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.geekcert.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 for a particular offense needs to investigate to understand the breakdown of the offense details.

How can the analyst do this?

A. Look at the magnitude information and its breakdown.

B. Look at all the event QIDs attached to the offense.

C. View the attack path of the offense.

D. Look at the list of categories, event low level categories and the events attached.

Correct Answer: A

QUESTION 2

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 3

Which statement about False Positive Building Blocks applies?

Using False Positive Building Blocks:

A. helps to prevent unwanted alerts, but there is no effect on performance.

B. helps to prevent unwanted alerts, and reduces the performance impact of testing rules that do not need to be tested.

C. has no impact on unwanted alerts, but it does reduce the performance impact of testing rules that do not need to be tested.

D. has no impact on unwanted alerts, or performance.

Correct Answer: A

Reference: https://community.carbonblack.com/t5/Knowledge-Base/Cb-Defense-UnderstandingEliminating-Unwanted-Alerts/ta-p/44924

QUESTION 4

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 5

There are 5 authentication servers that report to different Event Processors. There is a requirement to generate an Offense if there are 5 consecutive failed logins detected across any of the 5 Event Processors.

Which type of rule should the analyst create?

A. Global Rule

B. Persistent Rule

C. Local Rule

D. Offense Rule

Correct Answer: A

Explanation:

Global rules These rules use the Any domain modifier and run across all tenants.

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