PassQueen
a.k.a dumpsqueen.com

DevOps Institute AIOps Foundation V1.0

PEOPLECERT AIOps-Foundation

Version Demo

Total Demo Questions: 4

Total Premium Questions: 49

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, AIOps Fundamentals	10
Topic 2, AIOps in the Organization	9
Topic 3, Core Technologies	16
Topic 4, AIOps and Operations Metrics	10
Topic 5, AIOps Use Cases	4
Total	49

QUESTION NO: 1

A development team says that an AIOps platform is unnecessary because its monitoring tool already reports whether individual servers are healthy. Which explanation BEST describes the additional value of AIOps?

A. AIOps removes the need to collect monitoring data

B. AIOps is limited to reporting server availability

C. AIOps correlates data across tools and services to provide insight and support action at operational scale

D. AIOps replaces all operational decisions with automation

ANSWER: C

Explanation:

AIOps correlates data across tools and services to provide insight and support action at operational scale is correct. Traditional monitoring can identify the state of individual components, whereas AIOps brings together large volumes of heterogeneous operational data to reduce noise, identify relationships, detect anomalies, and support informed or automated responses.

AIOps does not remove the need for monitoring data; monitoring is an important source of operational telemetry. It is also not limited to server availability, and its purpose is not merely to replace operational teams with automation.

QUESTION NO: 2

What is a big advantage of AIOps over ITOA?

A. It works with large datasets

B. It can understand the past

C. It can predict the future

D. It helps operations be reactive

ANSWER: C

Explanation:

“It can predict the future” is correct because a defining advantage of AIOps is its use of artificial intelligence and machine learning to move IT operations beyond retrospective reporting and analysis toward prediction and proactive action. AIOps platforms ingest operational data such as logs, metrics, events, traces, and alerts, then apply analytical models to identify patterns, detect anomalies, correlate related signals, and recognize conditions that may lead to an incident. This enables teams to forecast likely service degradation or capacity problems and intervene before users experience a material impact. Predictive insight supports reduced downtime, faster resolution, and more reliable digital services, especially in complex, high-volume environments where manual interpretation of operational data is difficult. The AIOps Foundation perspective emphasizes using AI-driven capabilities to improve operational decision-making and automate or accelerate responses. IBM similarly describes AIOps as applying AI, analytics, and machine learning to IT operations, including identifying and resolving issues more proactively. See IBM’s AIOps overview and the PEOPLECERT AIOps Foundation certification page.

QUESTION NO: 3

What does reliability mean?

A. The ability to keep a functioning state

B. The ability to be timely and easily maintained

C. The ability to perform all desired functions

D. The ability to not create harm

ANSWER: A

Explanation:

The ability to keep a functioning state correctly expresses reliability. In IT operations, reliability is the extent to which a service or system continues to operate correctly and deliver its intended service over time, including under expected operating conditions. It is therefore concerned with sustained, dependable operation rather than a one-time demonstration that a function can be performed. A reliable service remains in a functioning state, or returns to that state promptly when disruption occurs, so that users can depend on it.

This meaning is central to AIOps because AIOps capabilities such as event correlation, anomaly detection, predictive analysis, and automated remediation help operations teams identify conditions that could threaten continued service before they become user-impacting incidents. Maintaining a functioning state requires observing service health, recognizing degradation, and taking effective corrective action. Google's Site Reliability Engineering guidance describes reliability in terms of meeting service-level objectives and managing the risk of service unavailability, reinforcing the operational focus on dependable service over time. The NIST glossary likewise defines reliability as the ability of a system to perform a required function under stated conditions for a specified period. See Google SRE: Service Level Objectives and NIST CSRC: Reliability.

QUESTION NO: 4

Reactive Operations rely on:

A. Leading indicators

B. Lagging indicators

C. Prediction and inference

D. Big Data

ANSWER: B

Explanation:

Reactive Operations rely on **Lagging indicators**. A lagging indicator records the result of an event or condition that has already happened, such as an incident ticket, an outage-duration report, a breached service-level target, or a post-incident review. Operations teams use these signals to recognize that service impact has occurred, investigate its cause, restore the service, and learn from the event. This reflects a reactive operating model because the organization acts in response to observed failures or degraded performance rather than intervening before user impact occurs. In the AIOps context, the movement toward proactive operations requires earlier, forward-looking signals and analytics that can identify emerging risk, detect anomalous behavior, and support prediction before an incident becomes visible through historical outcome measures. Understanding the distinction is important because lagging measures remain valuable for reporting operational outcomes, measuring reliability, and prioritizing improvement work, even as AIOps capabilities help teams reduce dependence on purely after-the-fact response. For background on measuring outcomes with lagging indicators and using leading indicators to improve service delivery, see the Google SRE Book's guidance on service-level objectives and the Atlassian incident-response overview.