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

IBM QRadar SIEM V7.3.2 Fundamental Analysis

QUESTION 1

What information is displayed in the default “Log Activity” page? (Choose two.)

A. QID

B. Protocol

C. Qmap

D. Log Source

E. Event Name

Correct Answer: DE

QUESTION 2

Where can an analyst working with Offenses add a regular expression test into an existing rule?

A. Left

B. Top

C. Bottom

D. Right

Correct Answer: B

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

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 5

What is the intent of the magnitude of an offense?

A. It measures the age of the event attached to the offense.

B. It measures the age of the offense.

C. It measures the importance of the offense.

D. It measures the importance of the event attached to the offense.

Correct Answer: B

Explanation:

The age of the offense.

Reference: https://www.ibm.com/docs/en/qsip/7.3.3?topic=management-offense-prioritization