How to Implement Secure Environment Separation

Dev/staging/prod isolation and deployment controls

Step 1: Define Environment Tiers

Establish clear boundaries between environments:

- Development: developer-owned, may use synthetic/anonymized data, relaxed controls
- Staging: production-like configuration, anonymized production data copy, stricter controls
- Production: full security controls, real data, change management required
- Each environment gets its own credentials, keys, and service accounts — never shared

Step 2: Implement Network Segmentation

Environments must be network-isolated:

- Separate VPCs/VNets per environment (or strict network policies in shared clusters)
- No direct network path from dev to production
- Staging can access production-like services but not production data
- Firewall rules enforced at infrastructure level, not application level

Step 3: Configure Deployment Controls

Enforce CIS 16.8 — separation of production and non-production:

- Production deployments require approval (manual gate or automated policy check)
- Canary deployments for high-risk changes (5% traffic, monitor, then full rollout)
- Rollback capability tested and documented for every deployment
- Deployment credentials scoped to minimum required permissions