McAfee MA0-104 Exam

Volume: 66 Questions

Question No: 1
The historical ACE function allows the user to perform retrospective correlations on older data. In which of the following devices is the data located that the historical correlation engine uses?

A. ELM

B. REC

C. ADM

D. ESM

Answer: A

Question No: 2
When preparing to apply a patch to the Enterprise Security Manager (ESM) and completing the ESM checklist, the command cat/proc7mdstat has been issued to determine RAID functionally The system returns an active drive result identified as [U J What action should be taken?

A. Apply the patch, this is a properly functional RAID which can be upgraded.

B. Apply the patch, drive 1 is active and can be upgraded.

C. Apply the patch, drive 2 is active and can be upgraded.

D. Contact support before proceeding with the upgrade.

Answer: D

Question No: 3
The McAfee Advanced Correlation Engine (ACE) ca n t >e deployed in one of two modes which are.?

A. Threshold and Anomaly.

B. Prevention and Detection.

C. Stateful and Stateless.

D. Historical and Real-Time.

Answer: D

Question No: 4
The Database Event Monitor (OEM) appliance prevents disclosure of Personally Identifiable Information (PI I) by employing which of the following features to those types of information?

A. Obfuscation masks

B. Pll filter masks

C. Sensitive data masks

D. Filter masks

Answer: C

Question No: 5
One or more storage allocations, which together specify a total amount of storage, coupled with a data retention time that specifies the maximum number of days a log is to be stored, is known as a

A. Storage Volume.

B. Storage Pool.

C. Storage Device.

D. Storage Area Network (SAN).

Answer: B

Question No: 6
Which of the following security technologies sits inline on the network and prevents attacks based on signatures and behavioral analysis that can be configured as a data source within the SIEM?

A. Firewall

B. Email Gateway

C. Host Intrusion Prevention System

D. Network Intrusion Prevention System

Answer: D

Question No: 7
Analysts can effectively use the McAfee SIEM to identify threats by ?

A. focusing on aggregated and correlated events data.

B. disabling aggregation, so all data are visible.

C. studying ELM archives, to analyze the original data

D. use the streaming event viewer to analyze data.

Answer: A

Question No: 8
If there is no firewall at the border of the network, which of the following could be used to simulate the protection a firewall provides?

A. Load balancer

B. Router Access Control List (ACL)

C. Switch port blocking

D. An email gateway

Answer: B

Question No: 9
When viewing the Policy Tree, what four columns are displayed within the Rules Display pane?

A. Action, Seventy, Aggregation, Copy Packet

B. Action, Seventy, Normalization, Copy Packet

C. Action, Seventy, Aggregation, Drop Packet

D. Enable, Severity, Aggregation, Copy Packet

Answer: A

Question No: 10
An organization notices an increasing number of ESM concurrent connection events. To mitigate ri sks related to concurrent sessions which action should the organization take?

A. Increase the concurrent session alarm threshold

B. Decrease the console timeout value

C. Increase the number of the concurrent sessions allowed

D. Customize the login page with the organization's logo

Answer: B

Question No: 11
Which of the following are the three default users defined within the Users and Groups option in the ESM properties?

A. NGCP, POLICY, REPORT

B. NGCP, BACKUP, REPORT

C. ADMIN, POLICY, REPORT

D. NGCP, SYSTEM, REPORT

Answer: D

Question No: 12
When displaying baseline averages using the automatic time range option, baseline data is correlated by using the same time period that is being used for the current query for which of the following past number of intervals?

A. Three

B. Seven

C. Five

D. Ten

Answer: C

Question No: 13
When the automated system backup is configured to include events, flows and log data, the first backup will capture all events, flows and logs

A. in the ESM database.

B. in the ESM database older than what is currently held in the Receivers.

C. inserted in the ESM database on the most recent Receiver poll.

D. in the ESM database from the current day.

Answer: D

Question No: 14
Event Aggregation is performed on which of the following fields?

A. Signature ID, Destination IP, User ID

B. Source IP, Destination IP, User ID

C. Signature ID, Source IP, Destination IP

D. Signature ID, Source IP, User ID

Answer: C

Question No: 15
Alarms using field match as the condition type allow for selected Actions to be taken when the Alarm condition is met. Which of the following McAfee ePolicy Orchestrator (ePO) Actions can be selected when creating such Alarm?