CCSK$^{\text{Q\&As}}$

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.geekcert.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

When configured properly, logs can track every code, infrastructure, and configuration change and connect it back to the submitter and approver, including the test results.

A. False

B. True

Correct Answer: B

B. True

When logs are properly configured, they can track and record every code, infrastructure, and configuration change made within a system or environment. This includes capturing information about the submitter and approver of the changes, as well as any associated test results. Logs play a crucial role in maintaining an audit trail and providing accountability for changes made in a system. By analyzing logs, organizations can track the history of changes, identify potential issues or security breaches, and ensure compliance with policies and regulations. Therefore, the statement is true.

QUESTION 2

Why do blind spots occur in a virtualized environment, where network-based security controls may not be able to monitor certain types of traffic ?

A. The network stack is out of alignment

B. Clouds do not occur in networked environments

C. Traffic is undetectable in virtual machines

D. Virtual machines may communicate with each other over a virtual network all on the same host rather than a physical network between servers

E. None of the above

Correct Answer: D

Blind spots occur in a virtualized environment because virtual machines (VMs) can communicate with each other over a virtual network within the same host rather than sending traffic over a physical network between separate physical servers. This means that network-based security controls that are designed to monitor traffic on physical networks may not be able to detect or monitor traffic between virtual machines on the same host.

Options A, B, and C are not accurate explanations for the occurrence of blind spots in virtualized environments.

QUESTION 3

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 4

Which governance domain deals with evaluating how cloud computing affects compliance with internal security policies and various legal requirements, such as regulatory and legislative?

A. Legal Issues: Contracts and Electronic Discovery

B. Infrastructure Security

C. Compliance and Audit Management

D. Information Governance

E. Governance and Enterprise Risk Management

Correct Answer: C

QUESTION 5

What is true of cloud built-in firewalls?

A. They operate exclusively outside of the hypervisor

B. Whichever features are not provided in the firewall, the cloud provider has an alternative

C. They operate exclusively outside of the SDN

D. They typically offer fewer features that newer physical firewalls

E. They provide identical configurations to physical firewalls

Correct Answer: D

D. They typically offer fewer features that newer physical firewalls SecGuiV4, P.96: All modern cloud platforms offer built-in firewalls, which may offer advantages over corresponding physical firewalls. These are software firewalls that may operate within the SDN or the hypervisor. They typically offer fewer features than a modern, dedicated next-generation firewall, but these capabilities may not always be needed due to other inherent security provided by the cloud provider.