CCSK$^{Q\&As}$

Certificate of Cloud Security Knowledge

Pass Cloud Security Knowledge CCSK Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/ccsk.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

ENISA: To mitigate credential compromise or theft, cloud provider can implement:

A. HR background checks

B. Hardening of virtual machines according to industry standard guidelines

C. Data-at-rest encryption

D. Portable applications using open APIs

E. Anomaly detection capabilities

Correct Answer: E

QUESTION 2

What is a challenge of application security in a cloud environment?

A. Non-uni ed interface

B. Limited detailed visibility

C. Isolated environments

D. Decreased application scope

E. Responsiveness

Correct Answer: B

Limited detailed visibility. Visibility and the availability of monitoring and logging are impacted, requiring new approaches to gathering security-related data. This is especially true when using PaaS, where commonly available logs, such as system or network logs, are often no longer accessible to the cloud user.

QUESTION 3

All assets require the same continuity in the cloud.

A. False

B. True

Correct Answer: A

QUESTION 4

Which type of application security testing should incorporate checks on API calls to the cloud service?

A. Dynamic Application Security Testing (DAST)

B. Unit Testing

C. Functional Testing

D. Static Application Security Testing (SAST)

E. All of the above

Correct Answer: D

Static Application Security Testing (SAST) is On top of the normal range of tests, these should ideally incorporate checks on API calls to the cloud service. Hence, Correct answer is D.

QUESTION 5

Which phase of the incident response lifecycle includes creating and validating alerts?

A. Preparation

B. Containment, Eradication, Recovery

C. Detection and Analysis

D. Auditing and Logging

E. Post-mortem

Correct Answer: C

QUESTION 6

You should disable remote access when working with immutable workloads.

A. True

B. False

Correct Answer: A

QUESTION 7

Big data includes high volume, high variety, and high velocity.

A. False

B. True

Correct Answer: B

QUESTION 8

CCM: A hypothetical company called "CertBus4Sure" provides a cloud based service to share con dential documents. The con dential documents are stored in their servers and are encrypted. How will CertBus4Sure ensure the protection of client data within their data center?

A. Audit plans should not be adopted and supported by the most senior governing elements of the organization (e.g. the board and the management)

B. Encrypt the data at rest and put in place appropriate measures for management of encryption keys

C. Implement redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, re suppression) and various security devices

D. Use a secure transfer channel (i.e. TLS)

Correct Answer: B

To ensure the protection of client data within their data center, Security4Sure should encrypt the data at rest. Encrypting data at rest helps safeguard sensitive information even if physical access to the servers is obtained.

Additionally, Security4Sure should put in place appropriate measures for the management of encryption keys. Proper key management ensures that only authorized individuals have access to the encryption keys, which are crucial for decrypting the data.

QUESTION 9

Which components typically comprise Infrastructure-as-a-Service (IaaS) providers?

A. Hardware, APIs, and Core Connectivity and Delivery

B. Integration and Middleware, APIS, and Data

C. Hardware, APIs, and Data

D. Presentation modality, APIs, Applications, and Data

E. Presentation modality, APIs, Applications, and Hardware

Correct Answer: A

Thus IaaS consists of a facility, hardware, an abstraction layer, an orchestration (core connectivity and delivery) layer to tie together the abstracted resources, and APIs to remotely manage the resources and deliver them to consumers.

QUESTION 10

What is defined as the process by which an opposing party may obtain private documents for use in litigation?

A. Discovery

B. Custody

C. Subpoena

D. Risk Assessment

E. Scope

Correct Answer: A

QUESTION 11

Which of the following is NOT a method of object storage encryption?

A. Externally managed encryption

B. File/folder encryption

C. Enterprise digital rights management

D. Proxy encryption

E. Client/application encryption

Correct Answer: C

QUESTION 12

How can cloud providers support a secure use of virtualization for cloud consumers?

A. By creating a secure chain of processes from the image used to run the VM through to a boot process with security and integrity

B. By locking, denying, or preventing access and then gradually enabling items as needed

C. By providing professional services to assist the consumer with configurations

D. Unfortunately, this is not a possible option for cloud consumers

E. By enabling full access to the consumer

Correct Answer: A

QUESTION 13

Which of the following statements best defines the "authentication" component of identity, entitlement, and access management (IdEA).

A. A guarantee that data in a repository is 100% unregulated

B. Updating security protocols to the latest version

C. Establishing/asserting the identity to the application

D. The process of specifying and maintaining access policies

E. None of the above

Correct Answer: C

C. Establishing/asserting the identity to the application

Authentication is the process of verifying and confirming the identity of a user or entity attempting to access a system, application, or resource. It involves presenting credentials (such as username and password, biometric data, or digital certificates) to prove one\\'s identity and gain access to the desired resource. The authentication component of identity, entitlement, and access management (IdEA) is responsible for validating and asserting the identity of users or entities interacting with an application or system.

QUESTION 14

Which statement best describes a data (information) dispersion fragmentation scheme?

A. A network is split into nodes; all of the nodes store only certain types of files.

B. Fragmented files are signed and stored together on a local server; data retrieval is arbitrary.

C. File fragments are sequentially placed on servers based on the physical location of the data user.

D. A cloud is split into cloudlets; each cloudlet stores a portion of the files based on an encryption algorithm.

E. A file is split into fragments; all of the fragments are sent to multiple physical storage repositories.

Correct Answer: E

E: data dispersion (sometimes also known as data fragmentation of bit splitting). This process takes chunks of data, breaks them up, and then stores multiple copies on different physical storage to provide high durability. Data stored in this way is thus physically dispersed. A single file, for example, would not be located on a single hard drive.

QUESTION 15

What is known as the interface used to connect with the metastructure and configure the cloud environment?

A. Administrative access

B. Management plane

C. Identity and Access Management

D. Single sign-on

E. Cloud dashboard

Correct Answer: B

As stated in Security-Guidance-v4.0, Pg 69 "cloud computing is the act of taking physical assets (like networks and processors) and using them to build resource pools. Metastructure is the glue and guts to create, provision, and deprovision the pool. The management plane includes the interfaces for building and managing the cloud itself, but also

the interfaces for cloud users to manage their own allocated resources of the cloud". Thus, the correct answer is 7 B. 7

CCSK PDF Dumps   **CCSK VCE Dumps**   **CCSK Braindumps**