Day 5

“CLOUD SECURITY”

AWS Secured Solution Design:

1. Identity & Monitoring: Use IAM roles, policies, and MFA for secure access; monitor activity with CloudTrail, GuardDuty, and Config for threat detection and compliance.
2. Infrastructure & Data Protection: Secure workloads with network boundaries, firewalls, system hardening, and encrypt data at rest and in transit using KMS and TLS.
3. Incident Response: Prepare for incidents with CloudFormation, IAM clean rooms, and CloudTrail logs to trace and recover from security breaches efficiently.

Azure Secured Solution Design:

1. Identity & Data Security: Implement IAM with centralized Active Directory and SSO; enforce MFA for root accounts. Encrypt data at rest (snapshots, volumes) and in transit for full data protection.
2. Network Protection: Use Azure Endpoint, NSG, and third-party firewalls (e.g., Palo Alto, Barracuda) to secure traffic across segmented network zones (Public, Private, DMZ).
3. Compliance & Resilience: Azure ensures physical data center security, meets legal compliance standards, and supports high availability via continuous audits, RTO/RTP targets, and tier-3/4 infrastructure.

GCP Secured Solution Design – 3-Point Summary

1. Hardware-to-Software Security: GCP secures its infrastructure from the ground up using custom-designed servers, hardware security chips, secure boot stacks, and cryptographically verified components.
2. Service & User Access Protection: GCP uses cryptographic authentication for inter-service communication, enforces strict user access via centralized identity services, and encrypts data in transit and at rest using KMS.
3. Operational & Network Security: GCP implements robust DDoS protection, secure software development practices, employee device security, and real-time intrusion detection to ensure end-to-end cloud defense.

--The End--