leaven.

Azure DevSecOps Service

Integrate security practices within your DevOps process to ensure ongoing auditing and maintenance

For organisations deploying applications on Microsoft Azure, speed and agility of development often results in security taking a back seat. The Azure DevSecOps Service automates security processes and continuous auditing enabling security being approached proactively within your development lifecycle.

Why consider Azure DevSecOps?

Adopting and implementing Security practices and methodologies is not an easy process and often seen as hinderance to cloud adoption and uptake, slowing down the momentum of developers who want to demonstrate progress. Consequently, security is considered as a milestone within a project, typically towards the end, and is often a manual process.

Typically, DevOps methodologies, tools and practices dilute the importance of security and it becomes an afterthought, leading to project delays or causing complexity and rework, between teams and, due to its manual nature, can result in some issues being missed.

The Azure DevSecOps Service enables security to be automated and a pervasive part of an organisation's entire development cycle. This ensures security is addressed proactively, reducing risk.

Azure DevSecOps helps organisations review their current security posture and take remedial steps to mitigate vulnerabilities on an ongoing basis. Reports are generated automatically on a pre-scheduled basis, ensuring any issues can be proactively raised and addressed by the development team.

The Azure DevSecOps Service enables organisations to adopt a secure development practice, leading to a robust and secure CI/CD process, every time.

Why do an Azure DevSecOps Review?

Key benefits of this offering include:

- Understand the current security profile of your Azure tenancy and Azure DevOps organisation and your current projects.
- Post audit, take remedial actions to quickly close vulnerabilities and adopt better secure development processes.
- Embed this process through workshops that help your organisation adopt their custom security posture.
- Reduce risk by automating security checking and reporting, allowing you to respond to gaps quickly.

Improved productivity

Azure DevSecOps is an enabler to better development practice leading to a secure and collaborative CI/CD development process, every time.

Integrated security

Azure DevSecOps enables security to be baked in development projects, enabling it to change continuously to the varying state of the project.

Maximise investment

Azure DevSecOps enables security to be automated, minimising vulnerabilities and aligning security closer to IT and business objectives.

leaven.

Azure DevSecOps Service: Helping ensure applications and workloads are always secure

Approach

The Azure DevSecOps Service comprises three key parts.

1. **Initial security review:** We create a baseline of understanding by using a range of tools to scan, audit and report on the current Azure subscriptions and Azure DevOps. Findings are discussed in a workshop format with key stakeholders, with one outcome to apply any fixes to all identified vulnerabilities.

2. **Application development security review:** We look at the security of application development using a range of leading toolsets. This can range from Threat modeling, Static Code Analysis, Security Verification Tests, Secure Cloud Configurations, IaC, Policy management.

3. **Secure Azure SecDevOps review:** Delivery of a formal report and presentation outlining high-level recommendations for both quick wins and long-term improvements – with identified next steps. This would also involve setting up Secure Development Framework for existing and future projects to adopt and implement.

Optional next steps
Following the completion of the Azure DevSecOps Service engagement, Leaven can help your organisation develop scheduled scans and automated report generation in a custom scheduled manner. This could potentially be incorporated into an ongoing management process.

Leaven Azure DevSecOps Service

Key scenarios

- Provide a completely secure platform for the development of native cloud applications, built on Microsoft Azure.
- Ensure that application code is being written to the highest security standards, and that vulnerability controls are checked automatically and addressed immediately.
- Require policies and procedures that help ensure that CI/CD pipelines are built and using security best practices.

Leaven is the cloud transformation business unit of CCL, New Zealand's largest locally-focused IT and cloud services company.

Find out more at www.concepts.co.nz.

About Leaven

Leaven enables New Zealand organisations to accelerate cloud adoption, digital innovation and business transformation.

We apply proven methodologies to enable your organisation to adopt public cloud services, innovate on the foundation they provide, and optimise and manage your environment, while maintaining governance and compliance requirements.