DUMPSARENA

Intel Security Certified Product Specialist

McAfee MA0-104

Version Demo

Total Demo Questions: 10

Total Premium Questions: 70

Buy Premium PDF

https://dumpsarena.com

sales@dumpsarena.com

QUESTION NO: 1

The normalization value assigned to each data-source event allows

A. increased usability via views based on category rather than signature ID

B. more efficient parsing of each event by the McAfee SIEM Receiver.

C. quicker ELM searches

D. the McAfee ESM database to retain fewer events overall.

ANSWER: A

QUESTION NO: 2

An organization notices an increasing number of ESM concurrent connection events. To mitigate risks 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: 3

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: 4

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: 5

Be default, events in McAfee SIEM are aggregated on which of the following three fields?

A. Signature ID, Source IP, Source Port

B. Signature ID, Source IP, Destination IP

C. Signature ID, Destination IP, Source User

D. Signature ID, Event ID, Source IP

ANSWER: B

QUESTION NO: 6

In the context of McAfee SIEM, the local protected network address space is a variable referred to as.

A. TRUSTED_NET

B. INTERNAL_NET

C. EXTERNAL_NET

D. HOME_NET

ANSWER: D

QUESTION NO: 7

McAfee's SIEM provides awareness of illicit behavior across multiple internal systems via

A. default data-source events.

B. default correlation events

C. default alerts.

D. default reports.

ANSWER: C

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

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

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