McAfee

Exam MA0-104

Intel Security Certified Product Specialist

Verson: Demo

[Total Questions: 10]

Question No : 1

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 : 2

While investigating beaconing Malware, an analyst can narrow the search quickly by using which of the following watchlists in the McAfee SIEM?

A. MTIE Suspicious and Malicious
B. TSI Suspicious and Malicious
C. GTI Suspicious and Malicious
D. MTI Suspicious and Malicious

Answer: C

Question No : 3

How often does the configuration and policy data from the primary Enterprise Security Manager (ESM) get synchronized with the redundant ESM?

A. Every 2 minutes
B. Every 5 minutes
C. Every 10 minutes
D. This is based on manual selection

Answer: B

Question No : 4

A backup of the ELM management database captures

A. ELM configuration settings
B. ELM configuration settings, and the ELM archive index
C. ELM configuration settings, the ELM archive index, and all archived ELM contents.
D. ELM configuration settings, the ELM archive index, and all archived ELM contents up to the ESM database retention limit.

Answer: B

Question No : 5

If the SIEM Administrator deploys the Enterprise Security Manager (ESM) using the Federal Information Processing Standards (FIPS) encryption mode, which of the following types of user authentication will NOT be compliant with FIPS?

A. Windows Active Directory
B. Radius
C. Lightweight Directory Access Protocol (LDAP)
D. Local Authentication

Answer: B

Question No : 6

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 : 7

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 : 8

The McAfee Advanced Correlation Engine (ACE) can 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 : 9

The possibility of both data source Network Interface Cards (NICs) using the shared IP and MAC address at the same time is eliminated by using which of the following?

A. iSCSI Adapter
B. iPMICard
C. PCI Adapter
D. SAN Card

Answer: B

Question No : 10

The primary function of the Application Data Monitor (ADM) appliance is to decode traffic at layer

A. one for inspection.
B. three for inspection.
C. five for inspection.
D. seven for inspection.

Answer: D