C1000-018 Q&As

IBM QRadar SIEM V7.3.2 Fundamental Analysis

Pass IBM C1000-018 Exam with 100% Guarantee

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

https://www.leads4pass.com/c1000-018.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

An analyst wants to analyze the long-term trending of data from a search. Which chart would be used to display this data on a dashboard?

A. Bar Graph

B. Time Series chart

C. Pie Chart

D. Scatter Chart

Correct Answer: A

Explanation:

You could use a bar graph if you want to track change over time as long as the changes are significant.

Reference: https://www.statisticshowto.com/probability-and-statistics/descriptive-statistics/bar-chart-bargraph-examples/

QUESTION 2

An analyst needs to find events coming from unparsed log sources in the Log Activity tab. What is the log source type of unparsed events?

A. SIM Generic

B. SIM Unparsed

C. SIM Error

D. SIM Unknown

Correct Answer: A

Explanation:

SIM Generic log source or by using the Event is Unparsed filter.

Reference: https://www.ibm.com/docs/en/qsip/7.3.3?topic=problems-troubleshooting-dsms

QUESTION 3

How many normalized timestamp field(s) does an event contain?

A. 2

B. 3

C. 4

D. 1

Correct Answer: B

Explanation:

There are 3 timestamp fields on events in Qradar.

Reference: https://www.ibm.com/mysupport/s/question/0D50z00006PEG2mCAH/why-do-i-see-differenttime-stamps-for-qradar-events?language=en_US

QUESTION 4

An analyst wants to view information about repeated offenders and IP addresses that generate many attacks or are subject to many attacks.

What should the analyst choose from the navigation options in the Offense tab?

A. By Event Category or By Event Source

B. By Source IP or By Destination IP

C. By Log Source IP or By Event Source

D. By Event or By Flows

Correct Answer: B

Explanation:

Use the navigation options on the left to view the offenses from different perspectives. For example, select

By Source IP or By Destination IP.

Reference: https://www.ibm.com/docs/en/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_users_guide.pdf

QUESTION 5

An analyst is encountering a large number of false positive results. Legitimate internal network traffic contains valid flows and events which are making it difficult to identify true security incidents.

What can the analyst do to reduce these false positive indicators?

A. Create X-Force rules to detect false positive events.

B. Create an anomaly rule to detect false positives and suppress the event.

C. Filter the network traffic to receive only security related events.

D. Modify rules and/or Building Block to suppress false positive activity.

Correct Answer: C

QUESTION 6

Which filter would an analyst apply in the Log Activity tab to get a list of log sources not reporting to QRadar?

A. Log source status does not equal active

B. Custom rule equals device stopped sending events

C. Log source type does not equal active

D. Log source status does not equal error

Correct Answer: A

QUESTION 7

Where can an analyst working with Offenses add a regular expression test into an existing rule?

A. Left

B. Top

C. Bottom

D. Right

Correct Answer: B

QUESTION 8

An analyst needs to investigate an Offense and navigates to the attached rule(s).

Where in the rule details would the analyst investigate the reason for why the rule was triggered?

A. Rule response limiter

B. List of test conditions

C. Rule actions

D. Rule responses

Correct Answer: A

QUESTION 9

How does an analyst view the base64 encoded string of an event\\'s raw payload that contains unprintable characters?

A. Copy the raw payload and use an external tool to view base64 data

B. Right click on the event –andgt; view base64 data

C. Log Activity –andgt; Under Payload Information, click base64 tab

D. Admin –andgt; Under Payload Information, click base64 tab

Correct Answer: B

QUESTION 10

An analyst needs to perform a Quick search to find events under the Log Activity tab that contains an ‘exe’ file during a certain time period.

How can the analyst do this?

A. On the Search bar select Quick Filter, then insert filter criteria for ‘/*.exe/’ and then select a time interval from the view option\\'s drop down.

B. Select Search – New Search from the menu bar, then select all the search criteria required from the UI options provided.

C. Select Quick Searches on the menu bar, then go through the list of saved searches available to see if one already exists, that can be altered.

D. On the Search bar select Quick Filter, insert: ‘exe, last 1 hour’ into the filter criteria, then click Search.

Correct Answer: A

Reference: https://www.ibm.com/support/pages/searching-your-qradar-data-efficiently-part-1-quick-filters