SAMPLE QUESTIONS for:
Test C2150-602, IBM Security Intelligence V1, Solution Advisor

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

item C2150-602.1.1.2
A customer previously purchased a QRadar Log Management system. A solution advisor then recommended to the customer to purchase a license to migrate to QRadar Security Information and Event Management (SIEM).

What base functionality of the SIEM was the solution advisor looking to achieve?

A. Risk Monitoring
B. Policy Enforcement
C. Vulnerability Management
D. Event and Flow Correlation

item C2150-602.1.3.2
A company offers 24/7 security intelligence monitoring for its clients using the IBM QRadar SIEM 3124 appliance. The clients are small business organizations. Recently, the clients had a disruption in their services due to a network failure.

What should the solution advisor recommend to help avoid such failures?

A. Set up a flow processor appliance.
B. Set up a deployment with a Data Node appliance.
C. Set up a QRadar High Availability (HA) appliance.
D. Forward the events using event forwarding from one QRadar 2100 appliance to another.

item C2150-602.1.7.4
A solution advisor is working with a technology client after a data breach to analyze malware by executing software in a restricted operating system environment, thus controlling the resources and processes the software may use.

How should a solution advisor describe this technique?

A. Sniffing
B. Clustering
C. Sandboxing
D. Port Scanning

item C2150-602.3.1.5
A customer is looking to move data (events and flows) to an offboard storage device using such an external storage solution as Fibre Channel and Internet Small Computer System Interface (ISCSI).

How should a solution adviser explain the benefit of this move?

A. Increases overall storage capabilities
B. Increases redundancy in a High Availability environment
C. Increases search performance and overall storage capabilities
D. Increases data write performance and overall storage capabilities

item C2150-602.4.2.4
A customer has asked the solution advisor to provide a Security Event Information Management "SIEM" Virtual deployment on premise.

According to the solution advisor, on which one of the following can QRadar SIEM be installed?

A. Amazon AWS
B. Microsoft Azure
C. VMware ESX 5.5
D. Oracle Virtual Machine

item C2150-602.5.4.3
An organization is reviewing their network and discovered a need to collect 11 Million Flows Per Interval.

Which fully licensed appliances should the solution adviser propose to the organization that meet the minimum number of Flows Per Interval?

A. 2 1728 Flow Processors
   2 1310 Collectors
B. 3 1728 Flow Processors
   3 1310 Collectors
C. **5 1728 Flow Processors**
   8 1310 Collectors
D. 11 1628 Event Processors