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

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 2

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 3

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 4

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 5

There are 5 authentication servers that report to different Event Processors. There is a requirement to generate an Offense if there are 5 consecutive failed logins detected across any of the 5 Event Processors.

Which type of rule should the analyst create?

A. Global Rule

B. Persistent Rule

C. Local Rule

D. Offense Rule

Correct Answer: A

Explanation:

Global rules These rules use the Any domain modifier and run across all tenants.

Reference: https://www.ibm.com/docs/en/SS42VS_7.3.2/com.ibm.qradar.doc/b_qradar_admin_guide.pdf

C1000-018 Practice Test C1000-018 Study Guide C1000-018 Braindumps