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.certbus.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

QUESTION 1

All assets require the same continuity in the cloud.

A. False

B. True

Correct Answer: A

QUESTION 2

What are major factors to building and managing a secure management plane?

A. Perimeter security; customer authentication; internal authentication and credential passing; authorization and entitlements; and logging, monitoring, and alerting

B. API management; end point security; logging; and authentication and authorization

C. Device patching and maintenance; internal authentication and credential passing; access management and logging, monitoring, and alerting

D. Perimeter security; customer authentication; internal authentication and credential passing; authorization and entitlements; and governance auditing

E. Perimeter patching; log authentication; external entitlement passing; credential alerting and customer security

Correct Answer: A

SG Page# 72 says "Delving into implementation specifics is beyond the scope of this Guidance, but at a high level there are five major facets to building and managing a secure management plane:"

Perimeter security:

Customer authentication:

Internal authentication and credential passing:

Authorization and entitlements:

Logging, monitoring, and alerting:

QUESTION 3

APIs and web services require extensive hardening and must assume attacks from authenticated and unauthenticated adversaries.

A. False

B. True

Correct Answer: B

QUESTION 4

To what extent does the CSA Guidance document suffice for legal advice in setting up relationships with cloud service providers?

A. The CSA Guidance document provides adequate legal advice under certain circumstances.

B. The CSA Guidance document provides an overview of selected issues and it is not a substitute for obtaining legal advice.

C. The CSA Guidance document provides copious amounts of relevant case law to enable legal inferences to be developed.

D. The CSA Guidance document does not discuss any legal issues at all.

E. The CSA Guidance document provides sufficient guidance to substitute for legal advice.

Correct Answer: B

Answer is B: CCSK Study Security Guide pg 37: highlights some of the legal issues raised by moving data to the cloud; contracting with cloud service providers; and handling electronic discovery requests in litigation. Our overview here cannot address every potential legal situation. To address your specific issues, you should consult with legal counsel in the jurisdiction(s) in which you intend to operate and/or in which your customers reside. In addition, be aware that laws and regulations change frequently, and thus you should verify the relevancy of information contained in this domain before relying on it. Domain 3 is concerned primarily with the legal implications of public cloud computing and third party-hosted private clouds.

QUESTION 5

Which statement best describes the options for PaaS encryption?

A. PaaS is very diverse and may include client/application, database, and proxy encryption as well as other options.

B. PaaS is strictly limited to client/application, database and proxy encryption.

C. PaaS is sensitive to application updates and therefore must be constantly refreshed with relevant keys.

D. PaaS is very diverse and would most likely include le/folder and instance-managed encryption.

E. PaaS is limited to public networks.

Correct Answer: A

A. PaaS is very diverse and may include client/application, database, and proxy encryption as well as other options.

PaaS (Platform as a Service) is a cloud computing service model that provides a platform for developers to build, deploy, and manage applications without managing the underlying infrastructure. PaaS offerings can be diverse, and the encryption options available within a PaaS environment can vary. It can include various encryption measures such as client/application, database, and proxy encryption, along with other security features. The range of encryption options depends on the specific PaaS provider and the services they offer.

QUESTION 6

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 7

Sending data to a provider\\'s storage over an API is likely as much more reliable and secure than setting up your own SFTP server on a VM in the same provider

A. False

B. True

Correct Answer: B

QUESTION 8

The containment phase of the incident response lifecycle requires taking systems o ine.

A. False

B. True

Correct Answer: B

B. True

In the incident response lifecycle, the containment phase involves taking systems offline as a measure to prevent further damage or spread of the incident. By isolating affected systems or network segments, organizations can limit the impact and reduce the risk of additional compromise or data loss. Taking systems offline during the containment phase allows security teams to assess the situation, investigate the incident, and implement necessary remediation measures without the interference of ongoing malicious activity. It also helps to

prevent the incident from spreading to other parts of the infrastructure or affecting additional systems or users.

While the specific actions taken during the containment phase may vary depending on the nature of the incident and organizational policies, temporarily taking systems offline is a common and effective step to contain and control the situation.

QUESTION 9

Even with immutable infrastructures, the production environment, should be actively monitored for changes and deviations from approved baselines.

A. False

B. True

Correct Answer: B

Section 10.1.4 states "Even when using immutable infrastructure, the production environment should still be actively monitored for changes and deviations from approved baselines."

QUESTION 10

Which statement best describes why it is important to know how data is being accessed?

A. The devices used to access data have different storage formats.

B. The devices used to access data use a variety of operating systems and may have different programs installed on them.

C. The device may affect data dispersion.

D. The devices used to access data use a variety of applications or clients and may have different security characteristics.

E. The devices used to access data may have different ownership characteristics.

Correct Answer: D

QUESTION 11

Which part of the incident response process is greatly complicated by the resource pooling and rapid elasticity of cloud infrastructure?

A. Recovery

B. Ballistics

C. Detection

D. Forensics

E. Preparation

Correct Answer: D

QUESTION 12

Installing security software designed for physical servers onto a virtualized server can result in severe degradation in performance.

A. False

B. True

Correct Answer: B

B. True

Installing security software designed for physical servers onto a virtualized server can result in severe degradation in performance. Security software that is not optimized for virtual environments may consume excessive resources, such as CPU and memory, leading to reduced performance and potentially impacting the overall efficiency and scalability of the virtualized environment. It\\'s important to use security solutions that are specifically designed for virtualized environments to avoid such performance issues.

QUESTION 13

ENISA: Because it is practically impossible to process data in encrypted form, customers should have the following expectation of cloud providers:

A. Provider should be PCI compliant

B. Provider should immediately notify customer whenever data is in plaintext form

C. Provider must be highly trustworthy and have compensating controls to protect customer data when it is in plaintext form

D. Provider should always manage customer encryption keys with hardware security module (HSM) storage

E. Homomorphic encryption should be implemented where necessary

Correct Answer: C

V10. IMPOSSIBILITY OF PROCESSING DATA IN ENCRYPTED FORM

Encrypting data at rest is not difficult, but despite recent advances in homomorphic encryption (27), there is little prospect of any commercial system being able to maintain this encryption during processing. In one article, Bruce Schneier

estimates that performing a web search with encrypted keywords -- a perfectly reasonable simple application of this algorithm -- would increase the amount of computing time by about a trillion (28). This means that for a long time to come,

cloud customers doing anything other than storing data in the cloud must trust the cloud provider.

QUESTION 14

For cloud consumers to be able to properly configure and manage their network security, what must cloud providers do?

A. Expose security controls

B. Provide security templates

C. Configure a default deny and enable controls as requested

D. Provide administrator access to the tenant

E. Provide API access

Correct Answer: A

A. Expose security controls

For cloud consumers to be able to properly configure and manage their network security, cloud providers must expose security controls. Cloud providers should provide customers with the necessary tools, interfaces, and options to configure and manage security settings and controls according to their specific needs and requirements. This allows cloud consumers to define and implement their desired security policies, firewall rules, access controls, and other security measures within the cloud environment.

While options B, C, and E might also play a role in facilitating cloud consumer control over network security, option A directly addresses the need for cloud providers to expose security controls, enabling consumers to have the flexibility and control to configure their network security settings.

QUESTION 15

ENISA: An example high risk role for malicious insiders within a Cloud Provider includes

A. Sales

B. Marketing

C. Legal counsel

D. Auditors

E. Accounting

Correct Answer: D