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.passapply.com/c1000-018.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

While creating a new custom property, which is a valid property type selection?

A. Flow Based

B. Event Based

C. AQL Based

D. Regular Expressions Based

Correct Answer: D

QUESTION 2

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 3

An analyst is investigating an Offense and has found that the issue is that a firewall appears to be misconfigured and has permitted traffic that should be prevented to pass.

As part of the firewall rule change process, the analyst needs to send the offense details to the firewall team to demonstrate that the firewall permitted traffic that should have been blocked.

How would the analyst send the Offense summary to an email mailbox?

A. Find the CRE Event in the Log Activity tab, open the event detail and select ‘Email linked Offense details’ from the ‘Action’ menu.

B. Search for the events linked to the Offense in the Log Activity tab; Select all events and copy them using CTRL-C then paste into an email client.

C. Open the Offense in the Offenses tab, select 'Email' from the 'Action' menu item and, optionally, add some extra information.

D. Identify the Offense in the Offense list, right click on the Offense and select 'Custom Action Script'; 'Offense Mailer'

Correct Answer: B

QUESTION 4

What is the difference between a Quick Search and an Advanced Search?

A. An Advanced Search uses a saved search, while a Quick Search uses a query language.

B. A Quick Search displays results by column, while an Advanced Search displays results by Category.

C. A Quick Search uses a saved search, while an Advanced Search requires a query language.

D. An Advanced Search displays results by Category, while a Quick Search displays results by column.

Correct Answer: C

Explanation:

Quick Search

Use the search box to quickly find documents by any keyword or criteria. Here you can also view and reuse your most recent and saved searches.

Advanced Searching

The advanced search allows you to build structured queries using the Jira Query Language.

Reference: https://support.netdocuments.com/hc/en-us/articles/206955786-Quick-Search

https://confluence.atlassian.com/jirasoftwareserver/advanced-searching-939938733.html

QUESTION 5

An analyst has observed that for a particular user, authentication to an organization\\'s critical server is different than the normal access pattern.

How can the analyst verify that all the authentications initiated from the user are valid?

A. Perform a search with filter Destination IP group by Username, then validate the Username

B. Perform a search with filter Source IP group by Username, then validate the Username

C. Perform a search with filter Username group by Source IP, then validate the Destination IP

D. Perform a search with filter Username group by Source IP, then validate the Source IP

Correct Answer: B