DUMPSARENA

RSA NetWitness Logs & Network Administrator Exam

RSA 050-11-CARSANWLN01

Version Demo

Total Demo Questions: 10

Total Premium Questions: 71

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

The accuracy of Automated Threat Detection is enhanced by configuring

A. Who is Lookup Service

B. Incident Rules

C. ESA Analytics Mappings

D. Context Hub

ANSWER: A

QUESTION NO: 2

If you choose "Stop Rule Processing" in your Application Rule definition, which of the following are action choices? (Choose three)

A. Keep

B. Filter

C. Truncate

D. Index

E. Transient

F. Remove

ANSWER: A B C

Explanation:

https://community.rsa.com/docs/DOC-42041

QUESTION NO: 3

When NetWitness receives a log from an event source that does not currently exist in the Admin. Event Sources list, what does it do?

A. Writes the log to the Archiver but not the Decoder

B. Parses the log to the Decoder, but in transient mode only

C. Adds the new Event Source to the existing list of Event Sources

D. Ignores the log altogether

ANSWER: C

QUESTION NO: 4

Which of the following statements about the REST interface are true? (Choose two)

A. The REST interface is available only for Concentrators and Decoders

B. The REST interface is available separately for each core Service on the Host

C. The REST interface for the Broker service defaults to 50103

D. The REST interface for the Concentrator service defaults to 51005

E. The REST interface for the Decoder service defaults to 50014

ANSWER: B C

QUESTION NO: 5

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

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 NO: 6

Which RSA NetWitness component indexes metadata extracted from network or log data and makes it available for querying?

A. Broker

B. Informer

C. Spectrum

D. Concentrator

ANSWER: D

QUESTION NO: 7

Which of the following are valid sources for the Context Hub? (Choose two)

A. RSA Endpoint

B. Respond Server

C. Health and Wellness module

D. Web Threat Detection

E. Reporting Engine

ANSWER: A B

QUESTION NO: 8

To allow for automatic email notification when your reports have run. (Choose two)

A. create a Report Rule

B. enable email notification in the Report rule

C. enable email notification in the Report Schedule view

D. create an output action in the Reporting Engine configuration

E. add the mail server as a data source to the Reporting Engine

ANSWER: C D

QUESTION NO: 9

To use RSA SecurID as an authentication method for administrators, what must be configured?

A. PAM

B. CHAP

C. RADIUS

D. LDAP

ANSWER: A

QUESTION NO: 10

When storage on the core devices fills to capacity, what happens?

A. new traffic cannot be ingested

B. the decoder leverages capacity in the concentrator, and collection continues

C. the decoder leverages capacity in the broker, and collection continues

D. the oldest stored sessions are deleted and collection continues

ANSWER: D