Deon Prinsloo

South Africa (Remote-first)

Email: deon66@gmail.com | Mobile: +27 71 252 8672

LinkedIn: www.linkedin.com/in/deon-prinsloo-0341b0332

Website: https://shieldcraft-ai.com

GitHub: https://github.com/Dee66/ShieldCraft-AI | https://github.com/Dee66/CodeCraft-AI

AI Solutions Architect (AWS) | Security, DevOps, and FinOps

AI Solutions Architect with over 15 years experience in designing, implementing, and deploying production-grade systems. Now focused on architecting and delivering secure, end-to-end GenAI and MLOps solutions on AWS, with core competencies in security and FinOps.

**Summary**

- Experienced in building and shipping production systems, end-to-end.

- Product ownership: architecture, application code, IaC, CI/CD, security, observability, cost management and guardrails.

- Comfortable leading both infrastructure and ML implementation.

- Flagship projects: ShieldCraft AI (Proactive Cybersecurity GenAI/MLOps on AWS) and CodeCraft AI (developer productivity with RAG).

**Profile** **Projects**

ShieldCraft AI - Proactive Cybersecurity GenAI/MLOps on AWS

Repo: https://github.com/Dee66/ShieldCraft-AI

ShieldCraft is an AWS-native platform that turns cloud security from reactive to proactive. I built it after seeing teams drown in alerts, misconfigurations, and struggle to close the loop from detected to fixed. ShieldCraft acts on the signal, not the noise—predicts what matters, validates defences continuously, and can auto-remediate (or generate runbooks with tailored AI guidance) safely within configurable guardrails.

What it does: Prioritizes risks, emulates real attacks, and executes fixes with full audit-ability, accountability, automated re-mediation (within guardrails), guided threat resolution and roll-back with observability and continuous monitoring.

Why it matters: Cuts MTTR, reduces alert fatigue, and raises confidence that controls actually work against novel threats.

How it works: Various (20+) AWS services working in harmony continuously and silently scan your infrastructure with strong governance and a pragmatic GenAI core for triage, reasoning, and remediation.

Benchmarked model efficiency via BEIR and MTEB tests, alongside comprehensive (850+) unit and integration tests.

Designed for production: Environment-aware IaC, fail-fast config validation, extensive tests, least-privilege layered security design and cost guardrails to keep it deployable in the real world.

CodeCraft AI

Repo: https://github.com/Dee66/CodeCraft-AI

CodeCraft is a developer productivity platform that helps teams truly understand large codebases, explain changes clearly, and keep documentation current without slowing engineers down. It grew out of two observations: proper on-boarding is both essential and expensive. CodeCraft’s initial intent was to assist this process, adapting to users across multiple departments and domains.

What it does: Automates on-boarding, analyses code & infrastructure and recommends best practice.

Why it matters: Cuts on-boarding time, reduces review thrash, and improves traceability across fast-moving teams. Acts as programming assistant, trained on the repository in question.

How it works: Retrieval-augmented generation over your repo and artifacts, tuned prompts and PEFT for your domain, AWS-native pipelines for secure, reproducible delivery.

**Certifications**

- AWS Certified Solutions Architect – Associate (SAA-C03)

- AWS Certified AI Practitioner (AIF-C01)

- In progress: AWS Certified Security – Specialty (SCS-C02)

Training

- Generative AI with Large Language Models (DeepLearning.AI + AWS)

- Machine Learning (Stanford)

- Supervised Machine Learning: Regression and Classification (Stanford)

- Unsupervised Learning, Recommenders, Reinforcement Learning

- Advanced Learning Algorithms (Stanford/DeepLearning.AI)

- In progress: Foundations of Cybersecurity (Google)

**Core Competencies**

* AI/MLOps Platform Architecture: Designing and deploying end-to-end Generative AI and MLOps solutions on AWS, including model orchestration, Retrieval-Augmented Generation (RAG) implementation, and scalable, secure CI/CD pipelines.
* Cloud Security by Design: Implementing robust security guardrails from the ground up, with expertise in least-privilege IAM, policy-as-code, encryption, and automated secrets management.
* FinOps & Cost Optimization: Architecting cost-aware solutions with clear tagging standards, budget alerts, and resource right-sizing to ensure financial accountability.
* Operational Reliability: Ensuring system resilience through config validation, negative testing, automated preflight checks, and robust observability for high availability.

**Languages and frameworks**

Python, Java, Node.js, Java/TypeScript, React, Next.js, NestJS, Spring (various)

GenAI and MLOps: Amazon SageMaker, Bedrock model access, LangChain, Hugging Face, Jupyter

AWS services: Organizations, Control Tower, security groups, API Gateway, Lambda, Step Functions, EventBridge, S3, KMS, Glue, Lake Formation, Athena, Secrets Manager, IAM, CloudWatch, Config, Security Hub, GuardDuty, Inspector, MSK, OpenSearch, Budgets, ECR, CloudTrail, ECS, Fargate, EKS

Infrastructure and tooling: AWS CDK in Python, CloudFormation, Docker, GitHub Actions, Poetry, Nox, Pytest, Pydantic

Data: PostgreSQL, Informix, MySQL, DynamoDB(Mongo), OpenSearch, RedShift, Lake Formation

Developer experience: Quality, robust code incorporating SOLID Principles, design patterns, extensive multi-path unit and integration testing, automated deployment workflows and Docusaurus documentation.

**Professional** **Experience** - Software Engineering

Technical Lead - Terra Firma Solutions | Jun 2022 – Dec 2024

- Architected and led a team to deliver a real-time solar energy management platform

- Orchestrated a large-scale migration from a monolithic Java codebase to a cloud-native microservices architecture on AWS, significantly improving performance and scalability.

- Wrote and and deployed cloud‑native microservices on AWS integrating with Azure, using Docker and Kubernetes for continuous and automated deployment.

- Implemented OAuth 2.0/JWT authentication and raised code quality via reviews, standards, and mentorship.

Senior Software Engineer - Loot | Mar 2018 – Nov 2021

- Led full-stack architecture and implementation for high-traffic e-commerce platforms (Loot Marketplace, Stylemode, Loot V2).

- Built reusable React and Node.js components integrated with Java backend APIs to improve UX and responsiveness.

- Optimized AWS deployments to handle peak traffic reliably.

- Mentored junior engineers and provided architectural guidance across frontend and backend stacks.

Software Engineer - PayGate | Apr 2017 – Mar 2018

- Shipped highly testable features within an Agile environment using SOLID principles and TDD.

- Integrated critical third‑party APIs to expand payment processing capabilities.

Software Engineer - NightsBridge | Aug 2014 – Mar 2017

- Developed and maintained Java‑based web applications using JavaScript, jQuery, Angular, and MySQL on Linux.

- Implemented SOAP/JSON web services within a servlet‑based architecture; gained strong MVC fundamentals.

Software Engineer - Magix | Feb 2013 – Jun 2014

- Contributed to enterprise solutions for financial clients (Old Mutual, Momentum, Nedbank) across the full SDLC.

Software Engineer - Technology Systems Solutions | Oct 2011 – Nov 2012

- Built Java backends and HTML UIs for various environments; early full‑stack experience.