

# Noah Frost

📍 Newcastle upon Tyne    ✉ REDACTED    ☎ REDACTED    🔗 [linkedin.com/in/nfroze](#)  
🐙 [github.com/nfroze](#)    🔗 [noahfrost.co.uk](#)

DevSecOps engineer with 8 months building security automation across 20 projects spanning CI/CD pipelines, Kubernetes security, cloud infrastructure, and AI-assisted incident response. 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 Platforms:** AWS (EKS, EC2, Lambda, GuardDuty, IAM), Azure, GCP, Terraform, CloudFormation

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




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




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

**Languages & Scripting:** Python, Bash, YAML, HCL

**Methodologies:** STRIDE, MITRE ATT&CK, DevSecOps, Infrastructure as Code, Policy as Code

## Projects

- DevSecOps Pipeline** | GitHub  End-to-end security pipeline integrating vulnerability scanning into deployment workflow
- Built automated pipeline using GitHub Actions with Checkov, Trivy, and Semgrep security gates blocking non-compliant code pre-deployment
  - Deployed containerised applications to Amazon EKS with GuardDuty threat detection and Splunk SIEM integration
  - Implemented GitOps workflow with ArgoCD for auditable, version-controlled deployments
- AI Governance Framework** | GitHub  Policy-as-code framework enforcing security and compliance standards across Kubernetes environments
- Developed Sentinel policies and OPA Gatekeeper constraints to automate compliance checks at admission control
  - Created Kubernetes admission webhooks rejecting workloads violating security baselines
  - Documented policy rationale mapping controls to compliance requirements
- AI-Assisted Security Operations** | GitHub  Automated incident response system using AI orchestration for threat remediation
- Integrated GuardDuty alerts with Lambda functions to automatically isolate compromised EC2 instances
  - Built Slack notification pipeline providing real-time security alerts to operations team
  - Reduced manual intervention in initial incident triage through automated containment workflows

- Kubernetes Security Platform** | GitHub  Comprehensive DevSecOps platform with monitoring, security scanning, and GitOps deployment
  - Deployed EKS cluster with ArgoCD, Prometheus, and Grafana for observability
  - Integrated Checkov, Semgrep, Gitleaks, and Trivy into CI pipeline catching vulnerabilities across code, secrets, containers, and IaC
  - Configured security scanning to run on pull requests with automated pass/fail gating
- Threat Modelling Framework** | GitHub  Security assessment methodology applied to healthcare application architecture
  - Applied STRIDE methodology to identify threats across application components and data flows
  - Mapped identified threats to MITRE ATT&CK framework for standardised threat intelligence
  - Produced risk assessment documentation with prioritised remediation recommendations
- AI-Assisted IaC Security** | GitHub  Infrastructure security scanning with AI-powered analysis and remediation suggestions
  - Implemented Checkov scanning for Terraform configurations with custom policy rules
  - Built automated IAM least-privilege analysis identifying over-permissioned roles
  - Created pre-commit hooks preventing insecure infrastructure reaching version control

**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

**Certifications**

CompTIA Security+

AWS Certified Cloud Practitioner

HashiCorp Certified: Terraform Associate

AWS Certified Solutions Architect – Associate – IN PROGRESS

**Education**

**Law (Criminal Justice) LLM, Northumbria University**

09/2023 – 2024

**Criminology BSc (Hons), University of Chester**

09/2016 – 09/2020