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

What information is included in flow details but is not in event details?

A. Log source information

B. Number of bytes and packets transferred

C. Network summary information

D. Magnitude information

Correct Answer: C

Explanation:

Flows represent network activity by normalizing IP addresses, ports, byte and packet counts, and other

data, into flow records, which effectively are records of network sessions between two hosts.

Reference: https://www.ibm.com/docs/en/qsip/7.3.2?topic=overview-qradar-events-flows

QUESTION 2

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 3

An analyst needs to use a new custom property in a rule.

What must be the mandatory characteristic of the custom property?

A. It must be shared.

B. It must be boolean.

C. It must be stored.

D. It must be extracted.

Correct Answer: B

QUESTION 4

From which tab in QRadar SIEM can an analyst search vulnerability data and remediate vulnerabilities?

A. Log Activity

B. Dashboard

C. Assets

D. Admin

Correct Answer: C

Explanation:

When IBM Security QRadar Vulnerability Manager is enabled, you can perform vulnerability assessment tasks on the Vulnerabilities tab. From the Assets tab, you can run IBM Security QRadar Vulnerability Manager scans on selected assets.

Reference: http://www.siem.su/docs/ibm/Administration_and_introduction/User_Guide.pdf

QUESTION 5

An analyst for a particular offense needs to investigate to understand the breakdown of the offense details.

How can the analyst do this?

A. Look at the magnitude information and its breakdown.

B. Look at all the event QIDs attached to the offense.

C. View the attack path of the offense.

D. Look at the list of categories, event low level categories and the events attached.

Correct Answer: A