GIAC
GCAD
Cloud Security Architecture and Design (GCAD)

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

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 6.0

Question: 1

Which of the following methods is most effective for defending data in cloud storage?

A. Using strong encryption and access controls
B. Disabling audit logging to reduce storage costs
C. Allowing unrestricted access to cloud storage buckets
D. Storing sensitive data in a publicly accessible repository

Answer: A

Question: 2

Which cloud identity security measures help reduce risks associated with unauthorized access? (Select two.)

A. Implementing Least Privilege Access
B. Using Hardcoded Credentials in Applications
C. Enforcing Role-Based Access Control (RBAC)
D. Disabling Multi-Factor Authentication (MFA)

Answer: A,C

Question: 3

Which security features are commonly found in cloud-based Key Management Systems (KMS)? (Select two.)

A. Centralized key storage and management
B. Manual key entry for every encryption process
C. Automatic key rotation
D. Unrestricted key distribution

Answer: A,C

Question: 4

Which of the following security measures can help prevent data leaks in the cloud? (Select two.)

A. Data Loss Prevention (DLP) solutions
B. Allowing unrestricted public access to storage buckets
C. Implementing encryption at rest and in transit
D. Using default security settings without modification

Answer: A,C

Question: 5

Which key feature of log aggregation enhances security monitoring in cloud environments?

A. Storing logs separately for each cloud region
B. Encrypting logs before sending them to a centralized repository
C. Generating logs only when an incident is detected
D. Discarding older logs to free up storage space

Answer: B

Question: 6

Which of the following is essential for secure incident response in a cloud environment?

A. Implementing a cloud-native Security Information and Event Management (SIEM) solution
B. Sharing access credentials across teams without restrictions
C. Using default security configurations without modifications
D. Keeping all incident response playbooks outdated

Answer: A

Question: 7

Which of the following security measures help in effective incident response in the cloud? (Select two.)

A. Enabling real-time monitoring and logging
B. Using manual responses for every security event
C. Deploying automated remediation workflows
D. Disabling audit logging to save storage space

Answer: A,C

Question: 8

What is the primary purpose of an Identity Provider (IdP) in an SSO system?

A. To store all user passwords locally
B. To manage user authentication and issue access tokens
C. To generate encryption keys for applications
D. To monitor network traffic for security threats

Answer: B

Question: 9

Which benefit does micro-segmentation provide over traditional perimeter security models?

A. It reduces reliance on identity-based access management
B. It enhances security by restricting internal east-west traffic
C. It completely eliminates the need for firewalls in cloud environments
D. It allows unrestricted communication between all cloud resources

Answer: B

Question: 10

Which cloud-native security tool is commonly used for micro-segmentation?

A. AWS IAM Policies
B. Azure Private Link
C. Google Cloud Firewall Rules
D. AWS Lambda Functions

Answer: C

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/