2. Security & Guardrails

Policy Rulesets (Enterprise & Org Level)

> We enforce "Policy as Code" to prevent accidental exposure:

Enterprise Level: Branch protection is **mandatory**	

Org Level:
• **Branch Rules**
  ◦ Prevent branch deletion
  ◦ Block force pushes
  ◦ Require 2 pull request approvals
  ◦ Require last push approval
  ◦ Require review thread resolution
  ◦ Bypass: Organization Admins (for PRs only)
• **Push Rules**
  ◦ Restrict changes to `.github/**/*` directory
  ◦ Max file path length: 25 characters
  ◦ Block `.bin` and `.exe` files
  ◦ Max file size: 4MB
  ◦ Bypass: Organization Admins (always)
• **Tag Rules**
  ◦ Prevent tag deletion
  ◦ Block force pushes to tags
  ◦ Enforce semantic versioning pattern (e.g., `1.2.3`, `2.0.0-beta.1`)	

Integrating ORCA & Shift-Left Security

ORCA Integration: Add the `orca-scan` action to your `.github/workflows/main.yml`. It will scan your container images and IaC templates before deployment.	
Shift-Left Pipeline: Use the **Security Tab** in GHE to view CodeQL and Dependabot alerts. Vulnerabilities rated "High" or "Critical" will automatically fail the build in the `Staging` environment.	
