Insight AI

CLIENT STORY

Automating Trust: How Insight AI Secured Cloud Infrastructure for a Public Sector Healthcare Provider



Healthcare

Story Snapshot

A regional organisation within the UK's public healthcare system faced critical infrastructure challenges, including manual cloud operations and significant security vulnerabilities.

With a pressing need to streamline operations, enhance security, and establish scalable best practices, the client turned to Insight AI. Through tailored DevOps consultancy and implementation, Insight AI has been delivering a secure, automated cloud infrastructure—empowering the healthcare provider to operate with confidence and agility in a highly regulated environment.

The Challenge

The healthcare provider's existing infrastructure had been built manually by internal staff, lacking automation, proper version control, and formalised QA processes. This exposed the system to potential data leaks and made maintaining operational continuity dependent on a small internal team.

With security scans revealing vulnerabilities and an urgent need to modernise, the organisation needed to:

- Automate infrastructure and implement DevOps best practices.
- Remediate security issues identified through internal tools and penetration testing.
- Establish governance and version control across cloud infrastructure and databases.
- Introduce CI/CD capabilities to support agility and reduce manual overhead.

Further constraints included a restricted budget typical of public sector projects, internal capacity limitations, and the need for full compliance with NHS-specific regulatory and data security frameworks.





The Solution

Insight AI partnered closely with the client's lead architect to implement a secure, scalable DevOps framework. The engagement began with auditing existing infrastructure and understanding client-specific security requirements.

Strategic Approach

Working in Kanban methodology, Insight AI engineers proposed to develop a roadmap based on existing JIRA epics and closely aligned the backlog with high-priority security fixes and infrastructure automation goals.

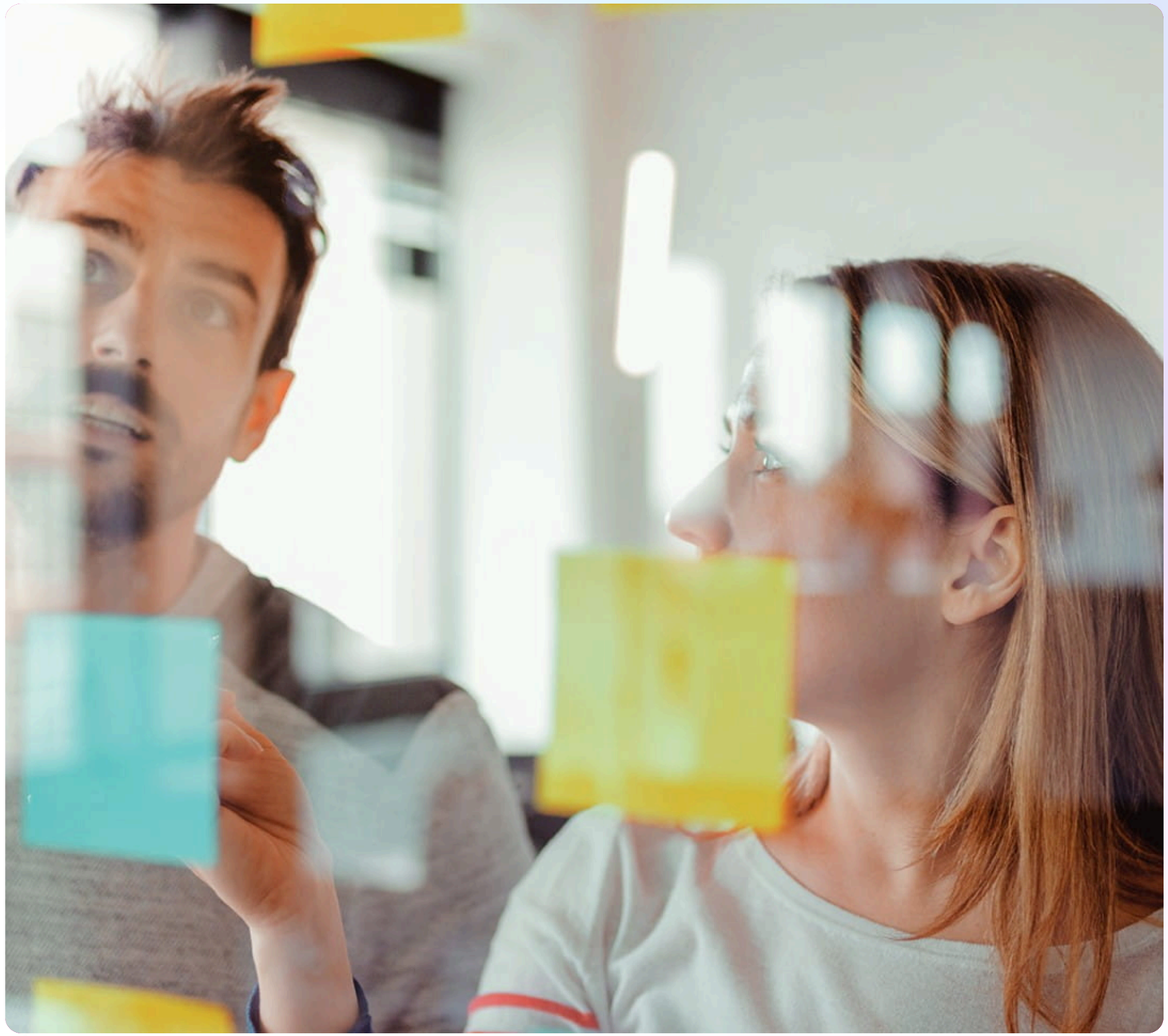
Technology Stack

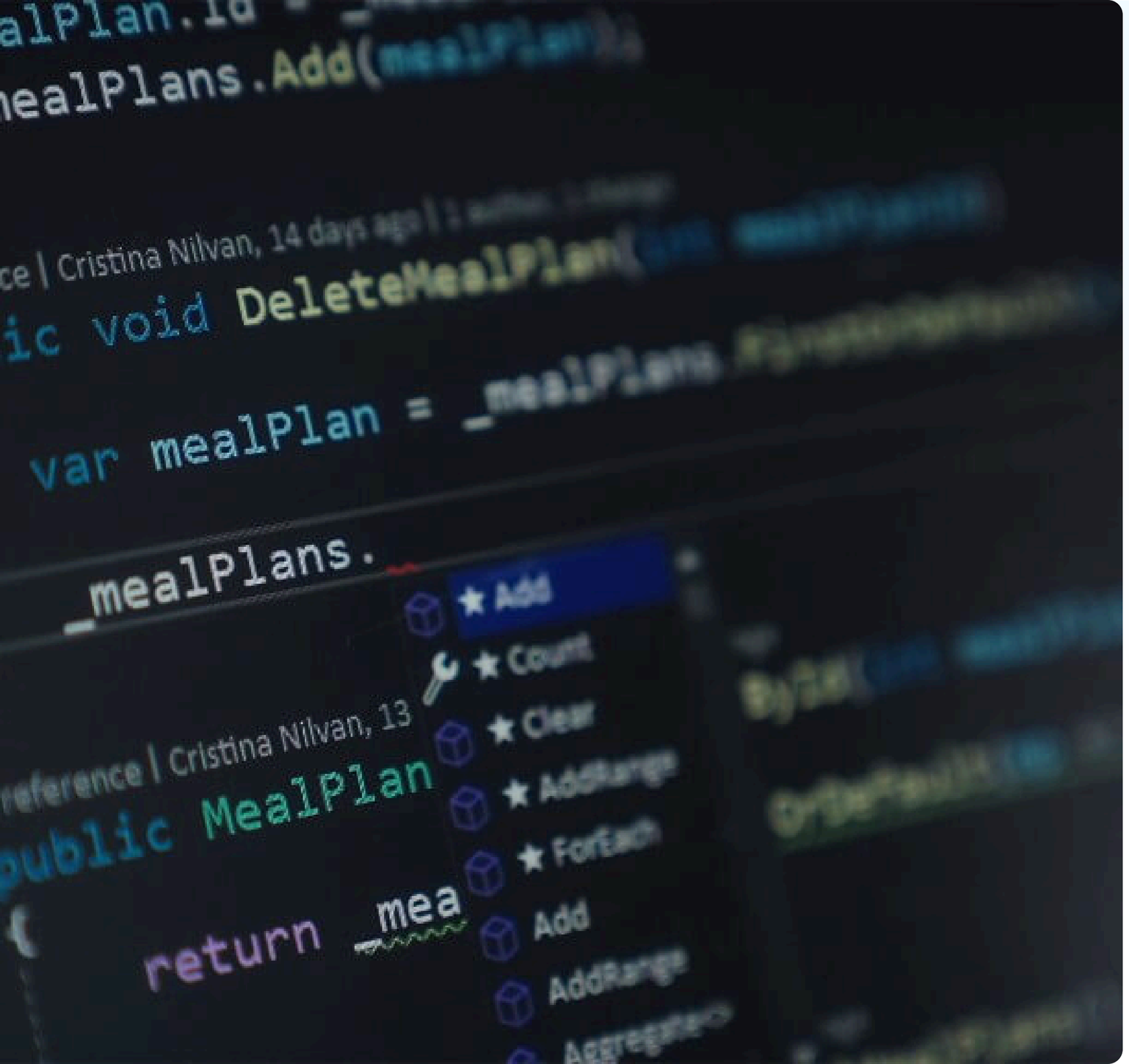
- **Infrastructure & Automation:** Terraform, Terraform Cloud.
- **Cloud Services:** AWS (RDS Aurora, RDS PostgreSQL, Redshift, QuickSight, Lambda, etc), Azure (Function Apps, Storage Accounts, SSO, Power BI).
- **Languages/Tools:** Python, Bash, GitHub Actions, JIRA, Confluence, Datadog.
- **Security & Compliance:** Use of AAD credentials for AWS access, proactive detection policies, version control for infrastructure and databases.

Results

- **Efficiency Gain:** Reduced manual configuration.
- **Security Compliance:** Remediated critical vulnerabilities and implemented monitoring.
- **Operational Agility:** Faster iteration via CI/CD pipelines.
- **Infrastructure Visibility:** All changes trackable, auditable, reversible.
- **Stakeholder Enablement:** Freed internal personnel for strategic focus.

The solution also laid the foundation for future enhancements without requiring a complete rebuild—maximising the client's investment.





Technical Highlights

- **Agile Delivery:** Kanban methodology with iterative releases.
- **Key Milestones:** Infrastructure audit, IaC implementation, CI/CD setup, pentest remediation.
- **Integration & Migration:** Transitioned to version-controlled automated environments.
- **Testing & Deployment:** GitHub Actions pipelines for traceability and minimal risk.

Bespoke Features:

- Full visibility of cloud changes via GitHub and CI/CD pipelines.
- Pentest remediation and real-time monitoring using Datadog.
- Transition to infrastructure-as-code to support audibility and rollback.
- Introduced version control across key cloud assets and datasets.
- Introduced docker container application from client's virtual machines (for a better scalability and maintenance).

All solutions are custom-built to address the organisation's unique limitations, compliance requirements, and long-term scalability needs.



Why Insight AI?

The client partners with Insight AI for its ability to deliver with transparency, technical precision, and consistent communication—critical factors in a public sector environment where previous engagements had faltered. Insight AI was chosen over competitors due to:

- **Proven DevOps expertise** and experience in cloud-first, compliance-driven sectors.
- **Strong collaborative ethos,** including regular syncs and detailed progress updates.
- **Ability to deliver cost-effective, future-ready solutions** under public sector constraints.

Insight AI

Thank you for reading

Confidentiality Statement

This document contains confidential and proprietary information belonging to Insight AI. It is intended solely for use by authorised personnel for understanding and implementing the tone of voice guidelines outlined herein.

Unauthorised disclosure, distribution, or copying of any part of this document is strictly prohibited. If you are not the intended recipient, please notify the sender immediately and delete this document from your system.

By accessing this document, you agree to maintain its confidentiality and to abide by the guidelines set forth by Insight AI for the protection of its intellectual property.