Duy Mach Tien

DevOps Engineer

Ho Chi Minh City, Vietnam duymt7356@gmail.com 0987 657 937 john-naeder duymt7356

Summary

DevOps engineer who builds the path from commit to production. Hands-on with Linux administration, containerization, CI/CD automation, Infrastructure as Code (IaC), secrets management, monitoring and backup/disaster recovery: bare-metal Kubernetes provisioned with Ansible, SLSA L3 signed pipelines, GitOps with Argo CD, and AWS deployments with centralised secrets and logging. Looking for a DevOps / Platform Engineer role where I can own delivery and infrastructure end to end.

Technical Skills

Containers & Orchestration: Docker, Kubernetes, Helm, Harbor

CI/CD & GitOps: GitLab CI, Argo CD, Tekton, Git

Cloud & IaC: AWS (EC2, ECS, ECR, S3, RDS, VPC, IAM, Route 53, CloudFront, CloudWatch, Secrets Manager), Ansible, Terraform

DevSecOps: Cosign, SLSA L3, Kyverno, Trivy, HashiCorp Vault (PKI, SSH CA, secrets), External Secrets Operator, Sealed Secrets, cert-manager

Backup & Disaster Recovery: Velero, Databasus (PostgreSQL PITR, restore verification)

Observability & Logging: Prometheus, Grafana, Loki

Networking & Proxies: Traefik, Nginx Ingress, Cloudflare Tunnel, Tailscale, Bind9 (DNS)

Data & Messaging: PostgreSQL, Redis, MinIO, MQTT, RabbitMQ

Operating Systems: Linux (Ubuntu, CentOS)

Programming: Bash, C# (Proficient); Python, Go, C++17 (Working Knowledge)

Work Experience

DIGI-TEXX, DevOps Intern — Ho Chi Minh City, Vietnam — Apr 2026 – present

- Rolled out centralised secrets management for Kubernetes with HashiCorp Vault and External Secrets Operator, so applications pull secrets by reference instead of carrying them in config; Reloader restarts the affected workloads automatically whenever a secret is rotated, and Vault Agent auto-renews TLS certificates issued by Vault PKI before they expire.
- Wrote a Helm chart with a value-generator that builds application config and the matching ExternalSecrets directly from centrally-managed Vault paths, cutting the time to onboard a new workload by roughly 80% and removing most of the manual setup.
- Built an end-to-end GitLab CI pipeline that builds the image, scans dependencies, lints the code, pushes to the registry, then signs and vulnerability-scans the artifact with Trivy and Harbor, generates an SBOM, and hands off to Argo CD for the GitOps deploy.
- Set up certificate-based SSH access on Vault's SSH certificate authority with Keycloak as the OIDC identity provider: engineers authenticate through SSO and receive short-lived signed certificates, with centrally-managed role-based access control (RBAC) so every login maps to a named role and expires on its own.
- Helped stand up the internal platform services on-premise with Docker Compose, then integrated SigNoz into the cluster and wrote the dashboards and alert rules the team now uses day to day, so latency and error-rate breaches page the team.

Sentrix Co., Ltd, Software Developer Intern — Ho Chi Minh City, Vietnam — Sept 2025 – Feb 2026

- Built the GitLab CI delivery pipeline for a React + .NET product: multi-stage Dockerfiles (Node to Nginx for the SPA, SDK to ASP.NET runtime for the services, pinned base images, non-root users), build, unit tests, dependency and secrets scanning, then push to Amazon ECR and roll out to Amazon ECS, with layer / NPM caching and per-branch preview environments so every pull request ships to its own isolated stack. Multi-stage builds cut the SPA image from ~1.1 GB to ~60 MB and each .NET service from ~1 GB to ~230 MB, shrinking both pull times and the vulnerability-scan surface.
- Owned the AWS side of the deployment: S3 + CloudFront for the React SPA, ECS / EC2 and RDS for the .NET services, IAM least-privilege roles per workload, and AWS Secrets Manager for runtime configuration, removing plaintext credentials from the repository entirely.
- Designed and shipped a centralised logging system: structured Serilog output from all .NET services shipped via Fluent Bit into OpenSearch, with correlation IDs propagated from the React client through to the backend, giving the team single-query tracing across a request's full path.
- Implemented fingerprint-based error grouping on top of that pipeline: exceptions are normalised and hashed by stack signature so recurring errors collapse into one issue with occurrence count, first / last seen, and affected users, cutting roughly 200 raw error notifications a day down to about 15 grouped issues, with only new or regressed signatures emailed to the team.

Projects

K8sSecDaP — SLSA-Secure Platform with eBPF Detection — Graduation Thesis Solo
Stack: K8s (kubeadm), Ansible, Calico, MetalLB, Tailscale, Argo CD, Tekton, Cosign, Kyverno, Kaniko, Harbor, Helmfile, cert-manager, Sealed Secrets, Prometheus, Grafana, Loki, eBPF (libbpf/CO-RE), Go, C++17 Sept 2025 – Apr 2026

- Provisioned a 3-node bare-metal Kubernetes cluster from scratch with Ansible over a Tailscale mesh (Calico CNI); idempotent roles bring nodes from bare reset to Ready in a single command, cutting provisioning from around 4 hours of manual work to about 20 minutes.
- Built a SLSA Level 3 CI pipeline with Tekton + Kaniko + Cosign: automated image signing, in-toto provenance, and Kyverno admission enforcement, pushing signed images to a self-hosted Harbor registry, with supply-chain integrity enforced end to end.
- Ran GitOps via Argo CD (App-of-Apps, auto-sync); bootstrapped cert-manager, Sealed Secrets, MetalLB for bare-metal LoadBalancer services, and ingress with Helmfile, plus full-stack observability with Prometheus, Grafana, and Loki.
- Designed and deployed an eBPF-based zero-trust detection system: a custom eBPF collector (kprobe tcp_v4_connect, CO-RE / libbpf) streaming into a C++17 detection engine, packaged as a per-node DaemonSet feeding a zero-trust SOC of Go / Python micro-services on NATS, PostgreSQL, and MinIO, backed by Longhorn persistent volumes with live Grafana dashboards.

E-Commerce Platform (Coffee Products) Team: 2
Stack: Java Spring Boot, Angular, ASP.NET Core, .NET WinForms, SQL Server, Redis, Docker, Traefik, Cloudflare Tunnel, AWS S3, CloudFront July 2025 – Sept 2025

- Delivered a full-stack e-commerce platform with synchronised web and desktop clients serving real product catalogue and order flows.
- Containerised and shipped the stack with Docker Compose behind a Traefik reverse proxy, exposed securely with zero open ports via Cloudflare Tunnel.
- Hardened the deployment with Traefik SSL (Let's Encrypt) and OWASP Top 10 practices (authentication, session handling, secure data handling); automated low-stock alerts and financial reports via scheduled jobs.

IoT Accident Monitoring & Alert System Team: 2
Stack: ESP8266, MPU6050, GPS (L80), ASP.NET 8.0, MQTT Mosquitto, Redis, InfluxDB, Grafana, Traefik, Docker Compose Apr 2025 – July 2025

- Engineered real-time accident detection with ESP8266 + MPU6050 + GPS, streaming telemetry via MQTT to a time-series InfluxDB backend.
- Built Grafana dashboards for live visualisation and automated alerting, enabling near-instant incident response.
- Containerised the full stack with Docker + Traefik reverse proxy for a reproducible, scalable deployment.

Education

BEng **Vietnam Academy of Cryptography Techniques**, Software Engineering — Ho Chi Minh City, Vietnam
Sept 2022 – Sept 2026

- GPA: 3.57 / 4.0
- Four-time recipient of the Academic Excellence Scholarship

Certifications and Courses

TOEIC (Listening & Reading): 890 / 990 — Dec 2024

Certified Kubernetes Administrator (CKA): KodeKloud — in progress

Docker Mastery: Kubernetes + Swarm: Bret Fisher — in progress

Languages

Vietnamese: Native

English: Professional working proficiency

Soft Skills

Problem-solving, teamwork, communication, adaptability, time management; proactive about picking up new technology and turning it into something that runs.