Cloud Fuel

Secure applications in Azure

For those who

- Are deploying or managing applications in Azure and want to ensure they are secure.
- Need to implement identity and access management to protect resources.
- Seek guidance in configuring network security, including firewalls and private endpoints.

Who will attend

Developers, IT operations, security engineers, and cloud architects.

Ensuring the security of your applications in Azure is crucial in today's threat landscape. CloudFuel helps you implement best practices for securing your applications in Azure by leveraging Azure's built-in security tools and services. From identity management to networking and security, we guide you in building a robust, secure, and compliant cloud environment.

The process

STEP 1

Introduction to Azure Security

Overview of Azure security tools and services. Importance of a layered security approach.

STEP 2

Identity and Access Management

Hands-on configuration of Azure Active Directory (AAD), role-based access control (RBAC), and managed identities. Implement multi-factor authentication (MFA) and conditional access policies.

STEP 3

Securing the Network

Configure network security groups (NSGs), Azure Firewall, and private endpoints. Best practices for securing virtual networks and enabling encrypted connections.

STEP 4

Vulnerabilities and Monitoring

Set up Microsoft Defender for Cloud and Azure Security Center. Learn how to monitor and respond to threats.

STEP 5

Compliance and Governance

Implement Azure Policy and Blueprints to enforce compliance. Explore tools for auditing and reporting to meet regulatory requirements.

Deliverables

Training
on Azure security tools and practices.

Documentation
of best practices, workshop outcomes, and actionable next steps.

info@cloudfuel.be
+32 498 88 15 74

Veldkant 33A
2250 Kontich