

QUESTIONS & ANSWERS

Kill your exam at first Attempt



RSA

050-ENVCSE01

CSE RSA enVision Essentials (new update)

QUESTION: 89

True or False: According to PCI Auditors, inadequate logging is one of the top three areas of failure for the Payment Card Industry (PCI) Data Security Standard (DSS).

- A. True
- B. False

Answer: A

QUESTION: 90

In the enVision data flow, which of the following sequences represents the correct series of events? (Check the one best answer.)

- A. Data collection, data reporting, nugget creation, IPDB storage, data packaging
- B. Data collection, IPDB storage, nugget creation, data packaging, data reporting
- C. Data collection, nugget creation, data packaging, IPDB storage, event reporting
- D. Data collection, data packaging, IPDB storage, nugget creation, event reporting

Answer: C

QUESTION: 91

What determines the severity level of an Alert Category? (Check the one best answer.)

- A. The threshold level of the Trend parameter.
- B. The greatest deviation from the baseline value.
- C. The level of output actions specified for an alert.
- D. The number of times a specific alert is repeated in a specified time period.

Answer: B

QUESTION: 92

For the functions of collecting, storing, and managing event log data RSA enVision utilizes what kind of database architecture? (Check the one best answer.)

- A. Internet protocol database
- B. Relational database
- C. Both
- D. RSA enVision does not use a database architecture

Answer: A

QUESTION: 93

True or False: A "log" is a record of an event or activity occurring within an organization's systems or networks.

- A. True
- B. False

Answer: A

QUESTION: 94

A single RSA enVision Site can NOT contain more than one of which of the following components? (Check the one best answer.)

- A. Local Collector (LC)
- B. Remote Collector (RC)
- C. Database Server (D-SRV)
- D. Application Server (A-SRV)

Answer: C

QUESTION: 95

The set of enVision services is the same for both single unit appliances and multiple unit appliances

- A. True
- B. False

Answer: B

QUESTION: 96

Which of the following describes the timestamp that is shown in the Event Viewer Date/Time field? (Check the one best answer.)

- A. The timestamp is from the source device for that event.
- B. The timestamp is from the enVision collector that is appended to the event.
- C. The timestamp indicates the time the event was first viewed in Event Viewer.
- D. The timestamp indicates the elapsed time between event origination and capture.

Answer: B

QUESTION: 97

What should you reference to determine if RSA enVision's standard reports comply with the Sarbanes-Oxley (SOX) or the BASEL II standards? (Check the one best answer.)

- A. Sarbanes-Oxley and BASEL II web sites which list compliance reports available from enVision
- B. The enVision administrative interface which by default includes both SOX and BASEL II reports
- C. The Best Practices tool section of the Overview Tab which provides an overview with links to compliance related documents
- D. The Compliance Report Filter (CRF) which can be downloaded from the RSA enVision Support web site to print all compliance reports

Answer: C

For More exams visit <https://killexams.com>



[KILLEXAMS.COM](https://killexams.com)

Kill your exam at First Attempt....Guaranteed!