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

QUESTION 1

An analyst needs to use a new custom property in a rule.

What must be the mandatory characteristic of the custom property?

A. It must be shared.

B. It must be boolean.

C. It must be stored.

D. It must be extracted.

Correct Answer: B

QUESTION 2

Which consideration should be given to the position of rule tests that evaluate regular expressions (Regex tests)?

A. They can only be used in Building Blocks to ensure they are evaluated as infrequently as possible.

B. They are usually the most specific. As such, they should appear first in the order.

C. They are usually the most expensive. As such, they should appear last in the order.

D. They are stateful tests. As such QRadar automatically evaluates them last.

Correct Answer: A

Reference: https://towardsdatascience.com/everything-you-need-to-know-about-regular-expressions8f622fe10b03

QUESTION 3

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 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

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]

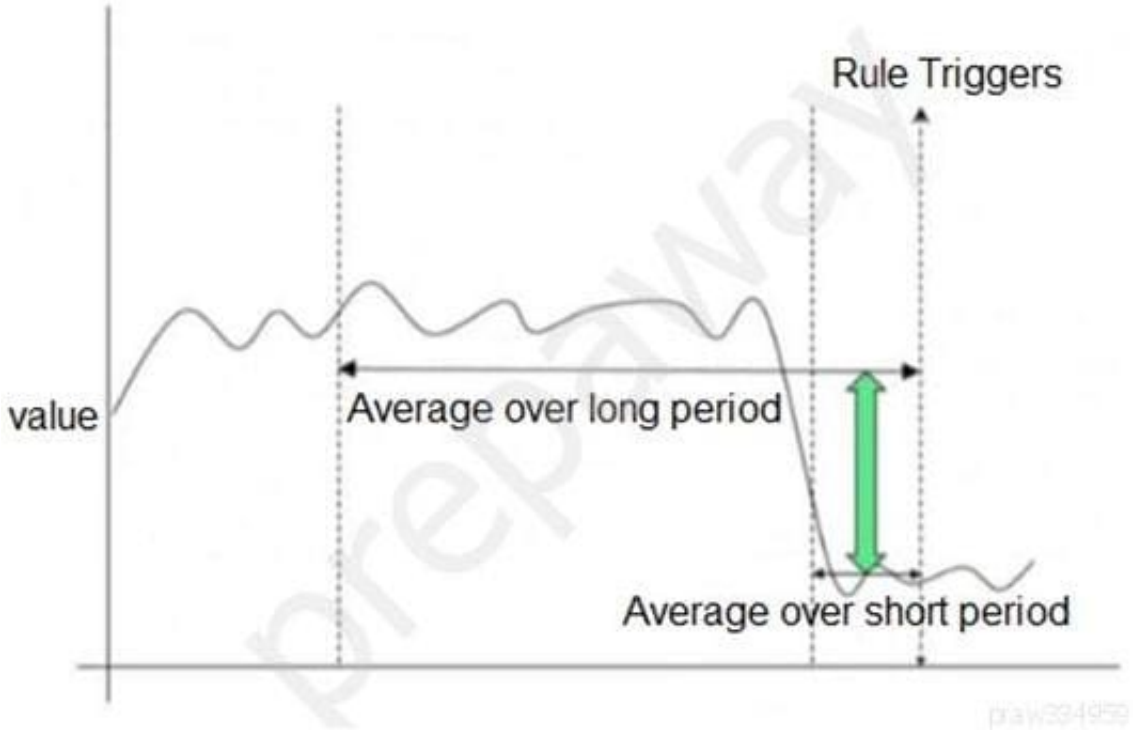
C. Source or Destination IP

D. Source IP [Indexed]

Correct Answer: A

QUESTION 6

The graph below shows a time series of a value. A rule has been created which will trigger at the indicated point.



Which type of QRadar rule has been used?

A. Common Rule

B. Threshold Rule

C. Behavioral Rule

D. Anomaly Rule

Correct Answer: B

QUESTION 7

Where can an analyst working with Offenses add a regular expression test into an existing rule?

A. Left

B. Top

C. Bottom

D. Right

Correct Answer: B

QUESTION 8

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 9

An analyst needs to find events coming from unparsed log sources in the Log Activity tab. What is the log source type of unparsed events?

A. SIM Generic

B. SIM Unparsed

C. SIM Error

D. SIM Unknown

Correct Answer: A

Explanation:

SIM Generic log source or by using the Event is Unparsed filter.

Reference: https://www.ibm.com/docs/en/qsip/7.3.3?topic=problems-troubleshooting-dsms

QUESTION 10

An analyst has to perform an export of events within a timeframe, but not all the columns are present in the log view for the time period the analyst has selected. The analyst only needs specific columns exported for an external analysis.

How can the analyst accomplish this task?

A. Edit the search and select the extra columns, then export the result with Action/Export to XML/Full Export. This export is only supported in XML.

B. Edit the search and select the extra columns, then export the result with Action/Export to XML/Visible Columns. This export is only supported in XML.

C. Edit the search result and select the extra columns, then export the result with Action/Export to CSV/ Full Export.

D. Edit the search result and select the extra columns, then export the result with Action/Export to CSV/ Visible Columns.

Correct Answer: D

Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=investigation-exporting-events