



**MICROSOFT SECURITY
USER GROUP
MEETUP
NORWAY / OSLO**



December Meetup

Tuesday, December 6th, 16:30 CET

Microsoft Norway

Dronning Eufemia gate 71



DevSecOps for AKS highlighting
different security controls throughout
the value chain

Kristina Devochko

Software Architect
Microsoft Azure MVP



Azure AD and DevSecOps in the context of
Azure/GitHub Enterprise

Jan Vidar Elven

Cloud Platform & Security Architect
Microsoft Security MVP





Jan Vidar Elven

Evidi AS

- Tech Lead Cloud Platform & Security
- MVP Security
- @JanVidarElven
- <https://gotoguy.blog>



“I’m an Identity & Security Expert that also do DevOps..”

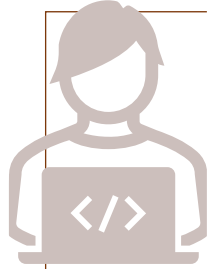


Agenda

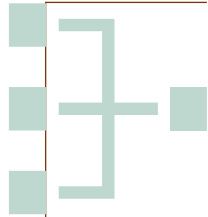
1. Enterprise Securing DevOps Environments Overview
2. Secure DevOps by Connecting Organization to Azure Active Directory
3. Overview over Defender for DevOps



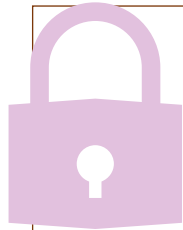
Protect the attack surfaces of Enterprise DevOps environments



Secure the
developer
environment



Secure the DevOps
platform
environments



Secure the
application
environments



Enterprise DevOps Overview

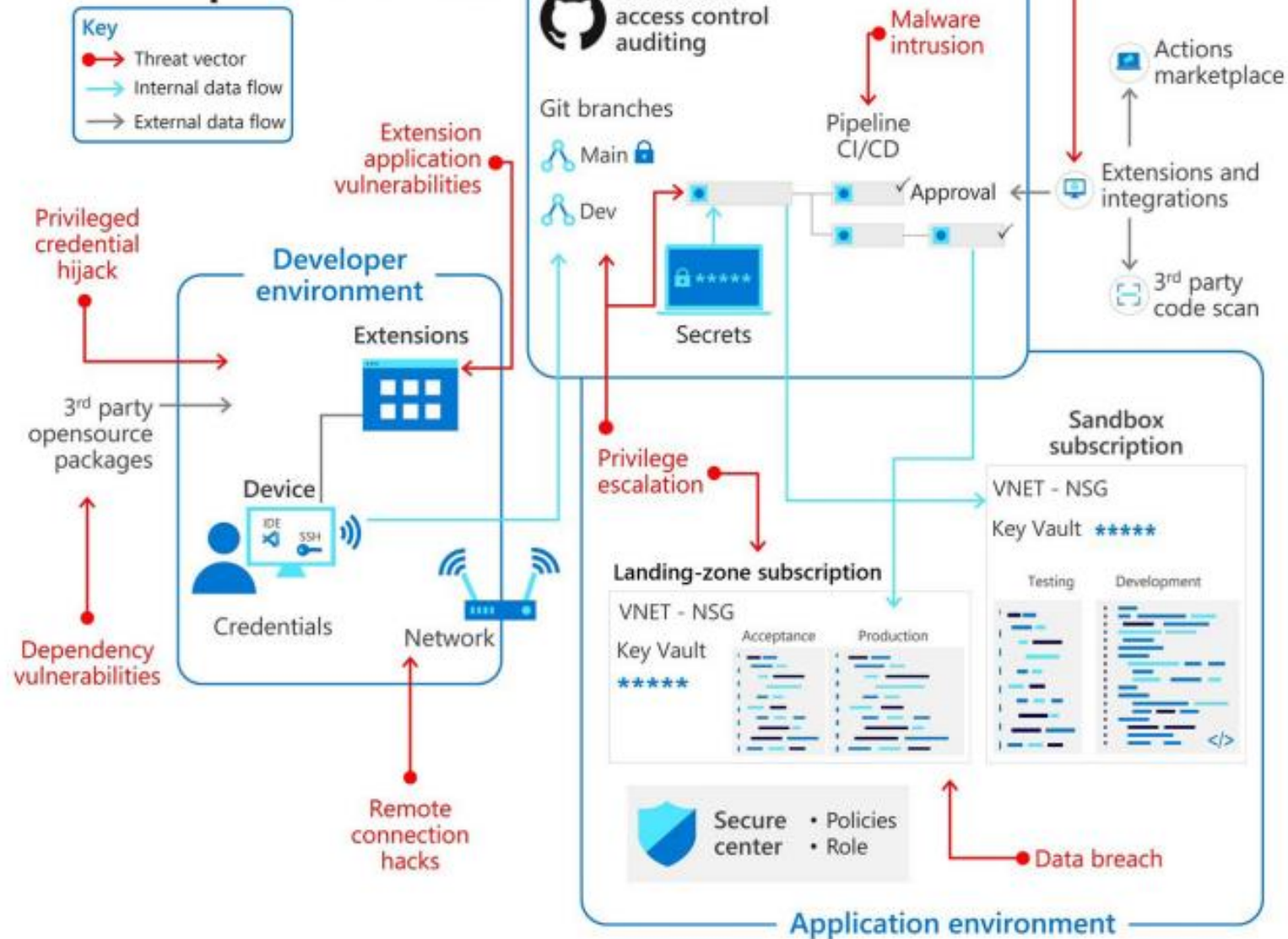


Figure 1 - Enterprise DevOps Environments Overview




Whitepaper: Securing Enterprise DevOps Environments

<https://azure.microsoft.com/en-us/resources/securing-enterprise-devops-environments/>





Secure Azure DevOps by Connecting to Azure Active Directory

 **Azure DevOps**

FabrikamFiber / Organization Settings / Azure Active Directory

Organization Settings

General

- Overview
- Projects
- Users
- Billing
- Auditing
- Global notifications
- Usage
- Extensions
- Azure Active Directory**

Azure Active Directory

Connect your organization to an Azure Active Directory.

[Follow steps and learn more](#)

Connect directory



Restrict DevOps organization creation

Microsoft Entra admin center

Home > Roles and administrators | All roles >

Azure DevOps Administrator | Assignments

Privileged Identity Management | Azure AD roles

Manage

- Assignments
- Description
- Role settings

Eligible assignments **Active assignments** Expiration

Search by member name or principal name

Name
Azure DevOps Administrator
Jan Vidar Elven (Cloud Admin)

Azure DevOps

jan.vidar@elven.no Switch directory

Almost done...

Name your Azure DevOps organization

dev.azure.com/ janvidar-test

We'll host your projects in

West Europe

Enter the characters you see

New Audio

⚠ Creating organizations is restricted in your organization. Contact your organization admin for more details.

Continue

Azure DevOps janvidarelven / Settings / Azure Active Directory

Organization Settings

janvidarelven

Search Settings

- General
 - Overview
 - Projects
 - Users
 - Billing
 - Global notifications
 - Usage
 - Extensions
 - Azure Active Directory**
- Security
 - Policies
 - Permissions
- Boards
 - Process
- Pipelines
 - Agent pools
 - Settings
 - Deployment pools

Azure Active Directory

Your organization is connected to the **Elven Azure AD** directory.

Elven Azure AD
elven.no
Tenant Id: 104742fb-...

Check out other frequently asked questions.

Disconnect directory Switch directory

Download Azure DevOps organizations connected to **Elven Azure AD** directory.

Download

Policies

Restrict organization creation ☒

If enabled, creating new organizations on the Elven Azure AD directory will be restricted from all users. People in the allow list and in the 'Azure DevOps Administrator' role are exempt from this restriction.

Allow list
Users or groups on this list will be exempt from this restriction and are allowed to create organizations. We recommend using groups. Find out more [here](#).

Add AAD user or group

Display error message
Azure DevOps organization creation is restricted in your Azure Active Directory. Contact your administrator for more details.

Edit display message



Restrictions for Personal Access Tokens (PAT)

Extensions

Azure Active Directory

Security

Policies

Permissions

Boards

Process

Pipelines

Agent pools

Settings

Deployment pools

Parallel jobs

OAuth configurations

Repos

Repositories

Artifacts

Storage

Restrict global personal access token creation

If enabled, new personal access tokens (PATs) must be associated with specific Azure DevOps organizations. Creating global tokens (tokens that work for all accessible organizations) will be restricted from all users.

Allow list

Users or groups on this list will be exempt from this restriction and are allowed to create global personal access tokens (PATs). We recommend using groups. Find out more [here](#).

Add AAD user or group

Restrict full-scoped personal access token creation

If enabled, new personal access tokens (PATs) must have limited and defined scopes. Creating full access tokens (PATs that work for all accessible scopes) will be restricted from all users.

Allow list

Users or groups on this list will be exempt from this restriction and are allowed to create full-scoped personal access tokens (PATs). We recommend using groups. Find out more [here](#).

Add AAD user or group

Enforce maximum personal access token lifespan

If enabled, the lifespan of new personal access tokens (PATs) will be limited to defined duration.

Maximum allowed lifespan for new tokens (in days)

30

Save

Allow list

Users or groups on this list will be exempt from this restriction and are allowed to create personal access tokens (PATs) with lifespans beyond the defined duration. We recommend using groups. Find out more [here](#).

Add AAD user or group

Automatically revoke leaked personal access tokens

If enabled, Azure DevOps personal access tokens (PATs) checked into public GitHub repositories will be automatically revoked. This policy applies to all PATs within Azure DevOps Organizations linked to your Azure AD tenant. [Learn More](#)

Security Best Practices for Azure DevOps

- Scope Service Accounts, Service Connections & Permissions
 - GitHub Connections
 - External guests
- Authentication Methods
 - Require MFA / Conditional Access
 - Limit use of PAT -> Use Identity Platform
- Control Network Access
- Secure Projects and DevOps Services

<https://learn.microsoft.com/en-us/azure/devops/organizations/security/security-best-practices?view=azure-devops>



Use Azure AD as Idp for Github Enterprise Cloud

- Centrally managed Authentication (SAML, SP-Initiated)
- SCIM provisioning (assigning users and groups)





Enable SAML single sign-on



ElvenOrg

Organization account [Switch to another account](#)

General

Features

Access

Billing and plans

Repository roles

Member privileges

Team discussions

Import/Export

Moderation

Code, planning, and automation

Repository

Codespaces

Actions

Webhooks

Discussions

Packages

Pages

Two-factor authentication

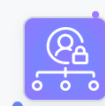
Requiring an additional authentication method adds another layer of security to your organization's GitHub account.

☐ Require two-factor authentication for everyone in the organization

Members, billing managers, and outside collaborators with personal accounts will be removed from the organization if they do not enable two-factor authentication. [Learn more.](#)

Save

SAML single sign-on



Tasks / Enable SAML single sign-on

Enable SAML single sign-on

If you centrally manage your users' identities with an identity provider (IdP), you can enable SAML single sign-on to protect your organization's GitHub account.

When you select "Enable SAML authentication" in the GitHub Enterprise Cloud - Organization settings, you will be prompted to create a new SAML configuration. (IdP).

[Read a step-by-step guide](#)

GitHub Enterprise Cloud - Organization

[Got feedback?](#)

Logo



Name *

GitHub Enterprise Cloud - Organization

Publisher

GitHub, Inc

Provisioning

Automatic provisioning supported

Single Sign-On Mode

SAML-based Sign-on

Linked Sign-on

URL

<https://github.com/business>

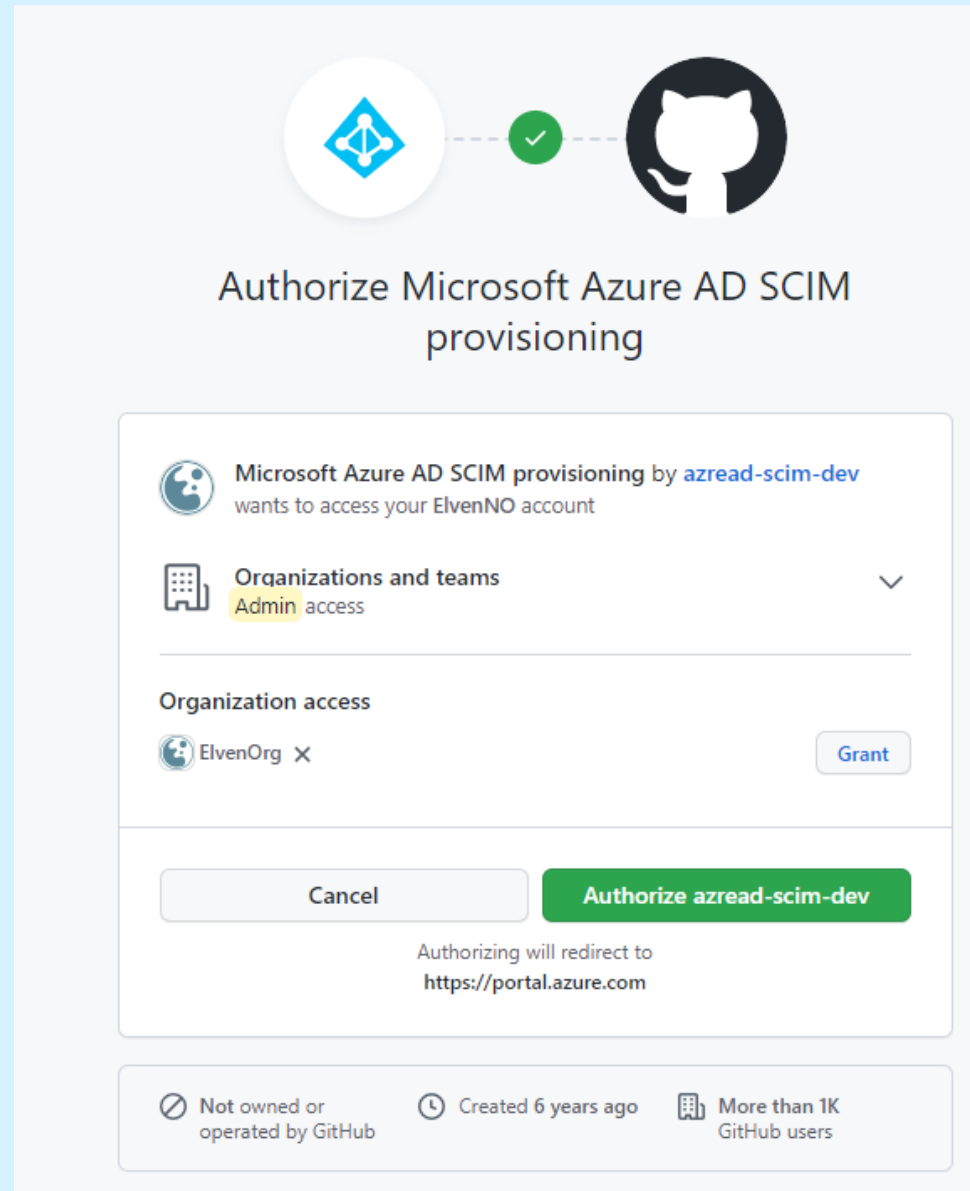
[Read our step-by-step GitHub Enterprise Cloud - Organization integration tutorial](#)

Use Azure AD to manage user access and enable single sign-on with GitHub. Requires an existing Github account.

Create

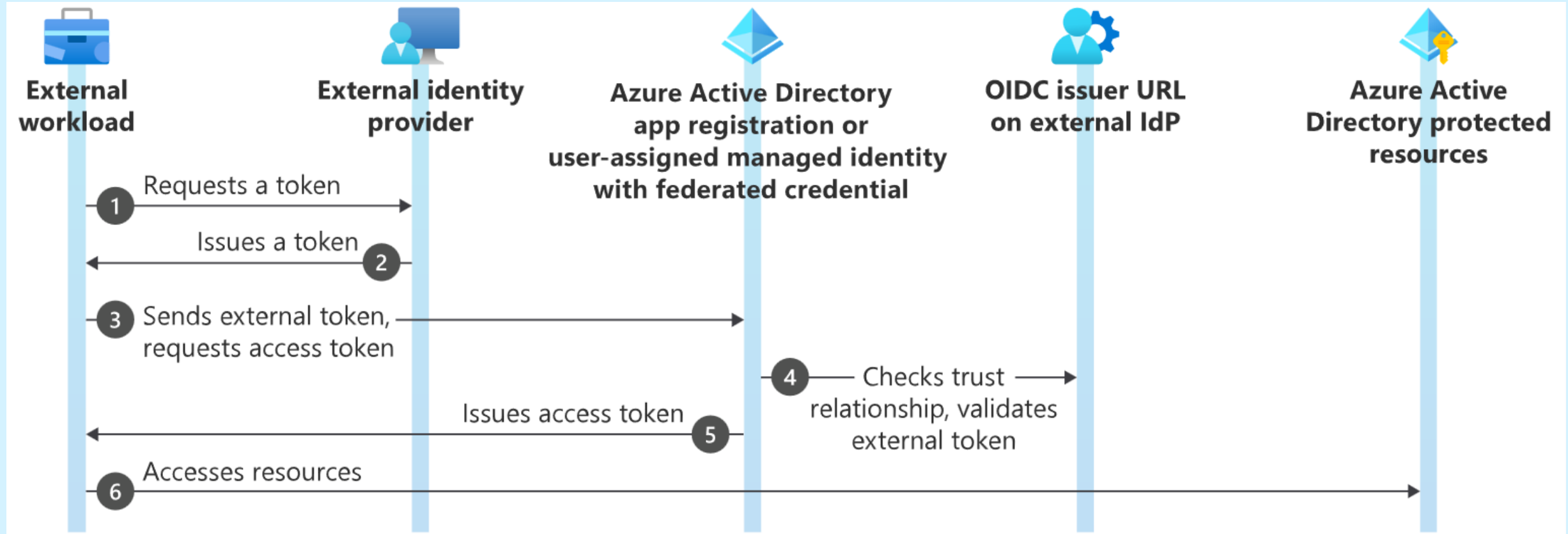


Configure GitHub for automatic user provisioning



<https://learn.microsoft.com/nb-no/azure/active-directory/saas-apps/github-provisioning-tutorial>

Workload Identity Federation GitHub -> Azure AD



<https://techcommunity.microsoft.com/t5/azure-developer-community-blog/build-secure-apps-on-hardened-dev-environments-with-secure/ba-p/2893917>



Defender for DevOps

Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | DevOps Security (Preview) ...

Showing 2 subscriptions | PREVIEW

Search

 < < Add environment Refresh DevOps workbook Guides and Feedback > Getting Started > Configure

- General
- Overview

Getting started

Recommendations

Security alerts

Inventory

Cloud Security Explorer (Preview)

Workbooks

Community

Diagnose and solve problems
- Cloud Security
- Security posture

Regulatory compliance

Workload protections

Firewall Manager

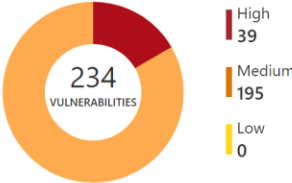
DevOps Security (Preview)
- Management
- Environment settings

Security solutions

Workflow automation

Security Overview

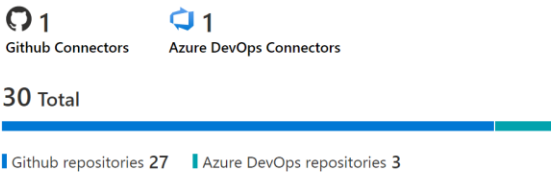
DevOps security vulnerabilities



DevOps security results



DevOps coverage



Search

Subscription... == Contoso Hotels Tenant - Production, CyberSec...

Resource Types == Github Repository, Azure DevOps Repository

<input type="checkbox"/> Name ↑↓	Pull request status	Total exposed secrets ↑↓	OSS vulnerabilities ↑↓	Total code scanning vulnerabilities ↑↓
<input type="checkbox"/> ASE_SG_Demo	N/A	● Unhealthy (1)	1	65
<input type="checkbox"/> RS_ramontest	N/A	● Unhealthy (1)	0	65
<input type="checkbox"/> DfDDemo	N/A	● Unhealthy (4)	17	16
<input type="checkbox"/> Toy-Website	N/A	● Unhealthy (2)	0	0
<input type="checkbox"/> Contoso Hotels	✔ On	● Unhealthy (1)	N/A	0
<input type="checkbox"/> RepositoriesSampleContent	N/A	● Healthy	0	0
<input type="checkbox"/> Toy-Website	✔ On	● Healthy	N/A	0
<input type="checkbox"/> DfD Demo	✔ On	● Healthy	N/A	0

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference#devops-recommendations>

Tip! Defender for Cloud Labs

 Welcome to Microsoft Defender for Cloud Labs!



Introduction

Our labs project help you get ramped up with Microsoft Defender for Cloud and provide hands-on practical experience for product features, capabilities, and scenarios. The labs are divided into 3 main tracks, a beginner (level 100/200) and an advanced (level 300+) track. The labs contain several modules cover different pillars such as Cloud Security Posture Management (CSPM) to Cloud Workload Protection (CWP). To start using our labs, you will need to create Azure Trial Subscription which provides you all capabilities for 30 days – so you have to finish this lab at this point to take advantage of the free trial. We continually update the content to include the latest capabilities – please feel free to [submit issue](#) for any changes and suggestions.


Beginner
(Level 100)


Intermediate
(Level 200)


Advanced
(Level 300+)

<https://github.com/Azure/Microsoft-Defender-for-Cloud/tree/main/Labs>





QA

Takk for meg!

