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 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 2

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 3

Which QRadar component stored Offenses?

A. Console

B. Data Node

C. Event Processor

D. Event Collector

Correct Answer: B

Explanation: QRadar Data Node Data Nodes enable new and existing QRadar deployments to add storage and processing capacity on demand as required. Data Nodes help to increase the search speed in your deployment by providing more hardware resources to run search queries on.

Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=overview-qradar-components

QUESTION 4

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

QUESTION 5

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