C2150-196^{Q&As}

IBM Security QRadar SIEM V7.1 Implementation

Pass IBM C2150-196 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/C2150-196.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official
Exam Center

QUESTION 1

How are user permissions applied using Log Source groups?

A. using user roles

B. applied to individual users

C. applied to network objects

D. applied to authorized services

Correct Answer: A

QUESTION 2

Where are firewall event details located using the IBM Security QRadar SIEM V7.1 interface?

A. Admin

B. Assets

C. Log Activity

D. Network Activity

Correct Answer: C

QUESTION 3

What are the main functions of the Report wizard within IBM Security QRadar SIEM V7.1?

A. to enable branding of reports with a customer\\'s logo or local identification information

B. to specify the schedule, layout, report content, output format, and distribution channels

C. to create new report groups which are placed in the existing hierarchy of reporting groups

D. to select from compliance, executive, log source, network management, and security

Correct Answer: B

QUESTION 4

Which Admin setting allows the monitoring of system load over 15 minutes?

A. System Configuration

B. System Activity Report

C. Forwarding Destinations

D. Global System Notifications

Correct Answer: D

QUESTION 5

Where is a LSX uploaded to IBM Security QRadar SIEM V7.1 to be used by a UDSM in the Admin Section?

A. Log Source Extensions> Add

B. Log Sources> Add > Extensions

C. System Settings> Extensions > Add

D. Systems and License Management> Add > Extensions

Correct Answer: A

QUESTION 6

Whatis the purpose of the offense index?

A. When the offense is created it will create indexes for other offenses.

B. It helps find the offenses faster when searching for offenses by a specific properly.

C. When the offense is created it will be added to anyexisting similar open offense with the same indexed value. If none exist, a new offense will be opened.

D. When the offense is created the magistrate will search for offenses with the same indexed value and add the offense to a list of offenses for the indexed value.

Correct Answer: C

QUESTION 7

After editing the IPTables configuration file, which command reloads the IPTables?

A. serviceiptables save

B. /etc/sysconfig/iptables restart

C. /opt/qradar/bin/iptables restart

D. /opt/qradar/bin/iptables_update.pl

Correct Answer: D

QUESTION 8

Which scenario best describes the actions that take place during a restore?

A. Existing files and database are backed up,archived files and database are restored, the event collection service is restarted.

B. Tomcat and all system processes are shut down, files and data records are extracted from the backup archive and restored to disk and the database, Tomcat and system processes are restarted.

C. Tomcat and database processes are shut down, existing files and database are backed up, archive contents are restored to disk and the database, Tomcat and the system processes are restarted.

D. Existing files and database records are merged with the archived files and database records, Tomcat and system services shut down, the merged records are inserted into their respective file locations and database tables, Tomcat and system services restart.

Correct Answer: B

QUESTION 9

What is the default setting for Major Updates in Auto Updates > Change Settings > Update Types?

A. Disable

B. Auto Install

C. Auto Update

D. Auto Integrate

Correct Answer: A

QUESTION 10

How can asset profiles be searched?

A. From the Assets tab

B. From the Offenses tab

C. Right-click on any

D. Address from the Actions pull-down menu

Correct Answer: A

QUESTION 11

What two types of retention buckets are available in IBM Security QRadarSEM V7.1? (Choose two.)

A. Flow

B. Event

C. Assets

D. Offense

E. Log Source

Correct Answer: AB

QUESTION 12

Which statement is true about the IBM Security QRadar SIEM (QRadar) Network Hierarchy?

A. It is used by QRadar to detect botnets.

B. It is used by QRadar to detect applications.

C. It is used by QRadar only totrack network activity.

D. It is used by QRadar to determine which IP addresses are local and remote.

Correct Answer: D

C2150-196 Practice Test   C2150-196 Study Guide   C2150-196 Exam Questions

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle
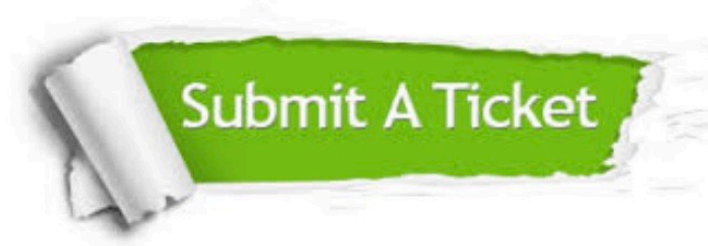
We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.pass4itsure.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:

One Year Free Update
Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee
To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy
We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.