snp technologies inc.

DevOps on Azure with GitHub

8 Week Implementation

Estimated cost- $25k

DevOps simplifies deployment from your repository to Azure using GitHub and GitHub Enterprise. By leveraging GitHub Actions, GitHub Issues, GitHub Codespaces, and GitHub Advanced Security, you can package and publish code, create GitHub web pages, automate, customize, and execute CI/CD.

With DevOps on Azure using GitHub, you can enable capabilities such as:

- Infrastructure: A standard template deployment across organizations using GitHub Actions pipelines.
- GitHub Actions: Automate, customize and execute workflows and discover, create, and share actions across the organization.
- Code security: Enable secret scanning, code scanning, and Dependabot alerts. Customize analysis with CodeQL packs.
- Administration: Manage access to your data, authentication, billing management, project insights, security, and customized settings.
- Enterprise Cloud: Harden security, hosted compute networking, IAM, Enforce policies, monitor user activity, and GitHub advanced security.

SNP's 4 Week Implementation Includes:

During our 4-week engagement, we will assess your repository, source code, current CI/CD practices, authentication, code security, open-source GitHub packages, and code merging practices with a proof of concept. We will then provide a customized approach and design to meet your needs.

Our 4 Step Approach:

Our engagement will include end-to-end DevOps using GitHub practices, such as:

1. Infrastructure as Code: A standard template for deploying your infrastructure resources using GitHub Actions and reusable workflows.
2. Source code management: GitHub Repos for managing application source code and separate repository for reusable workflows.
3. CI/CD: GitHub Actions for end-to-end DevOps setup and deployment to Azure services IAAS and PAAS platforms.
4. Documentation, Knowledge Transfer, with day-2 managed support

During our 4-week engagement, we will assess your repository, source code, current CI/CD practices, authentication, code security, open-source GitHub packages, and code merging practices with a proof of concept. We will then provide a customized approach and design to meet your needs.

Step 1: Infrastructure as code

- Assess/Learn about current infrastructure workloads.
- Identify the resource components required for the code-base deployment.
- Evaluate the network topology in line with best practices and potential for expansion (e.g., multi-cloud)
- Review the current security, governance, and identity practices.
- Prepare scripts for identified resources considering best
- practices – Terraform/ARM/Bicep.
- Standardize the template for at-scale deployment.
- Set up GitHub actions for deployment, and reuse workflows.
- Plan and test the standard template by deploying it to Sandbox Subscriptions using GitHub actions.
- Roll out to the production environment in the next steps.

Step 2: Source code management

- Assess, review, and understand your SDLC process, Branching strategy, Code review process, Pull requests and approvals, and Feature and hotfix release strategies.
- Understand repository structure, authentication, and permissions process.
- Identify and remove secrets in code and perform source code scanning for vulnerabilities leveraging GitHub Advanced Security
- Incorporate secret management tools to secure sensitive data
- Implements a proper and standardized workflow to simplify code management using GitHub Repos
- Secure access to GitHub repositories using access management policies.
- Protect branches using branch protection rules and PR merge methods.
- Validate and enhance security practices including user activities on the repository.
- Modernize applications to microservices to enhance performance and minimize downtime during maintenance.
- Manage self-hosted runners, caching dependencies, and storing artifacts.

Step 3: Continuous Integration and Continuous Deployment using GitHub Actions

Assess:

- Assess, review, and understand the current continuous integration and continuous deployment process.
- Pipeline policies, security, trigger events, and approval process for promoting to production environments.
- Current secret store integrations, Variables, and environment configuration files in the code.
- Containerize applications

Implement:

- Create a multi-stage GitHub workflow for more visibility, simplicity, and easier integrations using GitHub Actions.
- Connect to Azure using federated identity for deployments
- Set up self-hosted runners if required
- Ensure consistent build and deployment using GitHub Actions.
- Create, publish, consume and manage build artifacts using GitHub Packages.
- Cache workflow dependencies using GitHub cache actions for faster and more efficient workflows.
- Create reusable workflows to avoid duplication and quickly create new workflows.
- Leverage code scanning and secret scanning tools to identify vulnerabilities using GitHub Advanced Security.
- Implement deployment strategy to avoid downtime and last-minute failures.
- Implement image scanning for containerized applications.

Step 4: Documentation, Knowledge Transfer and Day-2 support

- As built documentation

  For discovery findings
  Planning document
  Defining solution architecture components
  Infrastructure deployment process document
  Build and release pipelines document – GitHub Actions
  Recommendations and best practices document.

- Templates - Terraform/ARM, reusable workflows, workflow templates, and Helm charts.
- Knowledge Transfer and Day-2 Support

  Hand over the documentation for review
  2 KT sessions to showcase the End-to-End DevOps process using GitHub
  Leverage SNP's DevOps on Azure using GitHub for simplifying deployment and for Day-2 support

snp technologies inc. Microsoft Azure

About SNP Technologies Inc.

SNP's consulting services help businesses of all sizes transform with innovative, cloud-based solutions that harness the power of Microsoft Azure.

We combine elements from our ISO certifications and Microsoft specializations as well as the most efficient and innovative technology tools and platforms to help our clients become more agile, more customer focused and more operationally efficient.

Member of
Microsoft Intelligent Security Association
Microsoft

TÜV NORD
TÜV NORD CERT GmbH
ISO/IEC 20000-1
ISO 20000-1:2018:
Service Management System

TÜV NORD
TÜV NORD CERT GmbH
ISO 22301
ISO 22301:2019:
Business Continuity Management System

TÜV NORD
TÜV NORD CERT GmbH
ISO/IEC 27001
ISO 27001:2013:
Information Security Management System

Let's move forward together with confidence. We're here to help at every step.

Email us: SNP's COO Prakash Parikh: prakash@snp.com