KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **Managing Cloud Security**

Title : WGU Managing Cloud Security (JY02)

Version : DEMO

1.Which phase of the cloud data life cycle involves activities such as data categorization and classification, including data labeling, marking, tagging, and assigning metadata?
A. Store
B. Use
C. Destroy
D. Create
Answer: D
Explanation:
The cloud data life cycle defines distinct stages that data goes through from its origin until its disposal. The Create phase is the very first stage, and this is where data is generated or captured by systems, applications, or users. At this point, data does not yet have context for storage or use, so it must be appropriately categorized and classified. Activities like labeling, marking, tagging, and assigning metadata are critical because they establish the foundation for enforcing controls throughout the rest of the life cycle.
Classification ensures that data is aligned with sensitivity levels, regulatory requirements, and business value. For example, financial records may be labeled “confidential” while general marketing content may be marked “public.” These distinctions guide how encryption, access controls, and monitoring will be applied in subsequent phases such as storage, sharing, or use.
According to industry frameworks, starting security at the Create phase ensures that controls “follow the data” across environments. Without proper classification at creation, organizations risk mismanaging sensitive data downstream.

2.Which phase of the cloud data life cycle involves the process of crypto-shredding?
A. Destroy
B. Create
C. Archive
D. Store
Answer: A
Explanation:
The Destroy phase of the cloud data life cycle is where information is permanently removed from systems. A common technique in cloud environments for this phase is crypto-shredding (or cryptographic erasure). Rather than physically destroying the media, crypto-shredding involves deleting or revoking encryption keys used to protect the data. Once those keys are destroyed, the encrypted data becomes mathematically unrecoverable, even if the underlying storage media remains intact.
This method is particularly useful in cloud environments where storage is virtualized and hardware cannot easily be physically destroyed. Crypto-shredding provides compliance-friendly assurance that sensitive data such as personally identifiable information (PII), financial data, or healthcare records cannot be accessed after retention periods expire or contractual obligations end.
By incorporating crypto-shredding into the Destroy phase, organizations align with standards for secure data sanitization. This ensures legal defensibility during audits and e-discovery and demonstrates proper lifecycle governance. The emphasis is on making data inaccessible while still maintaining operational efficiency and environmental responsibility.

3.In most redundant array of independent disks (RAID) configurations, data is stored across different

disks.
Which method of storing data is described?
A. Striping
B. Archiving
C. Mapping
D. Crypto-shredding
Answer: A
Explanation:
The method described is striping, which is a technique used in RAID configurations to improve performance and distribute risk. Striping involves splitting data into smaller segments and writing those segments across multiple disks simultaneously. For example, if a file is divided into four parts, each part is written to a separate disk in the RAID array.
This parallelism enhances input/output (I/O) performance because multiple drives can be accessed at once. It also provides resilience depending on the RAID level. While striping by itself (RAID 0) increases performance but not redundancy, when combined with mirroring or parity (e.g., RAID 5 or RAID 10), it offers both speed and fault tolerance.
The purpose of striping in the data management context is to optimize how data is stored, accessed, and protected. It is fundamentally different from archiving, mapping, or crypto-shredding, as those serve different objectives (long-term storage, logical placement, or secure deletion). Striping is central to high-performance storage systems and supports availability in mission-critical environments.

4.As part of training to help the data center engineers understand different attack vectors that affect the infrastructure, they work on a set of information about access and availability attacks that was presented. Part of the labs requires the engineers to identify different threat vectors and their names.
Which threat prohibits the use of data by preventing access to it?
A. Brute force
B. Encryption
C. Rainbow tables
D. Denial of service
Answer: D
Explanation:
The described threat is a Denial of Service (DoS) attack. In security contexts, a DoS attack aims to make a system, application, or data unavailable to legitimate users by overwhelming resources. Unlike brute force or rainbow table attacks, which target authentication mechanisms, or encryption, which is a defensive control, DoS focuses on disrupting availability—the “A” in the Confidentiality, Integrity, Availability (CIA) triad.
DoS can be executed in many ways: flooding a network with traffic, exhausting server memory, or overwhelming application processes. When scaled by multiple coordinated systems, it becomes a Distributed Denial of Service (DDoS) attack. In either case, the effect is the same—authorized users cannot access critical data or services.
For cloud environments, where service uptime is crucial, DoS protections such as rate limiting, auto-scaling, and upstream filtering are essential. Training data center engineers to recognize DoS helps them understand the importance of resilience strategies and ensures continuity planning includes availability safeguards.

5.An engineer has been given the task of ensuring all of the keys used to encrypt archival data are securely stored according to industry standards.
Which location is a secure option for the engineer to store encryption keys for decrypting data?
A. A repository that is made private
B. An escrow that is kept separate from the data it is tied to
C. An escrow that is kept local to the data it is tied to
D. A repository that is made public
Answer: B
Explanation:
Industry best practice requires that encryption keys are stored separately from the data they protect. This ensures that if the data storage system is compromised, attackers cannot immediately decrypt sensitive information. The use of a secure escrow system is a recognized approach.
An escrow provides controlled storage for encryption keys, ensuring they are only accessible by authorized processes and not co-located with the protected data. Keeping keys “local” to the data creates a single point of failure. A public or private repository without specialized protection mechanisms would also be insufficient due to risks of insider threats or misconfiguration.
By placing keys in an independent escrow system, the organization enforces separation of duties, strengthens defense-in-depth, and aligns with cryptographic standards from NIST and ISO. This practice is vital when dealing with archival data, where long-term confidentiality must be preserved even as systems evolve.