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.passapply.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

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 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

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 4

Which concept provides the abstraction needed for resource pools?

A. Virtualization

B. Applistructure

C. Hypervisor

D. Metastructure

E. Orchestration

Correct Answer: A

QUESTION 5

When associating the functions to an actor, what is used to restrict a list of possible actions dowr to allowed actions?

A. Permissions

B. Controls

C. Location

D. Functions

E. Actions

Correct Answer: B

page 65 : Controls: A control restricts a list of possible actions down to allowed actions. The table below shows one way to list the possibilities, which the user then maps to controls.