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.certbus.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

The administrator had set up several scheduled reports that can be executed by analysts every Monday, and the first day of each month. On Thursday, an executive requests one of the weekly reports.

If the analyst executes the report on Thursday, what information will the report contain?

A. Data from Monday to Sunday from the previous week.

B. Data from Thursday from the previous week to Wednesday from the current week.

C. Data from Monday to Thursday from the current week.

D. Data from Monday to Wednesday from the current week.

Correct Answer: C

QUESTION 2

From which tab in QRadar SIEM can an analyst search vulnerability data and remediate vulnerabilities?

A. Log Activity

B. Dashboard

C. Assets

D. Admin

Correct Answer: C

Explanation:

When IBM Security QRadar Vulnerability Manager is enabled, you can perform vulnerability assessment

tasks on the Vulnerabilities tab. From the Assets tab, you can run IBM Security QRadar Vulnerability

Manager scans on selected assets.

Reference: http://www.siem.su/docs/ibm/Administration_and_introduction/User_Guide.pdf

QUESTION 3

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.

Correct Answer: BC

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 4

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.

Correct 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 5

Why would an analyst update host definition building blocks in QRadar?

A. To reduce false positives.

B. To narrow a search.

C. To stop receiving events from the host.

D. To close an Offense

Correct Answer: D

Explanation:

Building blocks to reduce the number of offenses that are generated by high volume traffic servers.

Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=phase-qradar-building-blocks

QUESTION 6

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]

Correct Answer: A

QUESTION 7

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

Correct Answer: A

QUESTION 8

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 9

What is the reason for this system notification?

A. Deny ntpdate communication on port 423.

B. Deny ntpdate communication on port 223.

C. Deny ntpdate communication on port 323.

D. Deny ntpdate communication on port 123.

Correct Answer: D

Explanation:

38750129 - Time synchronization to primary or Console has failed.

The managed host cannot synchronize with the console or the secondary HA appliance

cannotsynchronize with the primary appliance.

Administrators must allow ntpdatecommunication on port 123.

Reference: https://www.coursehero.com/file/p35nlom9/Process-exceeds-allowed-run-time-38750122Process-takes-too-long-to-execute-The/

QUESTION 10

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

Correct Answer: A