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.passapply.com/c1000-018.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official Exam Center

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

An analyst has observed that for a particular user, authentication to an organization\\'s critical server is different than the normal access pattern.

How can the analyst verify that all the authentications initiated from the user are valid?

A. Perform a search with filter Destination IP group by Username, then validate the Username

B. Perform a search with filter Source IP group by Username, then validate the Username

C. Perform a search with filter Username group by Source IP, then validate the Destination IP

D. Perform a search with filter Username group by Source IP, then validate the Source IP

Correct Answer: B

QUESTION 2

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 3

What is the intent of the magnitude of an offense?

A. It measures the age of the event attached to the offense.

B. It measures the age of the offense.

C. It measures the importance of the offense.

D. It measures the importance of the event attached to the offense.

Correct Answer: B

Explanation:

The age of the offense.

Reference: https://www.ibm.com/docs/en/qsip/7.3.3?topic=management-offense-prioritization

QUESTION 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.

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 5

How does an analyst view the base64 encoded string of an event\\'s raw payload that contains unprintable characters?

A. Copy the raw payload and use an external tool to view base64 data

B. Right click on the event –andgt; view base64 data

C. Log Activity –andgt; Under Payload Information, click base64 tab

D. Admin –andgt; Under Payload Information, click base64 tab

Correct Answer: B

Latest C1000-018 Dumps C1000-018 Exam Questions C1000-018 Braindumps