RealValidExam

Try before you buy

Download a free sample of any of our exam questions and answers

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

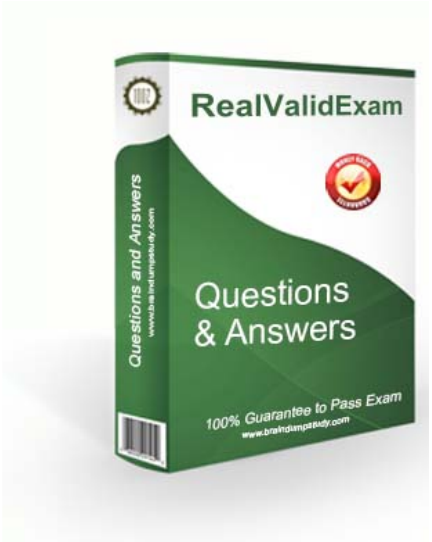
Choose an exam to sample

Select a vendor...

Select an exam...

Your email address

Download Now



QUALITY AND VALUE

RealValidExam Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.

TESTED AND APPROVED

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

EASY TO PASS

If you prepare for the exams using our RealValidExam testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

TRY BEFORE BUY

RealValidExam offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

http://www.realvalidexam.com

100% real and valid exam dumps can ensure you pass at the first attempt

Exam : **C1000-018**

Title : IBM QRadar SIEM V7.3.2 Fundamental Analysis

Vendor : IBM

Version : DEMO

NO.1 An analyst needs to create a dashboard item that can be shared with other users. What is the main step in this process?
A. Ask the administrator to modify the shared search criteria and test the dashboard.
B. Create and share the search criteria that the dashboard Item will use.
C. Enable a new custom dashboard and share it with users.
D. Have users index the shared search criteria for reuse.
Answer: C

NO.2 When is the rating of an Offense magnitude re-evaluated?
A. when the threat assessment changes
B. when new events are added to the Offens
C. when a port is opened
D. when the number of vulnerabilities increases
Answer: B

NO.3 An analyst needs to find events coming from unparsed log sources in the Log Activity tab.
What is the log source type of unparsed events?
A. SIM Unknown
B. SIM Error
C. SIM Generic
D. SIM Unparsed
Answer: C
Explanation
SIM Generic log source or by using the Event is Unparsed filter.

NO.4 An analyst has manually created a new log source in QRadar.
What is the Low Level Category that will be applied to all events sent from this log log source type is applied?
A. Unavailable
B. Stored
C. Unknown
D. Not Found
Answer: D

NO.5 QRadar collects information from numerous log sources and other agents. Sometimes these agents stop reporting to QRadar for a variety of reasons. There is a default rule in QRadar to help identify these cases called the Device Stopped Sending Events (DSSE) Rule.
What does the DSSE Rule do?
A. It checks for log sources which are reporting that they have not had any communication in a certain amount of time.
B. It listens for log sources that send out regular health events and triggers the Rule when encountered
C. It checks for Rules which have fired due to an absence of Events.

D. It runs when there is an absence of Events.
Answer: C

NO.6 What is the procedure to re-open a closed Offense?
A. Activate the Offense in the action/re-open drop down menu of the Offense tab.
B. A closed Offense cannot be re-opened.
C. Wait for new events/flows that will re-open the closed Offense.
D. Activate the Offense in action/re-open drop down menu in the Admin tab.
Answer: B
Explanation
Not possible to reopen a closed offense.

NO.7 An analyst is encountering a large number of false positive results. Legitimate internal network traffic contains valid flows and events which are making it difficult to identify true security incidents. What can the analyst do to reduce these false positive indicators?
A. Create an anomaly rule to detect false positives and suppress the event.
B. Create X-Force rules to detect false positive events.
C. Filter the network traffic to receive only security related events.
D. Modify rules and/or Building Block to suppress false positive activity.
Answer: C