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

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 2

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 3

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 4

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

Correct Answer: A

QUESTION 5

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