



Vendor: IBM

Exam Code: P1000-017

Exam Name: Technical Sales Foundations for IBM QRadar
for Cloud (QRoC) V1

Version: DEMO

QUESTION 1

What is Flow Bias?

- A. Rules test configuration that prioritize event test conditions over flow test conditions
- B. Rules test configuration that prioritize Flow test conditions over event test condition
- C. A calculation that describes the absolute size or data transfer bias of a flow entering or leaving the network
- D. A calculation that describes the relative size or data transfer bias of a flow entering or leaving the network

Answer: D

QUESTION 2

What is the value of vulnerability scan data, as a data Source in QRadar?

- A. Identify user behavior activity
- B. Identify and Prioritize potential security issues
- C. Correlate logs and network activity
- D. Collect and parse log source event

Answer: B

QUESTION 3

Which is a capabilities gap between on Prem QRadar and QRadar on Cloud

- A. Two Datacenters currently hosts QRadar on Cloud Environment
- B. QRadar on Cloud is unable to Scale beyond 100K events per second
- C. Installation of application tokens required IBM operation team interaction
- D. Investigation of the offences logs and data requires generation of support of service ticket

Answer: C

QUESTION 4

What is a qflow

- A. An external flow type that can provide high level and low-level categories from the parsed event data
- B. An external flow type that can automatically extract numerous fields from unencrypted event payload data
- C. An internal flow type that can capture vulnerability assessment information from unencrypted payload data.
- D. An internal flow type that can capture a portion of unencrypted payload data and can recognize layer 7 applications

Answer: D

QUESTION 5

When Should the TLS syslog Protocol be used?

- A. When receiving encrypted flows.
- B. When receiving encrypted events
- C. When receiving clear text flows
- D. When receiving clear test events.

Answer: B

QUESTION 6

What are the benefits of QRadar on cloud?

- A. Includes incidents and offences tuning services
- B. Includes system health Monitoring and offence management services
- C. Includes vulnerability management and dashboard configuration services
- D. Includes system health monitoring and infrastructure management services

Answer: D

QUESTION 7

Which approach should be used to develop and optimize custom rules

- A. Avoid using index properties,
- B. Use as many tests possible
- C. Start with payload and regex test
- D. Start with broad categories that narrow the data that a rule tests evaluates

Answer: D

QUESTION 8

What role does the data gateway play within a QRadar on cloud deployed?

- A. It is responsible for scheduling reports
- B. It is responsible for tracking user logins to QRadar On Cloud
- C. It is responsible for securely transferring data from the client's environment to the cloud instance
- D. It is responsible for transferring data from the cloud back to into client's on-premise environment

Answer: C

QUESTION 9

What type of super flow is unidirectional flow that has same source and multiple destinations?

- A. Type A superflow (Network Scans)
- B. Type B superflow (DDOS)
- C. Type C superflow (Port scans)
- D. Type D Superflow (XFE)

Answer: A

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



10% Discount Coupon Code: ASTR14