Free Questions for 050-11-CARSANWLN01 by ebraindumps

Shared by Mclean on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following statements best defines an RSA NetWitness application rule?

Options:

A- The rule filters, truncates, keeps or otherwise flags data analyzed by RSA NetWitness

B- The rule is used primarily to distribute content among RSA NetWitness appliances

C- The rule uses external intelligence based on IP addresses or domains to add contextual content to network traffic

D- The rule is an open programming language for customizing logic into the RSA NetWitness processing engine to identify new protocols or extract data to be indexed

Answer:

A

Question 2

Question Type: MultipleChoice

Which of the following actions can a Network Rule NOT perform?

Options:

A- Filter

B- Truncate

C- Alert

D- Forward

Answer:

D

Question 3

Question Type: **MultipleChoice**

The Reporting Engine is located on which device?

Options:

A- Decoder

B- Concentrator

C- ESA

D- NetWitness Server

Answer:

D

Question 4

Question Type: **MultipleChoice**

Administrators can use the Profile feature to limit views with (Choose three)

Options:

A- Meta groups

B- Custom column groups

C- Assigned pre-queries

D- Automated role assignment

E- Data privacy policies

F- List view

Answer:

A, B, C

Question 5

Question Type: MultipleChoice

Which of the following choices describes a fundamental unit of network traffic transmitted from one IP device to another?

Options:

A- Packet

B- Chart

C- Session

D- Schedule

Answer:

A

Question 6

Question Type: MultipleChoice

Which of the following statements is true regarding Packet-based analysis in general?

Options:

A- Packet-based analysis is required for viewing log and session data

B- Packet-based analysis is based on metadata capture reduced to packets

C- Packet-based analysis can be accomplished with common tools such as Wireshark

D- Packet-based analysis is accomplished using the table-map xml file

Answer:

B

Question 7

Question Type: MultipleChoice

The logical operators available for Querying in Investigations depend on the Index Level of the individual meta key Which Index Level limits your query to the logical operators "exists" and 'texists""?

Options:

A- IndexNone

B- IndexKeys

C- IndexValues

D- IndexAII

Answer:

B

Question 8

Question Type: MultipleChoice

The Context Hub runs as a service on which Host?

Options:

A- Decoder

B- Concentrator

C- ESA

D- Server

Answer:

C