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 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 2

What are the different flow types in QRadar?

A. L2L, L2R, R2R, R2L

B. Standard, Type A, Type B, Type C

C. Standard, Type 1, Type2, Type 3

D. Type 1, Type 2, Type 3, Type 4

Correct Answer: B

Reference: https://docplayer.net/19071559-Qradar-siem-7-2-flows-overview.html

QUESTION 3

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 4

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

QUESTION 5

When ordering these tests in an event rule, which of them is the best test to place at the top of the list for rule performance?

A. When the source is [local or remote]

B. When the destination is [local or remote]

C. When the event(s) were detected by one or more of [these log sources]

D. When an event matches all of the following [Rules or Building Blocks]

Correct Answer: A