RealTime Handson

10

DevSecOps

AZURE CLOUD
PROJECTS

PART 1

CREATING LEADERS

1. Secure CI/CD Pipeline with Azure DevOps and Azure Key Vault

Use Case

- Securely store and manage sensitive credentials, API keys, and certificates in **Azure Key Vault** and use them in a **CI/CD pipeline**.
- Automate deployment while ensuring secrets are never exposed in the pipeline.

Architecture

- **Azure DevOps** for CI/CD pipeline
- **Azure Key Vault** for secrets management
- **Azure App Service** as the deployment target

Implementation Steps

Step 1: Set Up Azure Key Vault
Create an **Azure Key Vault**:

```
az keyvault create --name MyDevSecOpsVault --resource-group DevSecOpsRG
--location eastus
```

Add a secret:

```
az keyvault secret set --vault-name MyDevSecOpsVault --name "DatabasePassword"
--value "MySecurePass123"
```

Step 2: Configure Azure DevOps Pipeline

1. **In Azure DevOps,** go to **Library > Variable Groups** and create a **new group.**
2. **Link the Key Vault** by selecting **Azure Key Vault as the source** and choose your vault.
3. **Add the secret from Key Vault** to the pipeline.

Step 3: Create a CI/CD Pipeline
Create a YAML pipeline (azure-pipelines.yml):

```
trigger:
 - main

pool:
```

```
  vmImage: 'ubuntu-latest'

variables:
  databasePassword: $(DatabasePassword)

steps:
  - task: UseAzureKeyVault@1
    inputs:
      azureSubscription: 'MyAzureServiceConnection'
      KeyVaultName: 'MyDevSecOpsVault'
      SecretsFilter: '*'

  - script: echo "Deploying application..."
    env:
      DB_PASSWORD: $(databasePassword)
```

Step 4: Deploy Securely to Azure App Service
Use Azure CLI in pipeline:
 az webapp config appsettings set --name MyWebApp --resource-group DevSecOpsRG --settings DB_PASSWORD=$(databasePassword)

1. Validate that the app retrieves **secrets securely**.

---

2. Implementing Azure Policy for Secure DevOps

Use Case

- Enforce security policies automatically in Azure using **Azure Policy**.
- Prevent insecure configurations (e.g., blocking public storage access).

Implementation Steps

Step 1: Create an Azure Policy

1. Go to **Azure Portal > Policy > Assignments > Assign Policy**.
2. Select **Built-in Policy**: "Storage accounts should restrict public access."
3. Set **Scope** to the subscription or resource group.

Step 2: Deploy the Policy via Azure DevOps
Create a **Bicep template** for the policy:

```
resource policyAssignment 'Microsoft.Authorization/policyAssignments@2022-06-01' =
{
  name: 'RestrictPublicStorage'
  properties: {
    displayName: 'Restrict Public Storage'
    policyDefinitionId:
'/providers/Microsoft.Authorization/policyDefinitions/abc123'
    scope: resourceGroup().id
  }
}
```

Deploy the policy in a **DevOps pipeline**:

```
- task: AzureCLI@2
  inputs:
    azureSubscription: 'MyAzureServiceConnection'
    scriptType: 'bash'
    scriptLocation: 'inlineScript'
    inlineScript: |
      az deployment group create --resource-group DevSecOpsRG --template-file
policy.bicep
```

1. Validate by trying to create a public storage account.

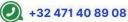# 3. Securing Containerized Applications using Azure Defender for Kubernetes

Use Case

● Monitor and secure a **Kubernetes cluster** using **Azure Defender** to detect threats.

Implementation Steps

Step 1: Enable Azure Defender for Kubernetes
Run the following CLI command:

CAREER BYTE CODE

REALTIME PROJECTS PLATFORM

91 COUNTRIES   241k Learners
subscriber

+32 471 40 89 08

CAREERBYTECODE.SUBSTACK.COM

```
az security pricing create --name KubernetesService --tier Standard
```

Step 2: Deploy a Kubernetes Application
Deploy a sample **NGINX** app:

```
kubectl create deployment nginx --image=nginx
```

Expose the app:

```
kubectl expose deployment nginx --type=LoadBalancer --port=80
```

Step 3: Monitor Security Events

1. Go to **Azure Security Center > Azure Defender > Kubernetes**.
2. View security recommendations.

---

4. Identity & Access Management with Azure AD for DevOps

Use Case

- Implement **RBAC (Role-Based Access Control)** to restrict access to DevOps pipelines.

Implementation Steps

Step 1: Configure Azure AD Roles
Create an Azure AD group:

```
az ad group create --display-name "DevSecOpsAdmins" --mail-nickname
"DevSecOpsAdmins"
```

1. Assign the **Azure DevOps administrator role** to this group.

Step 2: Apply RBAC to Azure DevOps

1. Go to **Azure DevOps > Organization Settings > Security**.
2. Assign **specific roles** to users.

5. Infrastructure as Code Security with Terraform & Sentinel

Use Case

- Enforce security guardrails in **Terraform deployments**.

Implementation Steps

Step 1: Create Sentinel Policies
Write a Sentinel policy to prevent public storage accounts:

```
policy "no_public_storage" {
  enforcement_level = "hard-mandatory"
  query = rule {
    all aws_s3_bucket as bucket {
      bucket.public_access_block_enabled is true
    }
  }
}
```

Step 2: Deploy Policy in Terraform Cloud

1. **Enable Sentinel Policy** in Terraform Cloud.
2. Run a **Terraform apply** to test the enforcement.

6. Static Code Analysis in DevOps Pipeline

Use Case

- Detect vulnerabilities in source code using **SonarCloud** in Azure DevOps.

Implementation Steps

Step 1: Configure SonarCloud

1. **Sign up** for SonarCloud.
2. Create a **SonarCloud token**.

Step 2: Integrate SonarCloud in DevOps

Add SonarCloud **Prepare Analysis task** in the pipeline:

```
- task: SonarCloudPrepare@1
  inputs:
    SonarCloud: 'SonarCloud'
    organization: 'my-org'
    projectKey: 'my-project'
```

---

7. Dynamic Application Security Testing (DAST) with OWASP ZAP

Use Case

- Scan **running applications** for security vulnerabilities.

Implementation Steps

Step 1: Install OWASP ZAP
Add a **ZAP Scan task** to the pipeline:

```
- task: OWASPZAP@2
  inputs:
    targetUrl: 'https://myapp.com'
```

Review **vulnerability reports** in DevOps logs.

---

8. Zero Trust Networking in Azure with Private Endpoints

Use Case

- Securely access **Azure services** over **private networks**.

Implementation Steps

Step 1: Create a Private Endpoint
Deploy a **private link** to an Azure SQL Database:

```
az network private-endpoint create --name PrivateSQL --resource-group DevSecOpsRG
--vnet-name MyVNet --subnet MySubnet --private-connection-resource-id
"/subscriptions/.../sqlServers/MySQLServer"
```

Step 2: Validate Secure Access

Try accessing the database from an **external network** (should be blocked).

---

9. Implementing Azure Sentinel for DevOps Monitoring

Use Case

- Monitor security events from **DevOps pipelines**.

Implementation Steps
Enable Azure Sentinel:
az sentinel workspace create --resource-group DevSecOpsRG --name SentinelWorkspace

   1.

Connect Azure DevOps logs:

```
az sentinel data-connector create --name DevOpsLogs
```

---

10. Secure API Gateway with Azure APIM & OAuth

Use Case

- Protect **APIs** using **OAuth authentication**.

Implementation Steps

Step 1: Deploy Azure API Management

Deploy APIM:

```
az apim create --name MyAPIM --resource-group DevSecOpsRG
```

1. Configure OAuth in **APIM policies**.

→ **TRAININGS**

WE ARE DIFFERENT

At CareerByteCode, we redefine training by focusing on real-world, hands-on experience. Unlike traditional learning methods, we provide step-by-step implementation guides, 500+ real-time use cases, and industry-relevant projects across cutting-edge technologies like AWS, Azure, GCP, DevOps, AI, FullStack Development and more.

Our approach goes beyond theoretical knowledge—we offer expert mentorship, helping learners understand how to study effectively, close career gaps, and gain the practical skills that employers value.

16+
Years of operations

91+
Countries worldwide

241 K Happy clients

🌐 **Our Usecases Platform**
https://careerbytecode.substack.com

🌐 **Our WebShop**
https://careerbytecode.shop

CareerByteCode
All in One Platform

CareerByteCode
Learning Made simple

STAY IN TOUCH WITH US!

Website

Our WebShop https://careerbytecode.shop
Our Usecases Platform https://careerbytecode.substack.com

E-mail
careerbytec@gmail.com

Social Media
@careerbytecode

Phone
+32 471 40 8908

HQ address
Belgium, Europe

CAREER BYTE CODE

REALTIME PROJECTS PLATFORM

91 COUNTRIES **241k Learners**

subscriber

+32 471 40 89 08

www

CAREERBYTECODE.SUBSTACK.COM

→ **CLOUD DEVOPS TRAINING**

REALTIME HANDON 6 MONTHS

WEEK 1-2

📌 **1 Year Platform Subscription Azure Cloud**

WEEK 3-6

Azure Cloud & Ansible & Docker

WEEK 7-10

Kubernetes & DevOps CI/CD

WEEK 11-12

Terraform & Automation

WEEK 13 – 16

Azure DevOps & Azure DevSecOps Assesment & Q&A

WEEK 17 – 22

Resume Writing 30 RealTime Projects Job Search

WEEK 23 – 24

Secure Job as an Leader

500+ RealTime Handson Usecases

Our Usecases Platform   https://careerbytecode.substack.com

CONTACT US   📞 **+32 471 40 8908**

For any RealTime Handson Projects

And for more tips like this

Follow

CareerByteCode

Like & ReShare

@careerbytecode