CCSK$^{Q\&As}$

Certificate of Cloud Security Knowledge

Pass Cloud Security Knowledge CCSK Exam with 100% Guarantee

Following Questions and Answers are all new published by Cloud Security Knowledge Official Exam Center

QUESTION 1

Which type of application security testing tests running applications and includes tests such as web vulnerability testing and fuzzing?

A. Code Review

B. Static Application Security Testing (SAST)

C. Unit Testing

D. Functional Testing

E. Dynamic Application Security Testing (DAST)

Correct Answer: E

E. Dynamic Application Security Testing (DAST)

Dynamic Application Security Testing (DAST) is a type of application security testing that involves testing running applications to identify vulnerabilities and security weaknesses. It simulates real-world attacks on the application and examines how it responds to those attacks. DAST typically includes tests such as web vulnerability scanning, penetration testing, and fuzzing. DAST tools send various inputs and payloads to the application, analyze the responses, and identify potential vulnerabilities such as injection flaws, cross-site scripting (XSS), and insecure configurations. Unlike Static Application Security

Testing (SAST), which analyzes the application\\'s source code, DAST focuses on the application in its deployed state. Therefore, the correct answer is E. Dynamic Application Security Testing (DAST).

QUESTION 2

In volume storage, what method is often used to support resiliency and security?

A. proxy encryption

B. data rights management

C. hypervisor agents

D. data dispersion

E. random placement

Correct Answer: D

QUESTION 3

Which statement best describes the Data Security Lifecycle?

A. The Data Security Lifecycle has six stages, is strictly linear, and never varies.

B. The Data Security Lifecycle has six stages, can be non-linear, and varies in that some data may never pass through all stages.

C. The Data Security Lifecycle has five stages, is circular, and varies in that some data may never pass through all stages.

D. The Data Security Lifecycle has six stages, can be non-linear, and is distinct in that data must always pass through all phases.

E. The Data Security Lifecycle has five stages, can be non-linear, and is distinct in that data must always pass through all phases.

Correct Answer: B

The statement that best describes the Data Security Lifecycle is:

B. The Data Security Lifecycle has six stages, can be non-linear, and varies in that some data may never pass through all stages.

The Data Security Lifecycle typically consists of six stages: Identify, Protect, Detect, Respond, Recover, and Review. These stages represent different activities and processes involved in securing data throughout its lifecycle. However, the lifecycle is not strictly linear, and the progression through these stages can vary depending on the specific data and its context.

Some data may not pass through all stages of the Data Security Lifecycle. For example, not all data may require the same level of protection or may not be subjected to the same detection and response mechanisms. The lifecycle is flexible and adaptable to different data types, risk levels, and security requirements.

QUESTION 4

Which of the following encryption methods would be utilized when object storage is used as the back-end for an application?

A. Database encryption

B. Media encryption

C. Asymmetric encryption

D. Object encryption

E. Client/application encryption

Correct Answer: E

11.1.4.2 Client-side encryption: When object storage is used as the back-end for an application (including mobile applications), encrypt the data using an encryption engine embedded in the application or client.

QUESTION 5

How should an SDLC be modified to address application security in a Cloud Computing environment?

A. Integrated development environments

B. Updated threat and trust models

C. No modification is needed

D. Just-in-time compilers

E. Both B and C

Correct Answer: B

Changing threat models. The cloud provider relationship and the shared security model will need to be included in the threat model, as well as in any operational and incident response plans. Threat models also need to adapt to reflect the technical differences of the cloud provider or platform in use.