Implement security through a pipeline using Azure DevOps (AZ-2001)

Description

Enhance the Security of Your DevOps Pipelines with Azure

Securing pipelines is essential to ensuring the integrity and reliability of deployments in a cloud environment. With our AZ-2001 training, you will learn how to implement security within a DevOps pipeline. This structured course guides you step by step through configuring Azure Pipelines, managing access, and securing repositories.

A Comprehensive Training to Master Pipeline Security

Through detailed modules and hands-on exercises, you will learn how to set up secure repositories, manage identities, and strengthen access to critical resources. This program will help you master the use of Azure DevOps, Azure Repos, and Azure Artifacts, while applying best practices in cybersecurity.

Course Content
Module 1: Configure a Secure Project and Repository Structure

- Organize project and repository structure
- Configure secure projects and repositories
- Move security repository away from the application project

Module 2: Configure Secure Access to Pipeline Resources

- Configure agent pools
- Use secret variables and variable groups
- Understand secure files
- Configure service connections
- Manage environments
- Secure repositories

Module 3: Manage Identity for Projects, Pipelines, and Agents

- Configure a Microsoft-hosted pool
- Configure agents for projects
- Configure agent identities
- Configure the scope of a service connection
- Understand and convert to a managed identity

Module 4: Configure and Validate Permissions

- Configure and validate user permissions
- Configure and validate pipeline permissions
- Configure and validate approval and branch checks
- Manage and audit permissions

Module 5: Extend a Pipeline to Use Multiple Templates

- Create a nested template
- Rewrite the main deployment pipeline
- Configure the pipeline and the application to use tokenization
- Remove plain text secrets
- Restrict agent logging
- Identify and conditionally remove script tasks

Module 6: Configure Secure Access to Azure Repos from Pipelines

- Configure pipeline access to packages
- Configure pipeline access to credential secrets
- Configure pipeline access to secrets for services
- Use Azure Key Vault to secure secrets
- Explore and secure log files

Module 7: Configure Pipelines to Securely Use Variables and Parameters

- Ensure parameter and variable types
- Identify and restrict insecure use of parameters and variables
- Move parameters into a YAML file
- Limit queue time variables
- Validate mandatory variables

Lab / Exercises

- This course provides you with exclusive access to the official Microsoft lab, enabling you to practice your skills in a professional environment.

Documentation

- Access to Microsoft Learn, Microsoft's online learning platform, offering interactive resources and educational content to deepen your knowledge and develop your technical skills.

Participant profiles

- Security operations analysts
- Cloud solutions architects
- DevOps engineers

- Developers specializing in secure deployment
- System administrators working on Azure

Prerequisites

- Basic knowledge of Azure DevOps and pipeline concepts
- Understanding of security principles (identities, permissions, and authentication)
- Experience with the Azure portal and cloud resource management

Objectives

- Configure a secure project and repository structure
- Manage secure access to pipeline resources
- Implement identity strategies and permission management
- Establish advanced permissions for users and pipelines
- Extend a pipeline by applying secure templates
- Restrict access to Azure Repos and manage secrets
- Secure the use of variables and parameters in pipelines

Description
Implement security through a pipeline using Azure DevOps (AZ-2001)
Niveau
Intermédiaire
Classroom Registration Price (CHF)
900
Virtual Classroom Registration Price (CHF)
850
Duration (in Days)
1
Reference
AZ-2001