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.certbus.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

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 2

Everyone involved in a forensic analysis is now convinced that account management events involving promotion of accounts to AD administrator groups must be reported on daily. What is the most efficient method to accomplish this in IBM Security QRadar V7.0 MR4 (QRadar)?

A. Such a report requires additional parsing of events using extra custom properties and then including these properties in a manual report.

B. A new rule must be created which triggers an offense every time an account is assigned to an AD administrator group. By examining the event in detail it can be determined if this was really anoffense or not.

C. The detailed search that the user has used to identify the relevant events must be saved first. Once it is saved, then it can be reused on demand, and it can also be used to build a custom report which can then be scheduled.

D. Automation or scripting is out of the question. The user has to repeat the analysis manually every time a similar incident occurs. The best the user can do is document the steps so that it is repeatable by anyone with access to the QRadar interface.

Correct Answer: C

QUESTION 3

What is used to parse an event (log record) in IBM Security QRadar V7.0 MR4?

A. CRE

B. DSMs

C. Qidmaps

D. Protocols

Correct Answer: B

QUESTION 4

Which two components are only part of the IBM Security QRadar V7.0 MR4 (QRadar) SIEM and cannot be found in the QRadar Log Management? (Choose two.)

A. Console

B. Flow Collector

C. Event Collector

D. Event Processor

E. Offense Manager

Correct Answer: BE

QUESTION 5

A user is complaining of slow traffic on a specific network segment. An administrator is investigating the source of the congestion using the IBM Security QRadar V7.0 MR4 (QRadar) Dashboard workspace named Top Applications. The

administrator has drilled down into the details of a traffic spike and is now on the Details tab.

If the administrator double-clicks on the top application in the list, and then sorts by the Total Bytes column, what information is displayed regarding the source and destination IPs of the devices?

A. The devices causing the least traffic for all applications

B. The devices causing the most traffic for all applications

C. The devices causing the least traffic for the selected application

D. The devices causing the most traffic for the selected application

Correct Answer: D

QUESTION 6

What are three of the basic pre-built Dashboard Overview types? (Choose three.)

A. Administrator

B. Network Overview

C. Server Monitoring

D. System Monitoring

E. Application Performance

F. Threat and Security Monitoring

Correct Answer: BDF

QUESTION 7

What is the Identity Information section used for?

A. To show which rules match an event

B. To show which log source an event belongs to

C. To show the High/Low level category of an event

D. To show the user information relative to an event

Correct Answer: D

QUESTION 8

What does it mean if events are coming in as stored?

A. The events are not mapped to an existing QID map.

B. The events are being captured and parsed by a DSM.

C. The events are being captured but not being parsed by a DSM.

D. The events are being stored on disk and will be parsed by a DSM later.

Correct Answer: C

QUESTION 9

Given the IBM Security Framework, IBM Security QRadar V7.0 MR4 fits into which two security domains? (Choose two.)

A. Data

B. People and Physical Security

C. Infrastructure, Network, or Endpoint

D. Applications and Application Security

E. IT Security/Compliance Analytics and Reporting

Correct Answer: CE

QUESTION 10

On the Offense Summary page, which filter is executed when the Flows icon or the link with the number of flows is clicked on?

A. A flow filter with all flows matching the source IP address

B. A flow filter with all flows matching the destination IP address

C. A flow filter with the Custom Rule Engine rule(s) for the last 24 hours

D. A flow filter with the Custom Rule Engine rule(s) for the duration of the offense

Correct Answer: D

QUESTION 11

On the Offense summary page, which filter is executed when the Events icon or the link with the number of events is clicked?

A. An event filter with all events matching the source IP address

B. An event filter with all events matching the destination IP address

C. An event filter with the Custom Rule Engine rule(s) for the last 24 hours

D. An event filter with the Custom Rule Engine rule(s) for the duration of the offense

Correct Answer: D

QUESTION 12

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 13

What is a prerequisite to create a report that contains at least one bar chart?

A. Have a color display and enable the JPanel

B. Have the role assigned to create (graphical) reports

C. Choose a search that has accumulated properties for the report

D. The search contained in the report must aggregate the results at least along one property

Correct Answer: D

QUESTION 14

Which flow direction would a user specify in order to see flows that are solely related to traffic that originates from the internal networks to external networks?

A. L2L

B. R2L

C. L2R

D. R2R

Correct Answer: C

QUESTION 15

What must be done in order to save a search criteria as a quick search?

A. Select Save Criteria and select My Dashboard

B. Select Save Criteria in the New/Edit Search dialog

C. Right-click on the filter and select Save as Quick Search

D. Select Save Criteria and select Include in my Quick Searches

Correct Answer: D

A2150-195 Practice Test A2150-195 Exam Questions A2150-195 Braindumps