Noah Frost

Newcastle upon Tyne   REDACTED   REDACTED   linkedin.com/in/nfroze   github.com/nfroze

noahfrost.co.uk

DevSecOps engineer with 15 infrastructure projects and an AI-powered homelab — an autonomous webapp pipeline and a self-hosted Kubernetes cluster with live observability and AI-driven operations. Trained under a Global CISO in DevSecOps methodology. Background in policing brings proven stakeholder communication, compliance mindset, and decision-making under pressure. AWS, Security+, and Terraform certified.

Technical Skills

Cloud & Infrastructure: AWS (EKS, EC2, Lambda, GuardDuty, IAM), Azure, GCP, Terraform, CloudFormation, K3s

Container Orchestration: Kubernetes, Docker, EKS, K3s, ArgoCD, Helm

CI/CD & Automation: GitHub Actions, GitLab CI, Jenkins, GitOps workflows

Security Tools: Checkov, Trivy, Semgrep, Gitleaks, OPA Gatekeeper, Sentinel, Splunk SIEM

Observability: Prometheus, Grafana, kube-state-metrics, node-exporter, ELK Stack

Networking & Security: Cloudflare Tunnel, Network Policies, RBAC, Pod Security Standards

Languages & Scripting: Python, Bash, YAML, HCL

Homelab

AI Build System & Kubernetes Cluster

Phase 1: Autonomous Webapp Pipeline

Designed and built an end-to-end autonomous build system (Jarvis) running on a dedicated Mac with its own GitHub account, AWS credentials, and deployment pipeline. The system takes a webapp brief and delivers a live, deployed application — hero art generation from a self-trained LoRA model, animation, build spec, autonomous code generation, and AWS deployment — with zero manual intervention.

- Architected agent workflow integrating OpenClaw, Claude Code, GitHub CLI, AWS, and Cloudflare into a single checkpointed pipeline
- Five production DevSecOps webapps built and deployed through this system, running on AWS for under $3/month combined
- Hub site, source code, and documentation: **nfroze.co.uk** ↗ **| github.com/NFrozeCLAWDBOT** ↗

Phase 2: Kubernetes Cluster & AI Operations

Provisioned a K3s cluster on the same Mac running Jarvis, hardened it to production security standards, deployed full observability, and published a self-hosted build log — served by the cluster it documents.

- K3s on Apple Silicon with Cloudflare Tunnel (zero inbound ports, no public IP, outbound-only QUIC connection)
- Security hardening: 4 namespaces with Pod Security Standards enforcement, 12 network policies (default deny), RBAC with scoped service accounts, non-root pods (UID 101), read-only rootfs, all capabilities dropped
- kube-prometheus-stack: Prometheus, Grafana (28 dashboards, publicly accessible), node-exporter, kube-state-metrics
- Jarvis queries cluster health via kubectl in real time — AI operator managing live infrastructure, not just building it

- **Live: k3s.nfroze.co.uk** ↗ **| Dashboard: dashboard.nfroze.co.uk** ↗

Projects

End-to-End DevSecOps Pipeline with SIEM Integration | GitHub

Production-grade security automation across the entire software delivery lifecycle with threat detection streamed to Splunk

- Built four-stage pipeline with Semgrep SAST, Trivy SCA, Gitleaks secrets detection, and Checkov IaC scanning with security gates blocking non-compliant code
- Deployed to Amazon EKS with GuardDuty findings and CloudWatch logs streaming via Lambda to Splunk Cloud
- Hardened Kubernetes manifests: non-root containers, read-only filesystem, all capabilities dropped, seccomp profiles enforced

AI/ML Governance with Policy-as-Code | GitHub

Dual-layer policy enforcement preventing non-compliant infrastructure and untracked ML models reaching production

- Developed Sentinel policies for HCP Terraform blocking GPU instance provisioning and enforcing AI resource tagging pre-apply
- Built OPA Gatekeeper admission webhooks requiring ML tracking labels and model registry URLs on Kubernetes deployments
- Mapped controls to EU AI Act compliance requirements with risk-level tagging

MCP Security Incident Response System | GitHub

AI-powered security operations enabling natural language investigation and automated containment of AWS threats

- Integrated GuardDuty with EventBridge-triggered Lambda to automatically isolate compromised EC2 instances via security group swap
- Built MCP server exposing five tools to Claude Desktop: findings list, deep-dive analysis, incident reports, isolation status, restoration
- Implemented Slack webhook notifications with finding details for real-time security operations visibility

MCP Kubernetes Health Monitor | GitHub

Natural language querying of Kubernetes cluster health with GitOps automation and full DevSecOps pipeline

- Deployed EKS cluster with ArgoCD automated sync and self-healing, Prometheus, and Grafana observability
- Integrated Checkov, Semgrep, Gitleaks, and Trivy into GitHub Actions catching vulnerabilities across code, secrets, containers, and IaC
- Built MCP server exposing cluster health tools: unhealthy pods, resource usage, comprehensive health reports

Healthcare Threat Model: STRIDE Analysis | GitHub

Comprehensive security threat model for HIPAA-compliant healthcare platform handling PHI and PII

- Identified 15 prioritised threats across authentication, data protection, API security, and infrastructure using STRIDE methodology
- Mapped threats to MITRE ATT&CK framework and HIPAA Security Rule requirements (§164.308—312)
- Produced remediation guidance with working code examples bridging security architects and developers

MCP-Powered IaC Security Remediation | GitHub

AI-native infrastructure security connecting Claude Desktop directly to Checkov scan results for conversational analysis

- Built MCP server with tools for scan analysis, remediation generation, security reports, and source code retrieval
- Created remediation engine with pre-built fixes for 20+ common AWS security checks covering S3, RDS, EC2, IAM, VPC
- Integrated with GitHub Actions artifacts for historical result retrieval and audit trail

Certifications

CompTIA Security+

AWS Certified Cloud Practitioner

HashiCorp Certified: Terraform Associate

AWS Certified Solutions Architect — Associate — IN PROGRESS

Training

DevSecOps Bootcamp, Led by Charlie Banyard, Global CISO 09/2024 – 11/2024 | Remote

- Security integration across software development lifecycle
- Cloud security architecture and threat detection
- Compliance automation and policy-as-code

Professional Experience

Police Constable, Metropolitan Police 02/2022 – 09/2023 | London, UK

Frontline officer responsible for incident response, evidence management, and multi-agency coordination

- Translated complex legal and procedural requirements for non-expert audiences including courts, social services, and public stakeholders
- Made time-critical decisions under pressure with incomplete information during active incidents
- Wrote detailed reports meeting evidential standards for criminal prosecution
- Coordinated with multiple agencies ensuring compliance with data protection and governance requirements

Education

Law (Criminal Justice) LLM, Northumbria University 09/2023 – 2024

Criminology BSc (Hons), University of Chester 09/2016 – 09/2020