Vendor: IBM

Exam Code: C2150-196

Exam Name: IBM Security QRadar SIEM V7.1 Implementation

Version: DEMO

QUESTION 1
Which connection type to the console is required to run qchange_netsetup?

A. Local
B. SSH
C. RDP
D. Telnet

Answer: A

QUESTION 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

QUESTION 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

QUESTION 4
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

QUESTION 5
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

QUESTION 6
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

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.

★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**