**Planned Tasks — Mapped to DevSecOps Pipeline Phases & Toolchain:**

| **Phase** | **Actions Planned** | **Tools / Projects** |
| --- | --- | --- |
| **Plan** | - Threat modeling - Security requirements - SECURITY.md | Project 24 (Threat Hunting), 26 (Intel Report), STRIDE / MITRE mapping |
| **Code** | - IDE Security (eslint-plugin-security) - Pre-commit hooks (Husky + lint-staged) - Secure coding (Helmet, rate-limit, validation, OAuth) | Project 10, 11, 12, 13 |
| **Test** | - Static code scan in CI (Semgrep) - Secrets scan (TruffleHog) - Dependency scan (Snyk / OWASP DC) | Project 9 |
| **Build** | - Static scanning of build artifacts (same as Test phase) - CI/CD GitHub Actions | Project 9 |
| **Release (Stage)** | - Dynamic scanning in stage env (ZAP baseline scan) | Project 9 |
| **Deploy (Prod)** | - Dynamic scanning in runtime (ZAP active scan / Postman API test) - Hardened Docker build - Nginx reverse proxy with secure headers | Project 22 |
| **Run** | - Periodic scanning (scheduled CI jobs for Semgrep + ZAP) - Logging and monitoring (Filebeat / ELK / basic SIEM) - Log Analysis (Project 29) | Project 30 |

What AWS could enable in this project:

✅ Use **EC2** for backend/frontend deployment (Dockerized)  
✅ Use **S3 + CloudFront** if you want static serving of frontend (optional)  
✅ Use **ACM** (AWS Certificate Manager) for HTTPS certs  
✅ Use **CloudWatch Logs** for basic monitoring/logging  
✅ Optional → use **Security Hub / GuardDuty** to show cloud security integration  
✅ Optional → manage with **Terraform** or AWS CDK for bonus DevSecOps value

Additional AWS-Related Tasks in Pipeline Phase:

| **Phase** | **AWS-specific Actions** |
| --- | --- |
| **Release** | Build multi-stage Docker image → push to EC2 or ECS |
| **Deploy** | Automate EC2 deploy → GitHub Actions or manually with AWS CLI |
| **Deploy** | Configure EC2 → Harden instance, configure Nginx reverse proxy |
| **Deploy** | Optional → use S3 + CloudFront for static frontend (Astro works great here) |
| **Run** | Enable **CloudWatch Logs** for backend and Nginx |
| **Run** | Periodic Cloud Security checks: Security Hub, GuardDuty alerts |
| **Run** | Optionally add **AWS Inspector** for EC2 instance scanning |

**Folder structure (suggested): -**

| **Folder / File** | **Purpose** |
| --- | --- |
| /resume-site/ | Main project root folder |
| /resume-site/frontend/ | Astro site |
| /resume-site/backend/ | Node.js API |
| /resume-site/.github/workflows/ | CI/CD (SAST, Secrets scan, DAST, Deploy to AWS) |
| /resume-site/Dockerfile | Multi-stage build (frontend + backend) |
| /resume-site/nginx/ | Nginx reverse proxy config (Dockerized or EC2 nginx) |
| /resume-site/aws/ | IaC → Terraform or AWS CLI scripts to deploy infra |
| /resume-site/aws/ec2-provisioning.md | Notes on EC2 instance config, security groups, hardening |
| /resume-site/aws/cloudfront-s3.md | Notes if using S3 + CloudFront (optional) |
| /resume-site/threat-models/ | Threat modeling artifacts |
| /resume-site/vulnerability-reports/ | SAST, DAST, Secrets scan reports |
| /resume-site/pentests/ | Manual pentest reports |
| /resume-site/log-analysis/ | Logs from backend + nginx + AWS CloudWatch parsing |
| /resume-site/docs/ | Architecture diagram (include AWS!), SECURITY.md, CHANGELOG.md |
| /resume-site/SECURITY.md | Disclosure policy and security contact |
| /resume-site/README.md | Project-specific README |
| /README.md | Main portfolio README |
| /SECURITY.md | Portfolio-wide security policy |