GIAC
GPCS
GIAC Public Cloud Security

Questions And Answers PDF Format:

For More Information – Visit link below:
https://www.certsgrade.com/

Version = **Product**

Latest Version: 6.0

Question: 1

In the context of cloud application services, which of the following practices are important for security hardening?
(Choose Two)
Response:

A. Using default configuration settings.
B. Implementing application layer encryption.
C. Regularly reviewing and updating security configurations.
D. Allowing unrestricted data access from any network.

Answer: B,C

Question: 2

Why is monitoring the execution of serverless functions important?
Response:

A. To track function performance
B. To ensure compliance with service-level agreements
C. To detect unauthorized access or unusual behavior
D. To automatically delete outdated functions

Answer: C

Question: 3

Your company is required to comply with several industry regulations, and you are tasked with ensuring that your cloud environment meets these compliance standards. After conducting an initial audit, you find several configuration issues that violate compliance benchmarks. What steps should you take to ensure ongoing compliance in the cloud environment?
(Choose three)
Response:

A. Use cloud compliance tools to automatically monitor and report on configurations
B. Implement encryption and multi-factor authentication for all sensitive resources
C. Disable all compliance monitoring tools to avoid additional costs
D. Regularly review and update IAM policies to comply with benchmarks

E. Remove compliance checks from non-critical resources to improve performance

Answer: A,B,D

Question: 4

What is the role of a Cloud Access Security Broker (CASB) in securing cloud storage?
Response:

A. To provide a virtual firewall for cloud services
B. To mediate access between cloud service users and providers
C. To manage the physical security of data centers
D. To ensure compliance with data storage regulations

Answer: B

Question: 5

What are best practices for managing credentials in a multicloud environment?
(Choose Three)
Response:

A. Use a centralized identity and access management system.
B. Store credentials locally on each cloud platform.
C. Regularly rotate and manage keys and credentials.
D. Ensure that all credentials are embedded in application code.
E. Audit and log all access to sensitive information.

Answer: A,C,E

Question: 6

Your company stores sensitive financial data on a public cloud storage platform. Recently, there have been attempts to access the storage buckets from unauthorized locations. What steps should you take to secure the storage platform and prevent further attempts?
(Choose three)
Response:

A. Enable encryption for data at rest and in transit
B. Restrict access to authorized IP addresses
C. Disable all security logs to reduce storage costs
D. Set up egress firewall rules and monitoring

E. Allow public access to the storage buckets to simplify access

Answer: A,B,D

Question: 7

What is the primary benefit of using private service endpoints in cloud environments?
Response:

A. To increase the network speed.
B. To allow public internet access to services.
C. To restrict access to services to internal network only.
D. To provide unlimited data storage.

Answer: C

Question: 8

Which encryption keys management practices are recommended for cloud data protection?
(Choose Two)
Response:

A. Store keys in a publicly accessible repository for easy access.
B. Use a dedicated security module for key management.
C. Rotate encryption keys periodically.
D. Use the same keys across multiple platforms for consistency.

Answer: B,C

Question: 9

How do conditional access policies enhance security in cloud environments?
Response:

A. By enforcing access rules based on the state of the user's device and location.
B. By providing unrestricted access to all users to enhance usability.
C. By encrypting data based on the user's role.
D. By auditing user activities in real-time.

Answer: A

Question: 10

The implementation of which technology can mitigate the risk of unauthorized data sharing from cloud storage?
Response:

A. Artificial Intelligence
B. Data Loss Prevention (DLP) systems
C. Load Balancers
D. Virtual Private Networks

Answer: B

For More Information – Visit link below:

https://www.certsgrade.com/

PRODUCT FEATURES

- 100% Money Back Guarantee
- 90 Days Free updates
- Special Discounts on Bulk Orders
- Guaranteed Success
- 50,000 Satisfied Customers
- 100% Secure Shopping
- Privacy Policy
- Refund Policy

16 USD Discount Coupon Code: NB4XKTMZ