Sample Questions for:
Test C2150-612, IBM Security QRadar SIEM V7.2.6

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

Item 1.2.4
What is a log source?
A. A data source that creates an event log
B. A flow collector that provides an event log
C. An external appliance that provide flow statistics
D. A configuration file defines the location of log information

Item 2.3.4
What is a common usage of reference data in QRadar?
A. Populating data list lookups in rules
B. Monitoring network utilization metrics
C. For generating reports on user activity
D. As a destination for log and network activity exports

Item 2.12.3
Which QRadar component stores and correlates log data from local and remote log sources?
A. QRadar Data Node
B. QRadar Flow Collector
C. QRadar Event Processor
D. QRadar Event Collector

Item 2.12.6
Which QRadar component hosts the Magistrate service which manages and prioritizes offenses?
A. QRadar Console
B. QRadar Manager
C. QRadar Risk Manager
D. QRadar Event Processor

Item 3.1.2
What is the proper URL for navigating to the QRadar console by IP address using a web browser?
A. ftp://<QRadar IP Address>
B. sftp://<QRadar IP Address>
C. http://<QRadar IP Address>
D. https://<QRadar IP Address>

Item 4.8.4
Which type of rule is the fastest and easiest way to track multiple events/Flows sequences over a period of time?
A. Custom Rule
B. Anomaly Rule
C. Threshold Rule
D. Behavioral Rule

Item 5.7.2
What is first used to derive an Asset's Name?
A. IP address
B. Given name
C. DNS host name
D. NetBIOS host name