets this criteria?

A. Below normal

B. Low

C. Scan only when the system is idle

D. Normal

Correct Answer: D

QUESTION 13

A security professional is configuring ENS for a client and wants to ensure applications will be prevented from executing software locally from the browser or email client. Which of the following McAfee-defined rules should be implemented?

A. Creating new executable files in the Windows folder

B. Installing browser helper objects or shell extensions

C. Registering programs to autorun

D. Running files from common user folders by common programs

Correct Answer: B

QUESTION 14

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

QUESTION 15

While tuning the firewall policy, the ePO administrator notices unauthorized traffic is being initiated by a file transfer utility application. If this is a recently approved application, in which of the following locations should this be configured to allow FTP traffic only with this application?

A. Add a new rule within the Access Protection policy to block port 21 and exclude the executable for the software.

B. Put a new rule in the Exploit Prevention policy to include the executable for the software for additional protection.

C. Exclude the process associated with the software within the On Access Scan policy\\'s Low-Risk Processes section.

D. Create an allow rule within the Rules policy for inbound/outbound on port 21 and the executable for the software.

Correct Answer: A