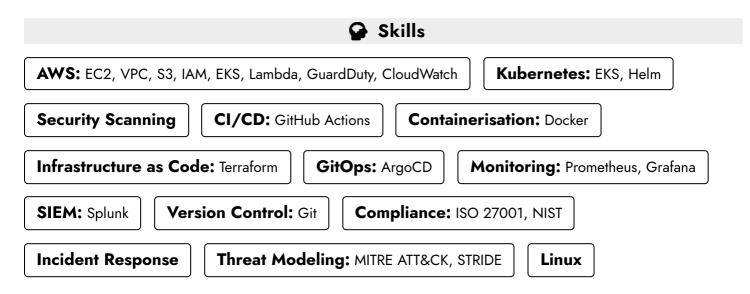
Noah Frost DevSecOps Engineer

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

Profile

DevSecOps Engineer focused on delivering secure, scalable cloud infrastructure with integrated security automation. 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.



Projects

Project 12: MCP Meets K8s

- Pioneered one of the first **Model Context Protocol** integrations for **Kubernetes**, enabling natural language cluster operations via Claude Desktop
- Deployed production DevSecOps platform on AWS EKS with GitOps via ArgoCD and Helm charts
- Integrated comprehensive security scanning pipeline: Semgrep (SAST), Trivy (SCA), Gitleaks (secrets), Checkov (IaC)
- Configured Prometheus and Grafana monitoring stack with CloudWatch integration for real-time observability
- Built infrastructure using Terraform with VPC isolation, EKS cluster, S3 storage, and IAM security
- Implemented **Docker** container security contexts and **Kubernetes** RBAC policies

Project 9: GitOps with ArgoCD & Monitoring

- 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 deployment failures using ServerSideApply for large resource handling
- Built Terraform modules for complete AWS infrastructure: VPC, EKS cluster, IAM roles with least privilege
- Debugged **DNS** resolution and **Terraform** module issues, demonstrating real-world troubleshooting skills

Project 5: End-to-End DevSecOps Transformation

- Built secure CI/CD pipeline using GitHub Actions with integrated security scanning across SDLC
- Deployed to AWS EKS with Docker containerization 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
- Configured AWS infrastructure: VPC networking, EC2 compute, S3 storage, IAM security
- Achieved 100% automation with Terraform for Infrastructure as Code deployment

Additional projects available at noahfrost.co.uk



DevSecOps Engineer [Bootcamp], KubeCraft

07/2025 - Present | Remote

- Present technical workshops on **MCP integrations**, **GitOps**, and **AWS EKS** deployments to 600+ member DevOps community
- Mentor engineers on implementing **CI/CD pipelines**, **Kubernetes** orchestration, and **security automation** through hands-on demonstrations
- Contribute to 3x weekly technical sessions, sharing production implementations of Terraform IaC and container security best practices
- Provide code reviews and architectural guidance for community projects focussing on **DevSecOps** patterns and **shift-left security**

DevSecOps Engineer [Self Directed], Self Employed

02/2025 - 07/2025 | Remote

- Designed and deployed 12 production-grade **DevSecOps** systems on **AWS**, implementing secure **EKS** clusters with **Terraform** and achieving 100% **Checkov** compliance for infrastructure security
- Automated security scanning across CI/CD pipelines using **GitHub Actions**, integrating **Semgrep** for SAST analysis, **Trivy** for container vulnerability detection, and **Gitleaks** for secrets management
- Implemented **GitOps** workflows using **ArgoCD** for **Kubernetes** deployments, reducing deployment times to under 5 minutes whilst maintaining comprehensive security validation
- Configured enterprise monitoring solutions with **Prometheus** and **Grafana** deployed via **Helm** charts, establishing real-time metrics collection and alerting for **Docker** workloads
- Integrated **Splunk SIEM** with **AWS CloudWatch** and **GuardDuty**, centralising security event monitoring and enabling rapid incident response capabilities
- Developed **Model Context Protocol** servers for Al-augmented operations, enabling natural language queries for **Kubernetes** cluster management and automated security incident analysis
- Documented reference architectures and security patterns, creating open-source repositories utilised by DevOps engineers for production implementations

DevSecOps Engineer [Bootcamp], Cyber Agoge

09/2024 - 02/2025 | Remote

- Completed intensive 6-month **DevSecOps** bootcamp led by experienced CISO, mastering enterprise security frameworks including **NIST**, **ISO 27001**, and practical implementation strategies
- 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
- Performed penetration testing on vulnerable applications using **Burp Suite**, **Metasploit**, and **Wireshark**, documenting exploitation paths and remediation strategies
- Developed incident response playbooks for ransomware and DDoS scenarios, applying NIST Incident Response Framework to simulated security breaches
- Implemented **SIEM** solutions for real-time security monitoring, configuring log aggregation, correlation rules, and automated alerting for threat detection
- Demonstrated rapid progression from foundational concepts to advanced implementations, with subsequent project portfolio leading to invitation as potential guest lecturer

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 and threat analysis
- Selected as **Deputy Captain** by cohort peers, demonstrating leadership capabilities in high-pressure operational environments requiring rapid decision-making and team coordination
- Conducted systematic investigations using evidence-based methodologies, developing pattern recognition and root cause analysis skills essential for security operations and threat hunting
- Produced detailed documentation for legal proceedings, ensuring accuracy and compliance with strict regulatory standards skills transferable to security audit trails and incident reporting
- Assessed dynamic risk scenarios and implemented mitigation strategies, building foundation for security risk assessment and threat modelling in technical environments
- Maintained **security clearance** eligibility through comprehensive vetting process, demonstrating integrity and trustworthiness required for handling sensitive infrastructure
- Received outstanding reference highlighting "exceptional critical thinking" and "strong work ethic" from police training tutor

Certificates

CompTIA Security+ □

AWS Certified Cloud Practitioner

HashiCorp Certified: Terraform Associate

AWS Certified Solutions Architect – Associate – IN PROGRESS

Education

Law (Criminal Justice) LLM, Northumbria University Final Term Paused

09/2023 - Present

Criminology BSc (Hons), University of Chester

09/2016 - 09/2020