DUMPSARENA

Intel Security Certified Product Specialist

McAfee MA0-104

Version Demo

Total Demo Questions: 10

Total Premium Questions: 70

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

A McAfee Event Receiver (ERC) will allow for how many Correlation Data Sources to be configured?

A. 1

B. 3

C. 5

D. 10

ANSWER: A

QUESTION NO: 2

Checkpoint firewalls provide logs to the McAfee SIEM Receiver in which of the following formats?

A. Syslog

B. open Platform for Security (OPSEC)

C. McAfee Event Format (MEF)

D. Common Event Format (CEF)

ANSWER: B

QUESTION NO: 3

Flow Aggregation is based on which of the following?

A. Source IP, Source Port, Destination IP

B. Source IP, Destination IP, Source User ID

C. Source IP, Destination Port, Host ID

D. Source IP, Destination IP, Destination Port

ANSWER: D

QUESTION NO: 4

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: 5

Which authentication methods can be configured to control alarm management privileges?

A. SNMP

B. SSH Key Pair

C. Active Directory

D. Access Groups

ANSWER: D

QUESTION NO: 6

When a Correlation Rule successfully triggers, this occurs at the

A. Correlation Element.

B. Correlation Processor.

C. Correlation Engine.

D. Correlation Manager.

ANSWER: C

QUESTION NO: 7

On the McAfee enterprise Security Manager (ESM), the default data Retention setting specifies that Event and Flow data should be maintained for

A. 365 days.

B. same value as configured on the ELM.

C. 90 Days

D. all data allowed by system

ANSWER: D

QUESTION NO: 8

Which of the following is the Primary function of the Event Receiver (ERC) in relation to the Enterprise Security Manager (ESM)?

A. Collect and parse events before the ESM pulls them form the ERC

B. Collect and parse the events before the receiver forwards them to the ESM

C. Collect and store the events before they are forwarded to the ESM for parsing

D. Collect and parse the events before forwarding them to the ELM

ANSWER: A

QUESTION NO: 9

Which of the following two appliances contain Event databases?

A. ELM and REC

B. ESM and ELM

C. ESM and REC

D. REC and ADM

ANSWER: C

QUESTION NO: 10

Reports can be created by selecting the ESM System Properties window, the Reports Icon in the top right of the ESM screen or by which of the following other method selecting the ESM System Properties window, the Reports Icon in the top right of the ESM screen or by which of the following other methods within Alarm Creation?

A. Actions tab

B. Conditions tab

C. Escalation tab

D. Summary tab

ANSWER: A