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

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

QUESTION 1

From which tab in QRadar SIEM can an analyst search vulnerability data and remediate vulnerabilities?

A. Log Activity

B. Dashboard

C. Assets

D. Admin

Correct Answer: C

Explanation:

When IBM Security QRadar Vulnerability Manager is enabled, you can perform vulnerability assessment tasks on the Vulnerabilities tab. From the Assets tab, you can run IBM Security QRadar Vulnerability Manager scans on selected assets.

Reference: http://www.siem.su/docs/ibm/Administration_and_introduction/User_Guide.pdf

QUESTION 2

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 3

An analyst needs to investigate an Offense and navigates to the attached rule(s).

Where in the rule details would the analyst investigate the reason for why the rule was triggered?

A. Rule response limiter

B. List of test conditions

C. Rule actions

D. Rule responses

Correct Answer: A

QUESTION 4

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 5

While creating a new custom property, which is a valid property type selection?

A. Flow Based

B. Event Based

C. AQL Based

D. Regular Expressions Based

Correct Answer: D