Vendor:IBM

Exam Code:C2150-196

Exam Name:IBM Security QRadar SIEM V7.1 Implementation

Version: Demo

QUESTION 1

Prom the Dashboard view, the Compliance Overview dashboard >Login Failures by User (real-time) workspace is being reviewed. Which link provides more details about these events?

A. View in Assets

B. View in Offenses

C. View in Log Activity

D. View in Network Activity

Correct Answer: C

QUESTION 2

When creating a behavioral rule in Automated Anomaly Analysis, which three components are weighted todetermine the rule?

A. autoregressive pattern, fit to underlying curve, and moving average

B. seasonal or cyclical behavior, underlying trend, and random fluctuation

C. previous period value, current observation, and average of residuals for future observations

D. length of the seasonal component, date range for the trend, and time window during the day

Correct Answer: B

QUESTION 3

Which three pieces of information must be supplied to properly set up a system user? (Choose three.)

A. user role

B. full name

C. room number

D. e-mail address

E. valid user name

F. contact phone number

Correct Answer: ADE

QUESTION 4

Where is the optimal location for IBM Security QRadar QFIow appliances to monitor Internettraffic?

A. in the datacenter

B. at the workstation switches

C. at the wireless access points

D. at an ingress/egress point in the network

Correct Answer: D

QUESTION 5

What must be done prior to clicking on False Positive if flows or events are being viewed in streaming mode?

A. click on the Pause button

B. click on the Refresh button

C. right-click on the event and click Filter

D. right-click on the event and click Additional Plug-ins

Correct Answer: A

QUESTION 6

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 7

Which two actions allow modification of the current displayed search result set? (Choose two.)

A. click on the Actions button

B. click on the Add Filter button

C. click on Quick Filter then select Show All

D. right-click on an item then select a filter option

E. click Search then select Manage Search Results

Correct Answer: BD

QUESTION 8

How are new reference sets created in IBM Security QRadar (QRadar)?

A. use the out-of-the-box tables

B. use the Reference SetMod.pl script

C. select New in the Rules Response Wizard

D. log into the QRadar Console and the PostgreSQL database

Correct Answer: C

QUESTION 9

Which component processes events against defined custom rules?

A. Magistrate

B. Flow Collector

C. Event Collector

D. Event Processor

Correct Answer: D

QUESTION 10

What does the command qchange_netsetup do?

A. It is used to upgrade the appliance\\'s network settings after the initial setup.

B. It is used to definethe MAC address of the interfaces during the initial setup.

C. It is used to change the appliance\\'s networking settings after the initial setup.

D. It is used to define the appliance\\'s networking settings during the initial setup.

Correct Answer: C

QUESTION 11

What is the last step to add aprotocol based log source?

A. on the Admin tab click Deploy Changes

B. from Log Sources, select Log Source Type, and click Save

C. from Log Sources, select Log Source Identifier, and click Save

D. on the Admin tab, select Actions and click Deploy Pull Configuration

Correct Answer: A

QUESTION 12

Which option is available for sharing offenses with non-IBM Security QRadar users?

A. provide URLt0 offense

B. invoke script forthird-party

Correct Answer: C

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

Need Help

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