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

KILL EXAMS

S2000-021 MCQs
S2000-021 TestPrep
S2000-021 Study Guide
S2000-021 Practice Test
S2000-021 Exam Questions

PASS

killexams.com

IBM

S2000-021

IBM Cloud Pak for Security V1.10 Administrator Specialty

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/S2000-021

Question: 1

Which of the following components is responsible for managing user authentication and access control in IBM Cloud Pak for Security V1.10?

A. QRadar
B. Resilient
C. Guardium
D. AppScan

Answer: B

Explanation: The Resilient component in IBM Cloud Pak for Security V1.10 is responsible for managing user authentication and access control. Resilient provides a secure environment for incident response and integrates with various identity and access management systems to ensure proper authentication and authorization of users accessing the platform.

Question: 2

Which of the following tasks can be performed using the Administration Console in IBM Cloud Pak for Security V1.10?

A. Managing user roles and permissions.
B. Generating compliance reports and metrics.
C. Analyzing security events and incidents.
D. Configuring network firewalls and security groups.

Answer: A

Explanation: The Administration Console in IBM Cloud Pak for Security V1.10 allows administrators to manage user roles and permissions. It provides a

centralized interface for creating user accounts, assigning roles, and defining access control policies, ensuring that users have appropriate privileges and permissions within the platform.

Question: 3

What is the primary purpose of the IBM Cloud Pak for Security V1.10 architecture?

A. To provide a centralized platform for managing security incidents and threats.
B. To enable seamless integration with third-party security tools and systems.
C. To automate security policies and compliance management processes.
D. To deliver advanced analytics and machine learning capabilities for threat detection and response.

Answer: A

Explanation: The primary purpose of the IBM Cloud Pak for Security V1.10 architecture is to provide organizations with a centralized platform for managing security incidents and threats. It integrates various security tools and systems, consolidating security data from multiple sources and providing unified visibility and control for effective incident response and threat management.

Question: 4

Which of the following troubleshooting techniques is recommended for resolving issues in IBM Cloud Pak for Security?

A. Rebooting the entire system
B. Rolling back to a previous software version

C. Analyzing system logs and error messages
D. Disabling security features temporarily

Answer: C

Explanation: Analyzing system logs and error messages is a recommended troubleshooting technique in IBM Cloud Pak for Security. It helps identify the root cause of issues and provides valuable information for resolving them effectively.

Question: 5

Which of the following Cloud Pak for Security components is responsible for collecting and analyzing security events from various data sources?

A. Security Information and Event Management (SIEM)
B. Threat Intelligence Exchange (TIE)
C. User Behavior Analytics (UBA)
D. Incident Response (IR)

Answer: A

Explanation: The SIEM component of IBM Cloud Pak for Security is responsible for collecting, aggregating, and analyzing security events from various data sources. It provides real-time monitoring, correlation, and alerting capabilities.

Question: 6

Which of the following actions can be performed using the Troubleshooting Console in IBM Cloud Pak for Security?

A. Viewing and analyzing log files for diagnosing issues.

B. Configuring network firewalls and security groups.
C. Creating and managing user accounts and permissions.
D. Generating compliance reports and audit logs.

Answer: A

Explanation: The Troubleshooting Console in IBM Cloud Pak for Security V1.10 allows administrators to view and analyze log files for diagnosing issues. It provides a centralized interface to access and search log data from various components, enabling administrators to identify and troubleshoot problems effectively.

Question: 7

Which component of IBM Cloud Pak for Security is responsible for managing user access, roles, and permissions?

A. Identity and Access Management (IAM)
B. Security Information and Event Management (SIEM)
C. User Behavior Analytics (UBA)
D. Threat Intelligence Exchange (TIE)

Answer: A

Explanation: The Identity and Access Management (IAM) component of IBM Cloud Pak for Security is responsible for managing user access, roles, and permissions. It ensures that users have appropriate access privileges based on their roles and responsibilities.

Question: 8

Which of the following protocols is commonly used for exchanging threat intelligence information in IBM Cloud Pak for Security?

A. HTTP
B. HTTPS
C. STIX
D. SNMP

Answer: C

Explanation: IBM Cloud Pak for Security supports the use of STIX (Structured Threat Information eXpression) for exchanging threat intelligence information. STIX is a standardized language for representing and sharing cyber threat information.

Question: 9

Which feature of IBM Cloud Pak for Security allows users to connect and integrate IBM and third-party data sources and assets?

A. Data Exchange
B. Threat Intelligence Exchange (TIE)
C. User Behavior Analytics (UBA)
D. Incident Response (IR)

Answer: A

Explanation: The Data Exchange feature of IBM Cloud Pak for Security enables users to connect and integrate IBM and third-party data sources and assets. It facilitates the exchange of information between different security tools and systems.

Question: 10

Which of the following components in IBM Cloud Pak for Security is responsible for vulnerability management?

A. Guardium
B. AppScan
C. BigFix
D. Resilient

Answer: B

Explanation: The AppScan component in IBM Cloud Pak for Security V1.10 is responsible for vulnerability management. AppScan performs automated security testing and scanning of applications and systems to identify vulnerabilities and potential security risks, helping organizations proactively mitigate such risks.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides 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 questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

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

Practice Test:

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

Guaranteed Success:

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

Updated Contents:

Killexams.com regularly updates its question bank of MCQs 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.