Cloud Security Checklist

Baseline hardening for AWS, Azure, and GCP environments.

Identity & access

- [ ] Enable MFA on root/owner and all privileged accounts
- [ ] Use roles and short-lived credentials, not long-lived keys
- [ ] Apply least-privilege IAM policies; review regularly
- [ ] Remove unused users, keys, and permissions

Network

- [ ] Default-deny security groups / firewall rules
- [ ] Avoid exposing databases and admin ports to the internet
- [ ] Use private subnets and bastion/VPN for admin access
- [ ] Restrict and log inbound/outbound traffic

Storage & data

- [ ] Block public access on object storage by default
- [ ] Encrypt data at rest and enforce TLS in transit
- [ ] Classify sensitive data and limit who can access it
- [ ] Enable versioning and backups for critical buckets

Logging & detection

- [ ] Turn on cloud audit logging (CloudTrail / Activity Logs)
- [ ] Centralize logs and set alerts for risky actions
- [ ] Enable native threat detection (GuardDuty / Defender / SCC)
- [ ] Review findings on a regular cadence

Posture & config

- [ ] Use a configuration baseline / benchmark (CIS)
- [ ] Scan infrastructure-as-code before deployment
- [ ] Tag resources and track ownership
- [ ] Run periodic access and config reviews

guardioninfosec@gmail.com