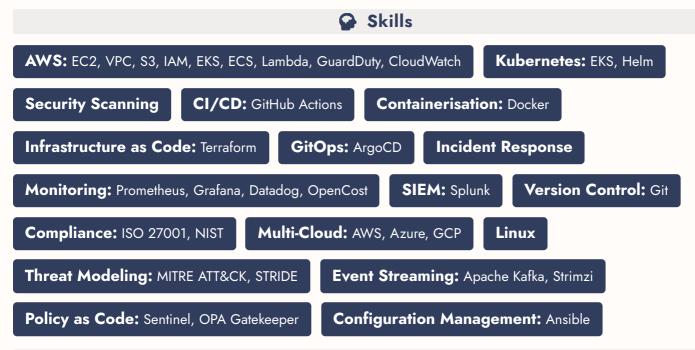
Noah Frost DevSecOps Engineer

REDACTED REDACTED Newcastle upon Tyne noahfrost.co.uk

in https://www.linkedin.com/in/noahfrost-devsecops/ github.com/nfroze

Profile

DevSecOps Engineer focused on delivering secure, scalable cloud infrastructure with integrated security automation. Built 17 production systems in 4 months. Experienced in AWS, Kubernetes, and GitOps workflows, with expertise in shift-left security practices and compliance scanning. Strong background in SIEM integration, container security, and infrastructure as code. Proven ability to streamline deployments and strengthen security posture through automated CI/CD pipelines.



Professional Experience

DevSecOps Engineer [Bootcamp], KubeCraft

07/2025 - Present | Remote

- Share technical insights from **17 DevSecOps projects** with **600+ member** community, demonstrating production implementations and architectural patterns
- Mentor engineers through code reviews and troubleshooting sessions, helping solve real-world infrastructure and security automation challenges
- Contribute to **3x weekly** community sessions, providing guidance based on hands-on experience building cloud platforms and CI/CD pipelines

DevSecOps Engineer [Self Directed], Self Employed

02/2025 - Present | Remote

- Designed and deployed 17 production-grade systems including Backstage developer platform achieving 70% cost reduction via hybrid EKS/ECS architecture, implementing secure clusters with Terraform and 100% Checkov compliance
- Built event-driven FinOps platform using Apache Kafka streaming (Strimzi operator) with OpenCost for real-time cost monitoring, achieving <30 second anomaly detection and increasing GPU utilisation from 60% to 85%
- Implemented Policy as Code governance using HCP Terraform Sentinel and OPA Gatekeeper on Kubernetes, preventing unauthorised resource provisioning and ensuring EU AI Act compliance
- Configured multi-cloud orchestration with **Ansible** and **Datadog** monitoring, deploying infrastructure across **AWS/Azure/GCP** in **12 minutes** using **GitOps** workflows
- Automated security scanning across CI/CD pipelines using GitHub Actions, integrating Semgrep (SAST), Trivy (containers), Gitleaks (secrets), and OWASP ZAP (DAST)
- Developed **Model Context Protocol** servers for Al-augmented operations, enabling natural language queries for **Kubernetes** cluster management and automated security incident analysis
- Integrated **Splunk SIEM** with **AWS CloudWatch** and **GuardDuty**, centralising security event monitoring with **Lambda** functions for real-time streaming
- Documented reference architectures creating open-source repositories with 700+ commits, currently developing AEGIS, FORGE, and SENTINEL - comprehensive AI security toolkit addressing OWASP Top 10 for LLMs

DevSecOps Engineer [Bootcamp], Cyber Agoge

09/2024 - 02/2025 | Remote

- Completed intensive 6-month DevSecOps bootcamp at one of UK's largest programs first graduate in program history invited by CISO to teach fortnightly project implementation lectures
- Conducted threat modelling exercises using **STRIDE** and **MITRE ATT&CK** frameworks, identifying vulnerabilities and designing security controls for enterprise cloud architectures
- Built and secured **AWS** infrastructure implementing **GuardDuty**, **VPC** security, and **IAM** policies with least privilege access controls across multi-tier applications
- Developed incident response playbooks and implemented **SIEM** solutions for real-time security monitoring with automated alerting for ransomware and DDoS scenarios

Police Constable, Metropolitan Police

02/2022 - 09/2023 | London, UK

- Completed rigorous police training through **Degree Holder Entry Programme (DHEP)**, developing investigative and analytical skills directly applicable to security incident response
- Selected as **Deputy Captain** by cohort peers, demonstrating leadership in high-pressure operational environments
- Held **RV/CTC clearance**, demonstrating proven vetting for sensitive roles and trustworthiness required for handling critical infrastructure



15+ Additional projects available at noahfrost.co.uk

Multi-Cloud Orchestration

- Built unified platform deploying AWS, Azure, and GCP infrastructure simultaneously in 12 minutes
- Implemented GitOps workflow with GitHub Actions triggering parallel Terraform provisioning across all clouds
- Developed OS-adaptive **Ansible** playbooks detecting **RedHat/Debian** for consistent **nginx** configuration
- Deployed **Datadog EU** agents providing single-pane-of-glass monitoring with **100% configuration parity**
- Configured unified **SSH** keys and **security groups** across **VPC**, **VM**, and **compute** resources

All Governance Framework

- Built dual-layer governance with Sentinel and OPA blocking £10K+/month unauthorised GPU provisioning
- Implemented **HCP Terraform** policies preventing **p3.2xlarge** instances (£3.06/hr) before provisioning
- Deployed OPA Gatekeeper on AWS EKS enforcing ML model tracking with clear policy violations
- Achieved 100% compliance with mandatory versioning and team attribution via Kubernetes admission control
- Reduced **EU AI Act** compliance reporting from 2 weeks to 2 hours through automated audit trails

& Al FinOps Platform

- Built real-time cost platform processing millions of events through **Apache Kafka** streaming on **AWS EKS**
- Deployed Strimzi Kafka operator with 3 brokers and 23 partitions for GPU and API cost events
- Implemented OpenCost, Prometheus and Grafana achieving <30 second anomaly detection
- Prevented £100K+ monthly overruns through event-driven monitoring of gpu-utilisation and ai-api-costs
- Configured complete **Terraform** infrastructure with **VPC** networking and **Helm** chart deployments

- Deployed production GitOps workflow using ArgoCD on AWS EKS achieving 2 minute deployments
- Implemented **Prometheus** and **Grafana** observability stack via **Helm** charts with pre-built dashboards
- Configured self-healing Kubernetes deployments where ArgoCD continuously ensures cluster matches Git state
- Resolved complex Prometheus CRD failures using ServerSideApply and debugged DNS/Terraform issues
- Built Terraform modules for complete AWS infrastructure: VPC, EKS cluster, IAM roles with least privilege

Find-to-End DevSecOps Transformation

- Built secure CI/CD pipeline using GitHub Actions with integrated security scanning across SDLC
- Deployed to AWS EKS with Docker containerisation and Kubernetes orchestration
- Automated security tools: Semgrep (SAST), Trivy (containers), Gitleaks, OWASP ZAP, Checkov
- Developed Lambda functions for GuardDuty to Splunk SIEM streaming via CloudWatch events
- Achieved 100% IaC automation with Terraform provisioning VPC, EC2, S3, and IAM security



CompTIA Security+

AWS Certified Cloud Practitioner

HashiCorp Certified: Terraform Associate

AWS Certified Solutions Architect - Associate - IN PROGRESS



Law (Criminal Justice) LLM, Northumbria UniversityFinal Term Paused

09/2023 - Present

Criminology BSc (Hons), University of Chester

09/2016 - 09/2020