Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

C1000-163 Dumps
C1000-163 Braindumps
C1000-163 Real Questions
C1000-163 Practice Test
C1000-163 Actual Questions

PASS

killexams.com

IBM

C1000-163

IBM Security QRadar SIEM V7.5 Deployment

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/C1000-163

Question: 1

Which integration option enables the ingestion of network flow data into IBM Security QRadar SIEM V7.5?

A. NetFlow Collector
B. Flow Processor
C. Flow Collector
D. Flow Log Agent

Answer: C

Explanation: The Flow Collector integration option allows the ingestion of network flow data into IBM Security QRadar SIEM V7.5. Flow Collectors receive flow data from network devices, such as routers and switches, and forward it to the Flow Processor for analysis. This enables the monitoring and detection of network traffic patterns and anomalies.

Question: 2

During the installation and configuration of IBM Security QRadar SIEM V7.5, which component is responsible for collecting event data from various sources?

A. Event Collector
B. Event Processor
C. Event Collector Agent
D. Event Collector Manager

Answer: A

Explanation: The Event Collector component in IBM Security QRadar SIEM V7.5 is responsible for collecting event data from various sources, such as network devices, servers, and applications. It acts as an intermediary between

the data sources and the Event Processor, forwarding the collected events for further processing and analysis.

Question: 3

How can IBM Security QRadar SIEM V7.5 integrate with the IBM X-Force Threat Intelligence service?

A. Through the X-Force Integration Module
B. Through the X-Force Collector
C. Through the X-Force API
D. Through the X-Force Event Processor

Answer: A

Explanation: The X-Force Integration Module enables the integration of IBM Security QRadar SIEM V7.5 with the IBM X-Force Threat Intelligence service. This integration allows QRadar to leverage threat intelligence information from X-Force, enhancing its ability to detect and respond to known threats and emerging security risks.

Question: 4

Which of the following factors should be considered when determining the architecture and sizing for IBM Security QRadar SIEM V7.5?

A. Number of events per second (EPS)
B. Retention period for log data
C. Number of concurrent users
D. All of the above

Answer: D

Explanation: The architecture and sizing of IBM Security QRadar SIEM V7.5 depend on several factors, including the number of events per second (EPS) that need to be processed, the retention period for log data, and the number of concurrent users accessing the system. These factors influence the hardware requirements and deployment configuration needed to ensure optimal performance and scalability.

Question: 5

What is the purpose of initial offense tuning in IBM Security QRadar SIEM V7.5?

A. To reduce false positive offenses
B. To increase the severity of offenses
C. To prioritize offenses based on risk level
D. To filter and discard irrelevant offenses

Answer: A

Explanation: Initial offense tuning in IBM Security QRadar SIEM V7.5 aims to reduce false positive offenses. By fine-tuning the correlation rules and event processing configurations, organizations can minimize the occurrence of false alarms and focus on genuine security incidents. This helps optimize the effectiveness of the security monitoring and response process.

Question: 6

What are the primary objectives of deploying IBM Security QRadar SIEM V7.5?

A. Centralized log management and analysis
B. Network traffic monitoring and analysis
C. User behavior analytics and anomaly detection

D. All of the above

Answer: D

Explanation: IBM Security QRadar SIEM V7.5 is a comprehensive security intelligence platform that aims to achieve centralized log management and analysis, network traffic monitoring and analysis, as well as user behavior analytics and anomaly detection. It provides a holistic approach to security monitoring and helps organizations identify and respond to potential threats effectively.

Question: 7

What are the key considerations for implementing multi-tenancy in IBM Security QRadar SIEM V7.5?

A. Data isolation and separation
B. Role-based access control (RBAC)
C. Tenant-specific configuration and customization
D. All of the above

Answer: D

Explanation: Implementing multi-tenancy in IBM Security QRadar SIEM V7.5 involves ensuring data isolation and separation between tenants, enforcing role-based access control (RBAC) to restrict access to tenant-specific data, and providing the ability to configure and customize each tenant's environment according to their specific requirements. These considerations are essential for organizations that need to support multiple entities or customers within a single QRadar deployment.

Question: 8

What should be considered when planning a migration or upgrade of IBM Security QRadar SIEM?

A. Compatibility of data sources and connectors
B. Impact on existing system configurations
C. Migration path and version compatibility
D. All of the above

Answer: D

Explanation: When planning a migration or upgrade of IBM Security QRadar SIEM, it is crucial to consider the compatibility of data sources and connectors with the target version, as well as theimpact on existing system configurations. Additionally, organizations need to identify the appropriate migration path and ensure version compatibility to ensure a smooth transition and minimize any potential disruptions to the security monitoring and management processes.

Question: 9

Which of the following factors can impact the system performance of IBM Security QRadar SIEM V7.5?

A. Number of active rules and offenses
B. Storage capacity and disk I/O
C. Network bandwidth and latency
D. All of the above

Answer: D

Explanation: The system performance of IBM Security QRadar SIEM V7.5 can be influenced by several factors, including the number of active rules and offenses, the storage capacity and disk I/O performance, as well as the network bandwidth and latency. It is essential to consider and optimize these factors to

ensure the system operates efficiently and delivers timely insights.

SAMPLE QUESTIONS

*These questions are for demo purpose only. **Full version** is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

***Actual Exam Questions**: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

***Exam Dumps**: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

***Practice Tests**: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

***Guaranteed Success**: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

***Updated Content:** Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

***Technical Support**: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*