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.pass4itsure.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 investigating a user\\'s activities and sees that they have repeatedly executed an action which triggers a rule that emails the SOC team and creates an Offense, indexed on Username.

The SOC team complained that they have received 15 emails in the space of 10 minutes, but the analyst can only see one Offense in the Offenses tab.

How is this explained?

A. There is a Rule Limiter on the Rule Action which creates the Offense, this should also be applied to the Rule Responses.

B. This is expected behavior, the offense will contain the information about all 15 events.

C. An Offense rule has been configured to send multiple emails upon Offense creation.

D. The Custom Rules Engine (CRE) has fallen behind and the additional Offenses will be created shortly.

Correct Answer: C

QUESTION 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

Correct Answer: BE

QUESTION 3

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.

Correct Answer: C

Reference: https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-users-guide/topics/concept/conceptjsa-user-anomaly-detection-rules.html#:~:text=Anomaly%20detection%20rules%20test%20the,patterns%20occur%20in%20your%20network.andtext=Typically%20the%20search%20needs%20to,%2C%

20thresholds%2C%20or%20behavior%20changes

QUESTION 4

An analyst is performing an investigation regarding an Offense. The analyst is uncertain to whom some of the external destination IP addresses in List of Events are registered.

How can the analyst verify to whom the IP addresses are registered?

A. Right-click on the destination address, More Options, then Navigate, and then Destination Summary

B. Right-click on the destination address, More Options, then IP Owner

C. Right-click on the destination address, More Options, then Information, and then WHOIS Lookup

D. Right-click on the destination address, More Options, then Information, and then DNS Lookup

Correct Answer: A

Explanation:

Navigate > View Destination Summary Displays the offenses that are associated with the selected

destination IP address.

Reference: https://www.ibm.com/docs/en/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_users_guide.pdf

QUESTION 5

An analyst needs to review additional information about the Offense top contributors, including notes and annotations that are collected about the Offense.

Where can the analyst review this information?

A. In the top portion of the Offense Summary window

B. In the bottom portion of the Offense main view

C. In the bottom portion of the Offense Summary window

D. In the top portion of the Offense main view

Correct Answer: C

Explanation:

In the bottom portion of the Offense Summary window, review additional information about the offense top contributors, including notes and annotations that are collected about the offense.

Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=investigations-investigating-offense-by-using summary-information

QUESTION 6

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 7

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.

Correct 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-anddelete-schedules?view=sql-server-ver15

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

After working with an Offense, an analyst set the Offense as hidden. What does the analyst need to do to view the Offense at a later time?

A. In the all Offenses view, at the top of the view, select “Show hidden” from the “Select an option” drop-down.

B. Search for all Offenses owned by the analyst.

C. Click Clear Filter next to the “Exclude Hidden Offenses”.

D. In the all Offenses view, select Actions, then select show hidden Offenses.

Correct Answer: C

Explanation:

To clear the filter on the offense list, click Clear Filter next to the Exclude Hidden Offenses search

parameter.

Reference: https://www.ibm.com/docs/fi/qradar-on-cloud?topic=actions-showing-hidden-offenses

QUESTION 10

What is the maximum time period for 3 subsequent events to be coalesced?

A. 10 minutes

B. 10 seconds

C. 5 minutes

D. 60 seconds

Correct Answer: B

Explanation:

Event coalescing starts after three events have been found with matching properties within a 10 second

window.

Reference: https://www.ibm.com/support/pages/qradar-how-does-coalescing-work-qradar