DUMPSBOSS.

IBM QRadar SIEM V7.3.2 Fundamental Analysis

IBM C1000-018

Version Demo

Total Demo Questions: 9

Total Premium Questions: 60

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

While creating a new custom property, which is a valid property type selection?

A. Flow Based

B. Event Based

C. AQL Based

D. Regular Expressions Based

ANSWER: D

QUESTION NO: 2

An analyst is investigating a series of events that triggered an Offense. The analyst wants to get more detailed information about the IP address from the reference set.

How can the analyst accomplish this?

A. Click on Searches tab then perform an Advanced Search

B. Click on Log Activity tab then perform a Quick Search

C. Click on Searches tab then perform a Quick Search

D. Click on Log Activity tab then perform an Advanced Search

ANSWER: A

QUESTION NO: 3

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

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 NO: 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

ANSWER: A

Explanation:

Reference: https://www.ibm.com/docs/en/qradar-on-cloud?topic=appliances-expensive-custom-rule-found

QUESTION NO: 5

Which use case type is appropriate for VPN log sources? (Choose two.)

A. Advanced Persistent Threat (APT)

B. Insider Threat

C. Critical Data Protection

D. Securing the Cloud

ANSWER: A B

Explanation:

Reference: https://www.ibm.com/docs/en/dsm?topic=management-threat-use-cases-by-log-source-type

QUESTION NO: 6

Which are the supported protocol configurations for Check Point integration with QRadar? (Choose two.)

A. CHECKPOINT REST API

B. SYSLOG

C. JDBC

D. SFTP

E. OPSEC/LEA

ANSWER: B E

QUESTION NO: 7

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

A. QID

B. Protocol

C. Qmap

D. Log Source

E. Event Name

ANSWER: D E

Explanation:

By default, the Log Activity tab displays the following parameters when you view normalized events:

Event Name	Specifies the normalized name of the event.
Log Source	Specifies the log source that originated the event. If there are multiple log sources that are associated with this event, this field specifies the term Multiple and the number of log sources.

Reference: https://www.juniper.net/documentation/en_US/jsa7.3.1/jsa-users-guide/topics/concept/concept-jsa-user-log-activity-monitoring.html

QUESTION NO: 8

When an analyst sees the system notification “The appliance exceeded the EPS or FPM allocation within the last hour”, how does the analyst resolve this issue? (Choose two.)

A. Delete the volume of events and flows received in the last hour.

B. Adjust the license pool allocations to increase the EPS and FPM capacity for the appliance.

C. Tune the system to reduce the volume of events and flows that enter the event pipeline.

D. Adjust the resource pool allocations to increase the EPS and FPM capacity for the appliance.

E. Tune the system to reduce the time window from 60 minutes to 30 minutes.

ANSWER: B C

Explanation:

User response

Adjust the license pool allocations to increase the EPS and FPM capacity for the appliance. Tune the system to reduce the volume of events and flows that enter the event pipeline.

Reference: https://www.ibm.com/docs/en/qsip/7.3.2?topic=appliances-maximum-events-flows-reached

QUESTION NO: 9

Which filter would an analyst apply in the Log Activity tab to get a list of log sources not reporting to QRadar?

A. Log source status does not equal active

B. Custom rule equals device stopped sending events

C. Log source type does not equal active

D. Log source status does not equal error

ANSWER: A