C1000-018$^{\text{Q\&As}}$

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.pass2lead.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

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 2

An analyst aims to improve the detection capabilities on all the Offense rules. QRadar SIEM has a tool that allows the analyst to update all the Building Blocks related to Host and Port Definition in a single page.

How is this accomplished?

A. Admin –andgt; Reference Set management

B. Assets –andgt; Asset Profiles

C. Assets –andgt; Server Discovery

D. Admin –andgt; Asset Profile Configuration

Correct Answer: C

QUESTION 3

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

QUESTION 4

What is displayed in the status bar of the Log Activity tab when streaming events?

A. Average number of results that are received per second.

B. Average number of results that are received per minute.

C. Accumulated number of results that are received per second.

D. Accumulated number of results that are received per minute.

Correct Answer: A

Explanation:

Status bar

When streaming events, the status bar displays the average number of results that are received per second.

Reference: https://www.ibm.com/docs/en/qradar-on-cloud?topic=investigation-log-activity-tab-overview

QUESTION 5

What could be a possible reason that events are routed directly to storage by the custom rule engine (CRE)?

A. System is under high load

B. A rule is processing 20,000 EPS

C. Event normalization issue

D. Event Parsing issue

Correct Answer: A