A2150-195 Q&As

Assess: IBM Security QRadar V7.0 MR4 Fundamentals

Pass IBM A2150-195 Exam with 100% Guarantee

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

https://www.leads4pass.com/a2150-195.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

What are three regulatory reports standard in IBM Security QRadar V7.0 MR4? (Choose three.)

A. SOX

B. NERC

C. HIPAA

D. BASEL

E. GPG13

F. ISO-9001

Correct Answer: ABC

QUESTION 2

Which two pages or tabs are added to the IBM Security QRadar V7.0 MR4 (QRadar) Log Management product after it has been upgraded to QRadar SIEM? (Choose two.)

A. Admin

B. Reports

C. Offenses

D. Dashboard

E. Network Activity

Correct Answer: CE

QUESTION 3

An IBM Security GRadar V7.0 MR4 (QRadar) user has access to QRadar offenses. How do offenses appear in their My Offenses page?

A. Rules that have been created by the admin and that trigger an offense will also automatically put the triggered offense under their My Offenses page.

B. When the admin accesses the All Offenses option, they select Offenses and drag and drop them to their My Offenses page. Other QRadar users will no longer see the offenses that are put under their My Offenses page.

C. Anyone with access to the Offenses page will see all offenses. Under the My Offenses option, the person will see all

offenses that have been assigned to them for further analysis and processing. These offenses are assigned from the All Offenses page by choosing the Assign option from the Action menu.

D. Rules that trigger an offense can also be configured in such way that the resulting offense is automatically assigned to the QRadar user who is notified of the offense by e-mail. The rule is configured to send an e-mail and if the e-mail address matches an e-mail addresse of any of the QRadar users then this offense is automatically added to the My Offenses page of this user.

Correct Answer: C

QUESTION 4

Which function queries for offenses using specific criteria and displays those offenses that match the criteria?

A. Find

B. Search

C. Offense Lookup

D. Right-click > Navigate

Correct Answer: B

QUESTION 5

When using the Quick Filter feature in the Network Activity tab, which character must be used in front of special characters to indicate that the character is part of the search term?

A. +(plus)

B. -(minus)

C. \ (backslash)

D. ? (question mark)

Correct Answer: C

QUESTION 6

Which four fields are used when importing assets from a CSV file?

A. IP, Name, Weight. Description

B. IP. Port, MAC Address, Weight

C. IP, Port. MAC Address. Description

D. IP, User, Host Name, Service Version

Correct Answer: A

QUESTION 7

Which statement about log source identifiers is true for the same log source identifier to be used more than once?

A. It must always be unique.

B. It must be unique amongst the same protocol.

C. It must be unique amongst the same log source group.

D. It must be unique amongst log sources of the same type

Correct Answer: D

QUESTION 8

Which two formats can a user export flow data from the Network Activity tab? (Choose two.)

A. RTF

B. XML

C. PDF

D. CSV

E. HTML

Correct Answer: BD

QUESTION 9

How does a user access the Extract a Custom Property section from a paused event screen in the Log Activity tab?

A. Actions menu > Extract Property

B. Double-click the event > Extract Property

C. Actions menu > Show All > Extract Custom Property

D. Right-click on the event > Properties > Extract Property

Correct Answer: B

QUESTION 10

When working with rules, why do some rules specify QID values and some specify events?

A. Only low and high level categories can be specified within rules.

B. It is a matter of convention; QIDmap and event names are the same.

C. Event names are more precise; multiple events can be to the same QIDmap entry.

D. QID values are more precise; multiple QIDmap entries can be to same event name.

Correct Answer: D

QUESTION 11

Which tab displays correlated security alerts in IBM Security QRadar V7.0 MR4?

A. Admin

B. Reports

C. Offenses

D. Log Activity

Correct Answer: C

QUESTION 12

The remote directory field can be left blank for which protocol?

A. FTP

B. TFTP

C. SFTP

D. FTPS

Correct Answer: A

QUESTION 13

A flow is always based on what?

A. unicast and any cast traffic

B. unicast and broadcast traffic

C. unicast. multicast, and anycast traffic

D. unicast, broadcast, and multicast traffic

Correct Answer: C

QUESTION 14

What are two IT Security Frameworks? (Choose two.)

A. ITIL

B. SLA

C. COBIT

D. ISO 27001

E. Common Criteria

Correct Answer: CD

QUESTION 15

How does IBM Security QRadar V7.0 MR4 (QRadar) use the information from vulnerability scanners?

A. The internal QRadar vulnerability scanner provides reports for auditors.

B. The results are used by QRadar to automatically patch and update the asset.

C. The information can be used to determine if an asset is vulnerable to an exploit.

D. Systems on which vulnerabilities are found are automatically monitored more closely.

Correct Answer: C