springline ADVISORY

Technology Advisory Case Study

Industry: Construction

Services: DevSecOps, Continuous Integration & Deployment

Technologies: Azure DevOps, SOOS, Microsoft .NET

Situation

A recent client was operating a platform where contractors could view plans, upload bids, and manage project documents. This system was critical for keeping projects moving and ensuring fair, timely bidding. However, manual deployments slowed down updates and introduced the risk of errors — potentially disrupting access to plans and bid submissions. Security was also a top priority, as vulnerabilities could expose sensitive financial and project data.

Solution

The team at MarksNelson, a Springline company, implemented automated pipelines in Azure DevOps to handle deployments for this platform. This eliminated manual steps, reduced human error, and ensured that updates would roll out quickly and reliably.

To strengthen security, the team integrated SOOS vulnerability scanning into the pipeline. Every code update is scanned automatically, and weekly scheduled scans provide an extra layer of protection. This proactive approach allows the team to catch vulnerabilities early, often before they're publicly disclosed, which helps protect the platform and user data.

Additional safeguards include code quality checks, automated testing, and role-based access controls, ensuring compliance and reducing operational risk.

Results

By adopting this DevSecOps approach, the team achieved:

- Zero manual deployment errors, ensuring uninterrupted access to plans and bidding tools
- Faster, more reliable release cycles improving the user experience for contractors and suppliers
- Early detection of vulnerabilities, protecting sensitive bid and project information
- Improved security posture through continuous scanning and compliance controls

This approach makes deployments secure, efficient, and repeatable — helping teams deliver high-quality software quickly without sacrificing security.