McAfee MA0-107 Exam

Volume: 70 Questions

Question: 1
A hospital in another county just received a new variant of ransomware that infected 70% of its systems. After learning the characteristics of this ransomware, 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 ransomware. 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

Answer: C

Question: 2
By using which of the following techniques does Real Protect scanner inspect suspicious files and activities on an endpoint to detect malicious patterns?

A. Machine learning

B. Intrusion prevention

C. Sandboxing

D. Static code analysis

Answer: B

Question: 3
An IT department is looking for a way to optimize performance with on-access scanning. To maximize security and minimize the impact on the system, on-access scanning should be configured to scan files at which of the following frequencies?

A. Disable on-access scanning.

B. Let McAfee decide.

C. Only scan files on write.

D. Only scan files on read.

Answer: C

Question: 4
In which of the following locations are the installation log files stored by default on a Windows machine?

A. %TEMP%\McAfeeLogs

B. %PROGRAMDATA%\McAfee\Logs

C. %USERDATA%\McAfeeLogFiles

D. %PROGRAMFILES%\CommonFiles\McAfeeLogs

Answer: C

Question: 5
Which of the following is the MAIN benefit of using Threat Intelligence Exchange (TIE) and Data Exchange Layer (DXL)?

A. They enable centralized management of adaptive-threat-protection policies.

B. They store and pass file reputation to managed endpoints and McAfee products.

C. They distribute signature-based content to managed systems.

D. They conduct scanning of files on managed systems for threats.

Answer: B

Question: 6
Security operations has recently received indicators of compromise (IOCs) detailing a new piece of malware for which coverage is not available. The threat advisory recommends a list of file paths and registry keys to prevent this new malware from successfully executing. Which of the

following ENS 10.5 features should be used to achieve this goal?

A. Web Control

B. Exploit Prevention

C. Real Protect

D. Access Protection

Answer: D

Question: 7
An administrator wants to add executables that are monitored with the Exploit Prevention engine. To which of the following policy sections should the executables be added?

A. Generic privilege escalation prevention

B. Exclusions

C. Signatures

D. Application protection rules

Answer: A

Question: 8
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.

Answer: B

Question: 9
A company's security posture requires the ENS firewall to be enabled; however, the team is unsure of communication flows in the environment. In which of the following modes should the ePO administrator deploy the firewall policy to achieve flow awareness?

A. Adaptive Mode

B. Interface Mode

C. Enforce Mode

D. Observe Mode

Answer: B

Question: 10
An ENS administrator wants the end user to be able to view the web safety information. In addition to enabling Web Control, which of the following describes the requirements for this?

A. The Web Control Plug-in site report must be enabled on the browser toolbar.

B. Content Action settings must be configured to specify the action to apply according to the site rating.

C. The Web Control Plug-in must be enabled in the browser, and "Warn" must be selected in Action Enforcement.

D. The Web Control Plug-in must be enabled in the browser, and the client browser toolbar must be enabled.

Answer: A

Question: 11
When creating an exploit prevention process exclusion, at least one identifier must be specified. Which of the following is an identifier?

A. DEP

B. MD5 hash

C. API

D. Caller module

Answer: B

Question: 12
Which of the following items are sent to the cloud when Real Protect scanning is enabled on endpoints that are connected to the Internet?

A. System information

B. Running process

C. Behavioral information

D. File reputation

Answer: B

Question: 13
An ePO administrator decides to define a trusted network in the firewall policy. This will result in:

A. an inbound directional allow rule for that remote network.

B. an outbound directional allow rule for that remote network.

C. a bidirectional allow rule for that remote network.

D. a bidirectional deny rule for that remote network.

Answer: A

Question: 14
Which of the following server roles has a McAfee-defined policy bundled with the product?

A. Exchange

B. Internet Information Services (IIS)

C. Active Directory