DUMPSARENA

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://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 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

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: 2

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: 3

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: 4

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: 5

An analyst needs to perform Offense management.

In QRadar SIEM, what is the significance of “Protecting” an offense?

A. Escalate the Offense to the QRadar administrator for investigation.

B. Hide the Offense in the Offense tab to prevent other analysts to see it.

C. Prevent the Offense from being automatically removed from QRadar.

D. Create an Action Incident response plan for a specific type of cyber attack.

ANSWER: C

Explanation:

Protecting offenses:

You might have offenses that you want to retain regardless of the retention period. You can protect offenses to prevent them from being removed from QRadar after the retention period has elapsed.

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

QUESTION NO: 6

An analyst noticed that from a particular subnet (203.0.113.0/24), all IP addresses are simultaneously trying to reach out to the company's publicly hosted FTP server. The analyst also noticed that this activity has resulted in a Type B Superflow on the Network Activity tab.

Under which category, should the analyst report this issue to the security administrator?

A. Syn Flood

B. Port Scan

C. Network Scan

D. DDoS

ANSWER: A

QUESTION NO: 7

An analyst observed a port scan attack on an internal network asset from a remote network.

Which filter would be useful to determine the compromised host?

A. Any IP

B. Destination IP [Indexed]

C. Source or Destination IP

D. Source IP [Indexed]

ANSWER: A

QUESTION NO: 8

An auditor has requested a report for all Offenses that have happened in the past month. This report generates at the end of every month but the auditor needs to have it for a meeting that is in the middle of the month.

What will happen to the scheduled report if the analyst manually generates this report?

A. The scheduled report needs to be reconfigured.

B. The analyst needs to delete the scheduled report and create a new one.

C. The report will get duplicated so the analyst can then run one manually.

D. The report still generates on the schedule initially configured.

ANSWER: B

Explanation:

Shared schedules must be deleted manually using the Schedules page in the web portal or the Shared Schedules folder in Management Studio. If you delete a shared schedule that is in use, all references to it are replaced with report-specific schedules.

If you delete a shared schedule that is used by multiple reports and subscriptions, the report server will create individual schedules for each report and subscription that previously used the shared schedule. Each new individual schedule will contain the date, time, and recurrence pattern that was specified in the shared schedule. Note that Reporting Services does not provide central management of individual schedules. If you delete a shared schedule, you will now have to maintain the schedule information for each individual item.

Reference: https://docs.microsoft.com/en-us/sql/reporting-services/subscriptions/create-modify-and-delete-schedules?view=sql-server-ver15

QUESTION NO: 9

What is the purpose of Anomaly detection rules?

A. They inspect other QRadar rules.

B. They detect if QRadar is operating at peak performance and error free.

C. They detect unusual traffic patterns in the network from the results of saved flow and events.

D. They run past events and flows through the Custom Rules Engine (CRE) to identify threats or security incidents that already occurred.

ANSWER: C

Explanation:

Reference: https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-users-guide/topics/concept/concept-jsa-user-anomaly-detection-rules.html#:~:text=Anomaly%20detection%20rules%20test%

20the,patterns%20occur%20in%20your%20network.&text=Typically%20the%20search%20needs%20to,%2C%20thresholds%2C%20or%20behavior%20changes