

Intel Security Product Specialist MA0-104

Intel Security Certified Product Specialist

Thank You for Downloading MA0-104 Updated Exam Questions

<https://certs4sale.com/mcafee/ma0-104-pdf-exam-dumps>

Version: 8.0

Question: 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: 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 functionality. 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: 3

The McAfee Advanced Correlation Engine (ACE) can be 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: 4

The Database Event Monitor (DEM) appliance prevents disclosure of Personally Identifiable Information (PII) by employing which of the following features to those types of information?

- A. Obfuscation masks

- B. PII filter masks
- C. Sensitive data masks
- D. Filter masks

Answer: C

Question: 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: 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: 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

THANK YOU FOR DOWNLOADING MA0-104 UPDATED EXAM QUESTIONS

Note: Thanks For Trying The Demo Of Our MA0-104 Exam Product

Visit Our Site to Purchase the Full Set of Actual MA0-104 Exam Questions With Answers.

Money Back Guarantee



Click The Link Below

<https://certs4sale.com/mcafee/ma0-104-pdf-exam-dumps>