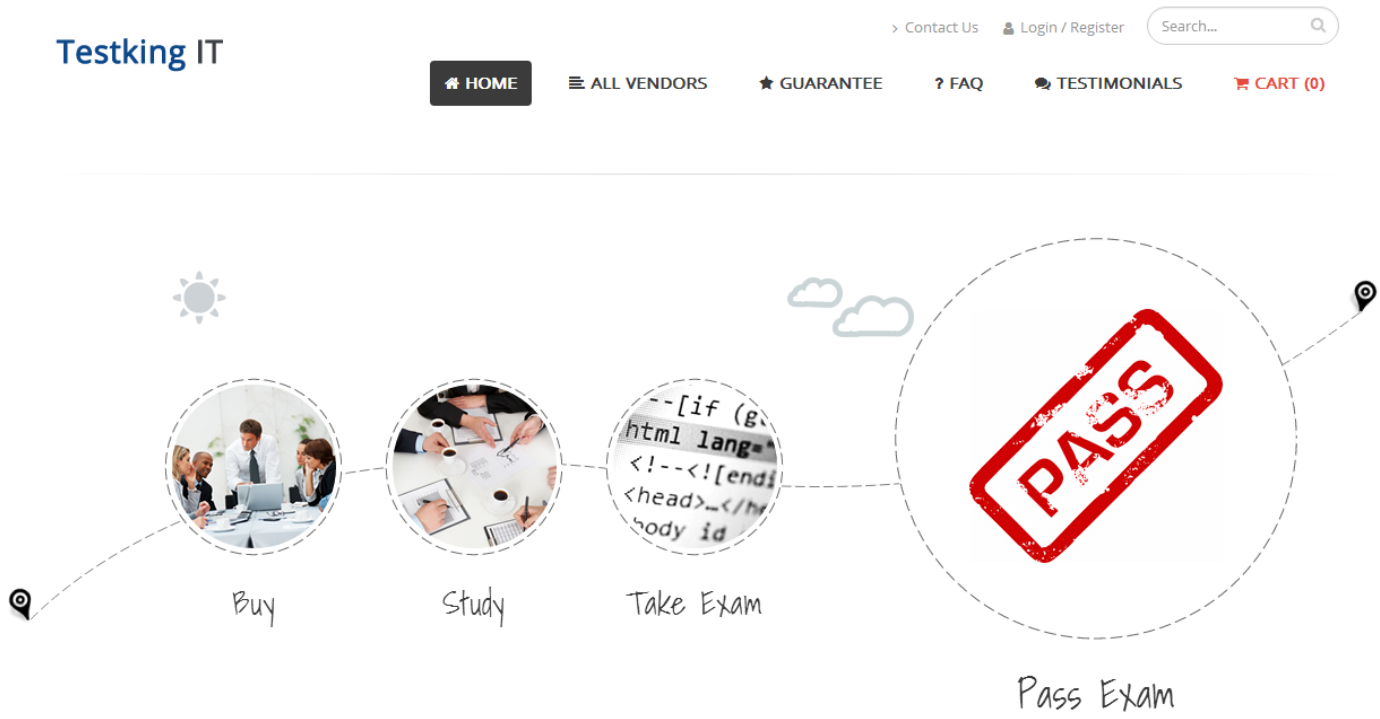
TestkingIT



Try **Desktop Test Engine** before you buy

We're not the only ones **happy** about TestKingsIT Practice Material ...

48236+ customers in 100+ countries use TestKingsIT Test Engine. Meet our customers.

iMessenger VOREED GetCustom JET ORANGE iCompany Paradoxx

http://www.testkingit.com/

Latest practice material - Exam Cram - TestKingIT

Exam : **000-196**

Title : IBM Security QRadar SIEM V7.1 Implementation

Vendor : IBM

Version : DEMO

NO.1 What are false positive rules?
A. Rules that create offenses that the user should ignore.
B. Rules that have matched could severely impact the environment.
C. Rules that make use of the tests relation And Not. The test that follows this relation, if positively matched, will be negated and evaluated as not matched.
D. They are mostly made out of building blocks and filtered out events or flows from the Correlation Rule Engine pipeline using selection criteria that deem the matching events or flows should not contribute to an offense.
Answer: D

NO.2 What must be done to obtain a token for an Authorized Service for WinCollect?
A. Select Authorized Service under the WinCollect plug-in
B. Add the service as an Authorized Service in the Admin tab
C. Go to System and License Management and add an Authorized Service
D. Go to Console Settings and add the already configured WinCollect as an Authorized Service
Answer: B

NO.3 What is a best practice when creating users and assigning roles?
A. For one-off user creation or for a quick task, assign a user to the Admin role.
B. Create a role for each user to make it easy to manage an individual's permissions.
C. To make user management less time-consuming, create general user accounts with broad to specific permissions that can be shared between staff.
D. Group users with like duties together and create roles with permissions that satisfy their business requirements; create roles for individuals only in cases of a special permission requirement.
Answer: D

NO.4 Which connection type to the console is required to run qchange_netsetup?
A. Local
B. SSH
C. RDP
D. Telnet
Answer: A

NO.5 What will happen when a user sets a search as default?
A. The search will be set as the user's default search.
B. All IBM Securily Qradar SIEM V7.1 (QRadar) users will have that search set as their default search.
C. QRadar users will be able to select that search as their default from a list of searches.
D. Only users with permission to view the data in the search results will see the search as an option.
Answer: A

NO.6 Which log file contains all of the relevant logging data for IBM Security Qradar SIEM V7.1?
A. /var/log/qradar.txt
B. /var/log/qradar.log
C. /var/log/messages

D. /var/log/qradar.error
Answer: B

NO.7 Which infrastructure components must be present before installing any of the virtual appliances?
A. VMware ESX 3.7 with VMware vSphere client 3.9 fix pack 12
B. VMware ESXi 4.0.8 with VMware Workstation 9.0 installed on the desktop
C. VMware ESXi 4.1 with VMware vSphere client 4.1 installed on the desktop
D. VMware Workstation 8.0.4 or above with VMware vSphere client 4.0 installed on the desktop
Answer: C

NO.8 On the Index Management page, what does the value of the Data Written column represent?
A. The total amount of data the indexer has processed.
B. The total amount of data consumed on disk by the index.
C. The amount of data the indexer processed during the selected time range.
D. The amount of data consumed on the disk by the index during the selected time range.
Answer: D