SAMPLE QUESTIONS for:
Test C1000-018, IBM QRadar SIEM V7.3.2 Fundamental Analysis

Note: The **bolded** response option is the correct answer.

Question C1000-018.1.2.8

A QRadar user needs to enable/disable few of the rules. Which role permission is required for enabling and disabling the rule?

A. Offenses > Maintain CRE Rules
B. Offenses > Maintain Use Cases
C. Offenses > Toggle Custom Rules
D. Offenses > Maintain Custom Rules

Question C1000-018.1.2.10

Which mode provides an analyst with a real-time view of their current event activity by displaying a continuously updating sample of the most recent events?

A. Live Events
B. Real Time (displaying)
C. Real Time (streaming)
D. Last Interval (auto refresh)

Question C1000-018.2.3.4

How does an analyst determine which rules are most active in generating Offenses?

A. Assets -> Rules -> click Offense Count to reorder the column in ascending order
B. Admin -> Rules -> click Offense Count to reorder the column in descending order
C. Offenses -> Rules -> click Offense Count to reorder the column in ascending order
D. Offenses -> Rules -> click Offense Count to reorder the column in descending order

---
Question C1000-018.2.3.6

What is the maximum length of the Notes field in the Offenses tab?

A. 1000
B. 1200
C. 1500
D. 2000

Question C1000-018.2.3.9

How many active Offenses can be in the QRadar system?

A. 2500
B. 3000
C. 3500
D. 4000

Question C1000-018.2.11.3

The analyst needs to export an Offense outside QRadar to make a report of the incident.
Which export format is supported? (Choose two)

A. TSV (Tab Separated Values)
B. CSV (Comma Separated Values)
C. Fixed Field Text (Plain Text)
D. XML (Extensible Markup Language)
E. HTML (Hypertext Markup Language)

Question C1000-018.2.11.6

What period of inactivity causes an offense to go into dormant state?

A. 5 days
B. 5 hours
C. 30 days
D. 30 minutes

Question C1000-018.3.2.3

A high number of Offenses are being generated for a specific event type.
What can the analyst do to investigate why Offenses are being created?

A. Review the health notification Offense rules.
B. Review the rules used in creating the Offense.
C. Review the Offense and enable the Offense high event rules.
D. Review the log sources and enable the anomaly Offense detection rules.

Question C1000-018.5.6.2

Which time stamp is used to determine whether events are being queued in the event pipeline for performance or licensing reasons?

A. Start Time
B. Device Time
C. Storage Time
D. Log Source Time