Cloud Security

Quiz

🛡️ Cloud Security Quiz (True/False) –[Intermediate Level]

Instructions: Read each statement carefully and mark it as True (T) or False (F).

1. Data stored in cloud environments is always encrypted by default.
   T / F

2. The shared responsibility model means cloud providers handle everything related to security.
   T / F

3. Identity and Access Management (IAM) policies are critical to secure cloud resources.
   T / F

4. All data breaches in the cloud occur due to provider vulnerabilities.
   T / F

5. Cloud Security Posture Management (CSPM) tools help detect misconfigurations in cloud infrastructure.
   T / F

6. Multi-cloud environments make security management simpler and more centralized.
   T / F

7. Zero Trust Architecture can be effectively applied to cloud environments.
   T / F

8. Encrypting data in transit is unnecessary if data at rest is encrypted.
   T / F

9. Public cloud platforms are inherently insecure compared to on-premise data centers.
   T / F

10. Cloud-native services like AWS Inspector and Azure Defender assist in vulnerability management.
   T / F

✅ Answer Key (for instructor or self-check)

1. False – Not all data is encrypted by default; users must often enable it.

2. False – Shared responsibility means both provider and customer are accountable.

3. True

4. False – Many breaches happen due to customer misconfigurations.

5. True

6. False – Multi-cloud environments often add complexity to security operations.

7. True

8. False – Both data at rest and in transit should be encrypted.

9. False – Security depends on configuration and management, not just the environment.

10. True