Startel
Dé IT-opleider

Microsoft: Implement security through a pipeline using Azure DevOps Zelfstudiepakket

In dit zelfstudiepakket zit het officiële cursusmateriaal, een labomgeving en een achievement code (badge). Je hebt 180 dagen toegang tot de labomgeving.

Algemene omschrijving

In dit zelfstudiepakket zit het officiële cursusmateriaal, een labomgeving en een achievement code (badge). Je hebt 180 dagen toegang tot de labomgeving.

Het zelfstudiepakket Microsoft: Implement Security Through a Pipeline Using Azure DevOps is specifiek ontworpen om professionals te voorzien van de benodigde kennis en vaardigheden om beveiliging naadloos te integreren in hun DevOps-praktijken. Door dit zelfstudiepakket door te nemen leer je hoe jij een sterke beveiligingscultuur kunt opbouwen binnen jouw ontwikkelteams en processen, met behulp van Azure DevOps als het centrale platform.

Dit zelfstudiepakket neemt je mee op een diepgaande reis door de verschillende aspecten van het implementeren van beveiliging binnen jouw CI/CD-pijplijnen. In dit zelfstudiepakket ontdek je hoe Azure DevOps jou kan helpen bij het automatiseren van beveiligingstaken, het vroegtijdig identificeren van kwetsbaarheden en het waarborgen van de naleving door het gehele ontwikkelproces. Van het instellen van beveiligde ontwikkelpraktijken tot aan het beheren van toegangsrechten en het configureren van beveiligingsbeleid, dit zelfstudiepakket behandelt alle essentiële gebieden.

Dit zelfstudiepakket zorgt ervoor dat je up-to-date blijft met de meest recente beveiligingsmethoden en -hulpmiddelen binnen Azure DevOps. Door dit zelfstudiepakket door te nemen krijg je inzicht in hoe jij deze toe kunt passen om jouw projecten veiliger te maken. Of het nu gaat om het werken aan zakelijke of persoonlijke projecten, in dit zelfstudiepakket leer je hoe jij de integriteit en veiligheid van jouw applicaties kunt waarborgen.

Doelgroep

Het zelfstudiepakket Microsoft: Implement Security Through a Pipeline Using Azure DevOps is een essentiële stap voor professionals die zich inzetten voor het ontwikkelen van veilige en robuuste softwareoplossingen.

Door deel te nemen aan dit zelfstudiepakket verbeter je niet alleen jouw eigen kennis en vaardigheden op het gebied van cybersecurity, maar draag je ook bij aan het verhogen van de algemene beveiligingsstandaarden binnen jouw organisatie.

Dit zelfstudiepakket is met name geschikt voor de volgende mensen:

- **Softwareontwikkelaars**
  - Door dit zelfstudiepakket door te nemen leren softwareontwikkelaars hoe ze beveiligingspraktijken kunnen integreren in hun dagelijkse werkzaamheden, waardoor de veiligheid van de software vanaf het begin wordt gewaarborgd.
- **DevOps-specialisten**
  - DevOps-specialisten die de brug vormen tussen softwareontwikkeling en systeembeheer, zullen ontdekken hoe ze op een effectieve manier beveiligingsmaatregelen kunnen integreren in CI/CD-pijplijnen met Azure DevOps. Dit stelt hen in staat om een veilige softwareleveringspijplijn te ontwikkelen en te onderhouden, wat essentieel is voor het beschermen tegen beveiligingsrisico's.
- **Cybersecurityprofessionals**
  - Voor diegenen die zich specifiek richten op het beveiligen van informatiesystemen, biedt dit zelfstudiepakket inzicht in hoe Azure DevOps kan worden gebruikt om beveiligingstaken te automatiseren en te verbeteren.
  - Dit zelfstudiepakket helpt cybersecurityprofessionals om beveiligingsbeleid en -controles naadloos te integreren in de ontwikkelings- en operationele processen.
- **Cloudarchitecten**
  - Cloudarchitecten die verantwoordelijk zijn voor het ontwerpen van veilige cloudinfrastructuur en -oplossingen zullen in dit zelfstudiepakket leren hoe ze Azure DevOps kunnen gebruiken voor het implementeren van beveiligingspraktijken in cloudgebaseerde projecten, wat cruciaal is voor het handhaven van de integriteit en beveiliging van cloudomgevingen.

Leerdoelen

Door dit zelfstudiepakket door te nemen zul je de volgende kennis en vaardigheden verkrijgen:

- Beveiligde toegang tot pijplijnbronnen configureren.
- Machtigingen configureren en valideren.
- Een project- en opslagstructuur configureren om veilige pijplijnen te ondersteunen.
- Een pijplijn uitbreiden om meerdere sjablonen te gebruiken.
- Identiteit beheren voor projecten, pijplijnen en taakagenten.

Voorkennis

Voordat je dit zelfstudiepakket doorneemt raden we aan dat jij beschikt over de volgende kennis en vaardigheden:

- Basiskennis van Azure DevOps.
- Basiskennis van beveiligingsbegrippen, zoals identiteiten en machtigingen.
- Ervaring met het gebruik van het Microsoft Azure-portaal om middelen te creëren, zoals Azure Key Vault en het configureren van toegangsrechten.

Onderwerpen

Module 1: Configure a project and repository structure to support secure pipelines

- Separate a project into team projects and repositories.
- Separate secure files between projects.
- Move the security repository away from a project.
- Assign project and repository permissions.
- Organize a project and repository structure.

Module 2: 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.
- Convert to a managed identity in Azure DevOps.

Module 3: Configure secure access to pipeline resources

- Identify and mitigate common security threats.
- Configure pipeline access to specific agent pools.
- Manage secret variables and variable groups.
- Secure files and storage.
- Configure service connections.
- Manage environments.
- Secure repositories.

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 in Azure DevOps.

Module 5: Extend a pipeline to use multiple templates

- Create nested templates.
- Rewrite the main deployment pipeline.
- Configure the pipeline and the application to use tokenisation.
- Remove plain text secrets.
- Restrict agent logging.
- Identify and conditionally remove script tasks in Azure DevOps.

Module 6: Configure secure access to Azure Repos from pipelines

- Configure pipeline access to packages.
- Configure credential secrets and secrets for services.
- Ensure that the secrets are in the Azure Key Vault.
- Ensure that secrets aren't in the logs.

Module 7: Configure pipelines to securely use variables and parameters

- Ensure that parameters and variables retain their type.
- Identify and restrict insecure use of parameters and variables.
- Move parameters into a YAML file that protects their type.
- Limit variables that can be set at queue time.
- Validate that mandatory variables are present and set correctly in Azure DevOps.