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.leads4pass.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 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

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 3

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 4

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 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

C1000-018 PDF Dumps C1000-018 Practice Test C1000-018 Study Guide