# NIC Cloud Connect

Oslo Spektrum
November 7 - 9

nic Cloud Connect

# Craig Forshaw

## Getting started with Defender for DevOps

nic Cloud Connect

# Craig Forshaw

- Azure Solutions Architect & Cybersecurity Architect Expert @ Crayon http://www.linkedin.com/in/craig4shaw
- Organiser – Microsoft Security User Group

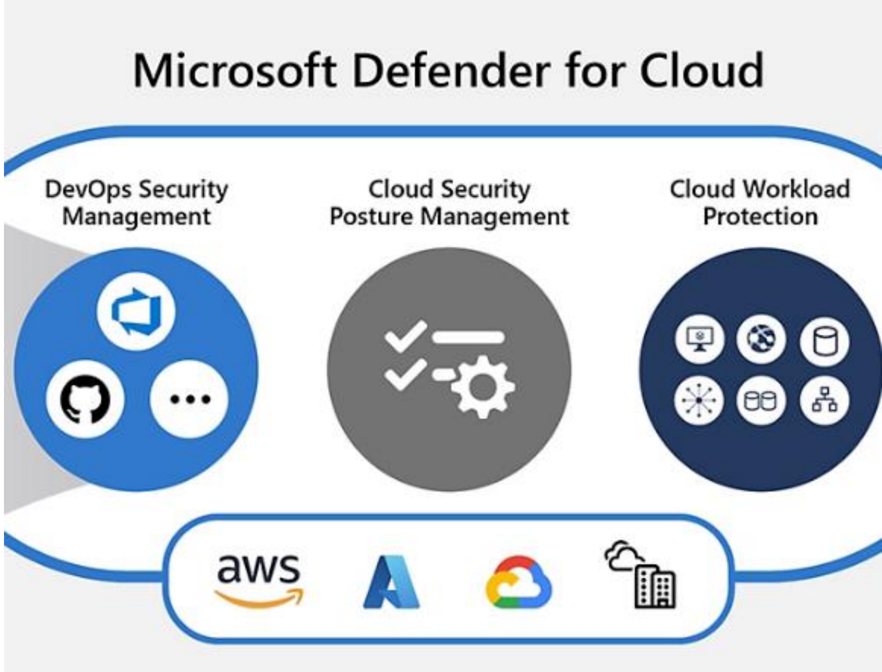
- Traditional infra guy who made the jump to IaC coding in 2019
- Hobbies; Football, Cycling, Skiing
- Terrible at gaming!

# Agenda

- Defender for DevOps
- Demo 1 – Connecting to Defender for DevOps
- Demo 2 – Configure the Microsoft Security DevOps GitHub action
- Demo 3 – Remediate security fixes in a pull request
- Best practices

# Defender for DevOps

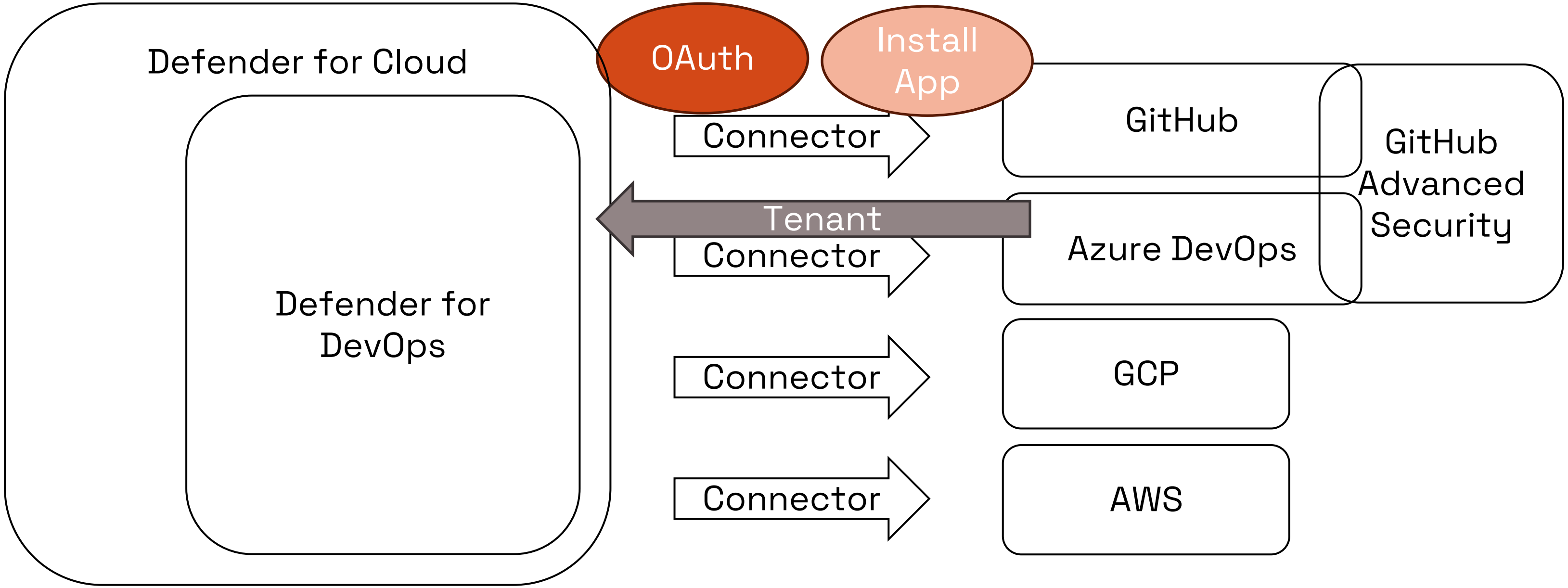
- Service available in Defender for Cloud for security teams to manage DevOps security across multiple environments
- Unified visibility into DevOps security posture
- Findings from code, secret and vulnerability scanning can be prioritised for remediation via pull request annotations
- Public preview since October 2022.


Microsoft Defender for Cloud
DevOps Security Management
Cloud Security Posture Management
Cloud Workload Protection
aws

# Why do we need it?

- Secret exposure
- Vulnerabilities in code
- Inexperienced developers
- Sprint deadlines / pressure to deliver
- SOC visibility

# Architecture



# User Permissions

- **Contributor** for the Azure subscription you have associated in Defender for cloud
- **Security Admin** in the subscription for  Defender for Cloud

- GitHub org admin
- Azure DevOps

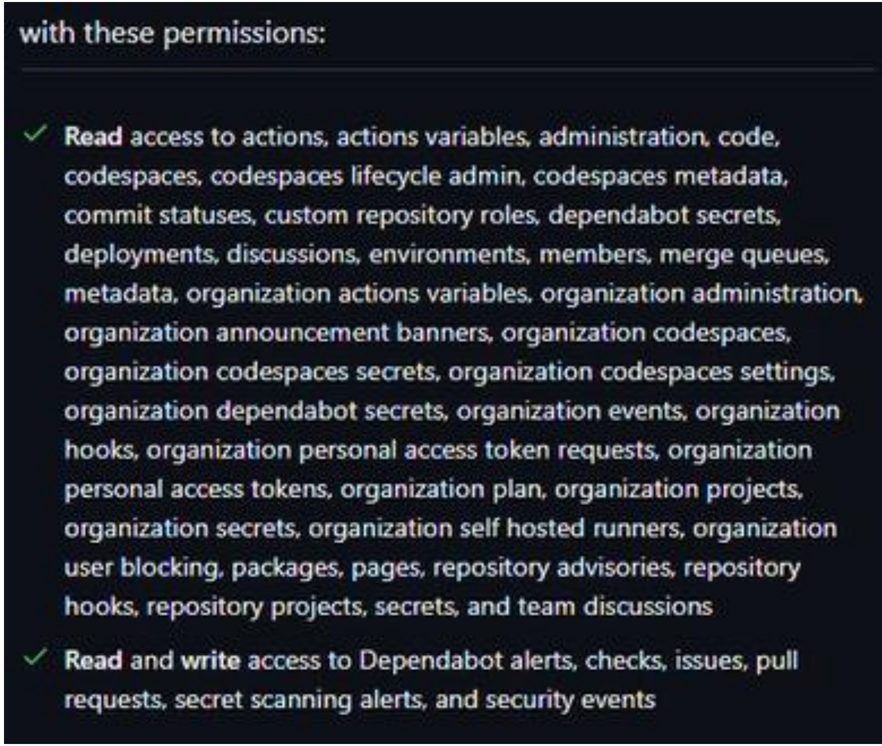
  Org admin

  Basic or Basic + Test plan level

  OAuth > on

# Connector Permissions

- Read access to… pretty much everything
- Read and write access for alerting, events and pull requests



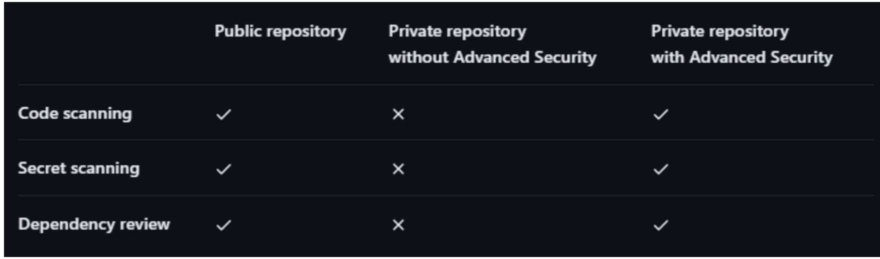
with these permissions:

✓ **Read** access to actions, actions variables, administration, code, codespaces, codespaces lifecycle admin, codespaces metadata, commit statuses, custom repository roles, dependabot secrets, deployments, discussions, environments, members, merge queues, metadata, organization actions variables, organization administration, organization announcement banners, organization codespaces, organization codespaces secrets, organization codespaces settings, organization dependabot secrets, organization events, organization hooks, organization personal access token requests, organization personal access tokens, organization plan, organization projects, organization secrets, organization self hosted runners, organization user blocking, packages, pages, repository advisories, repository hooks, repository projects, secrets, and team discussions

✓ **Read** and **write** access to Dependabot alerts, checks, issues, pull requests, secret scanning alerts, and security events

# GitHub Advanced Security

- Required for Defender for DevOps reporting in Azure
- Code scanning with codeQL – app code languages
- Secret scanning – secrets from partner program
- Dependency review
- Available in GitHub Free, Pro, Team, GitHub Enterprise Cloud and Azure DevOps



| | Public repository | Private repository without Advanced Security | Private repository with Advanced Security |
|---|---|---|---|
| Code scanning | ✓ | × | ✓ |
| Secret scanning | ✓ | × | ✓ |
| Dependency review | ✓ | × | ✓ |

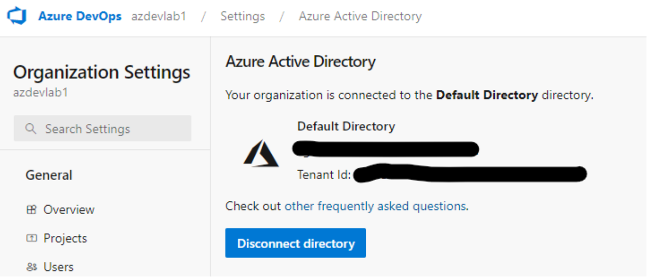
nic Cloud Connect

# Demo 1

- Connect GitHub repositories to Defender for DevOps

nic Cloud Connect

# Azure DevOps Connector



Azure DevOps azdevlab1 / Settings / Azure Active Directory

## Organization Settings

azdevlab1

Search Settings

General

- Overview
- Projects
- Users

## Azure Active Directory

Your organization is connected to the **Default Directory** directory.

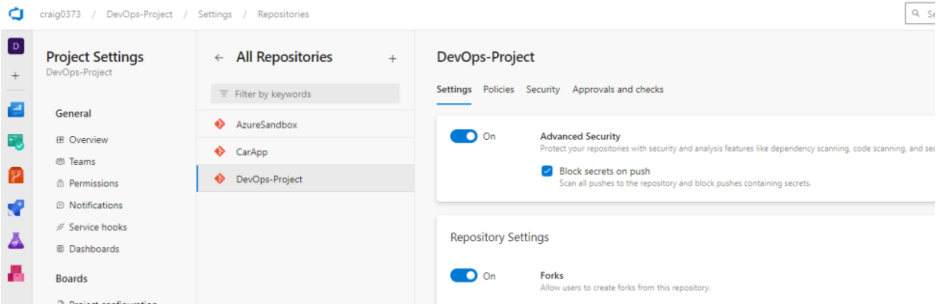
Default Directory

[redacted]

Tenant Id: [redacted]

Check out other frequently asked questions.

Disconnect directory



craig0373 / DevOps-Project / Settings / Repositories

## Project Settings

DevOps-Project

General

- Overview
- Teams
- Permissions
- Notifications
- Service hooks
- Dashboards

Boards

## All Repositories

Filter by keywords

- AzureSandbox
- CarApp
- DevOps-Project

## DevOps-Project

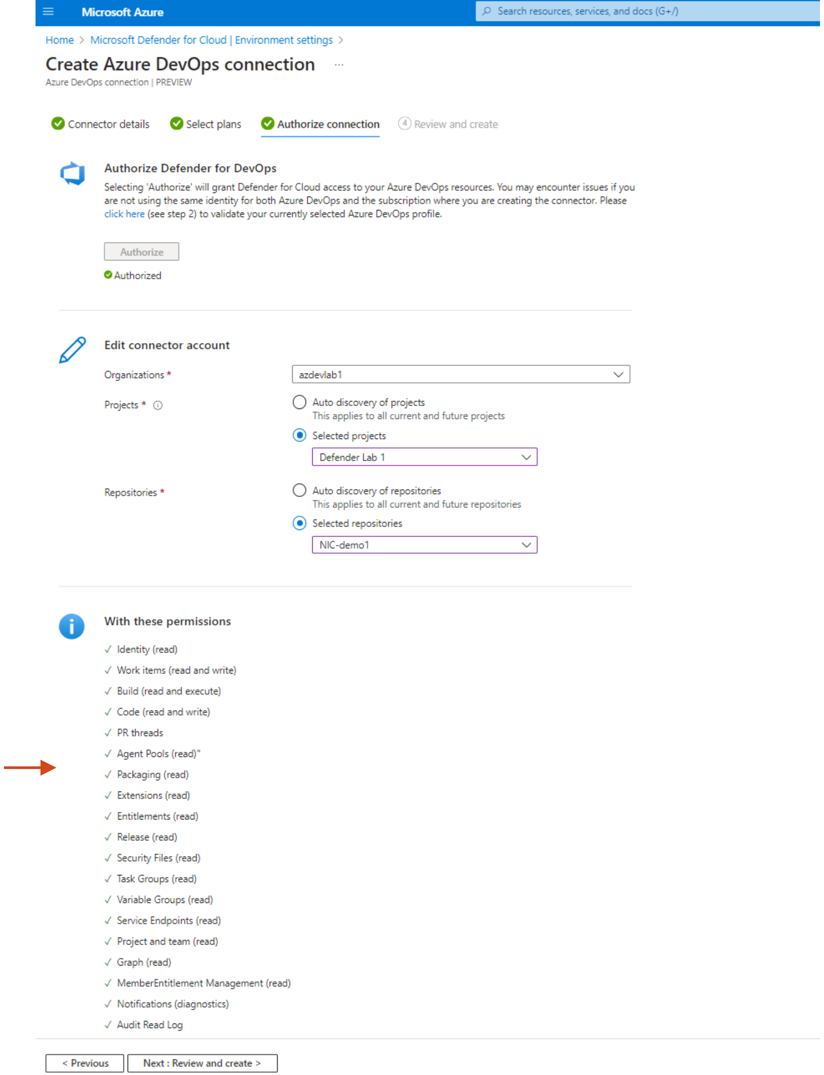
Settings | Policies | Security | Approvals and checks

On — **Advanced Security**
Protect your repositories with security and analysis features like dependency scanning, code scanning, and se

☑ Block secrets on push
Scan all pushes to the repository and block pushes containing secrets.

Repository Settings

On — **Forks**
Allow users to create forks from this repository.



Microsoft Azure | Search resources, services, and docs (G+/)

Home > Microsoft Defender for Cloud | Environment settings >

## Create Azure DevOps connection

Azure DevOps connection | PREVIEW

✓ Connector details | ✓ Select plans | ✓ Authorize connection | (4) Review and create

### Authorize Defender for DevOps

Selecting 'Authorize' will grant Defender for Cloud access to your Azure DevOps resources. You may encounter issues if you are not using the same identity for both Azure DevOps and the subscription where you are creating the connector. Please click here (see step 2) to validate your currently selected Azure DevOps profile.

Authorize

✓ Authorized

### Edit connector account

Organizations *: azdevlab1

Projects *:
○ Auto discovery of projects
This applies to all current and future projects
● Selected projects
Defender Lab 1

Repositories *:
○ Auto discovery of repositories
This applies to all current and future repositories
● Selected repositories
NIC-demo1

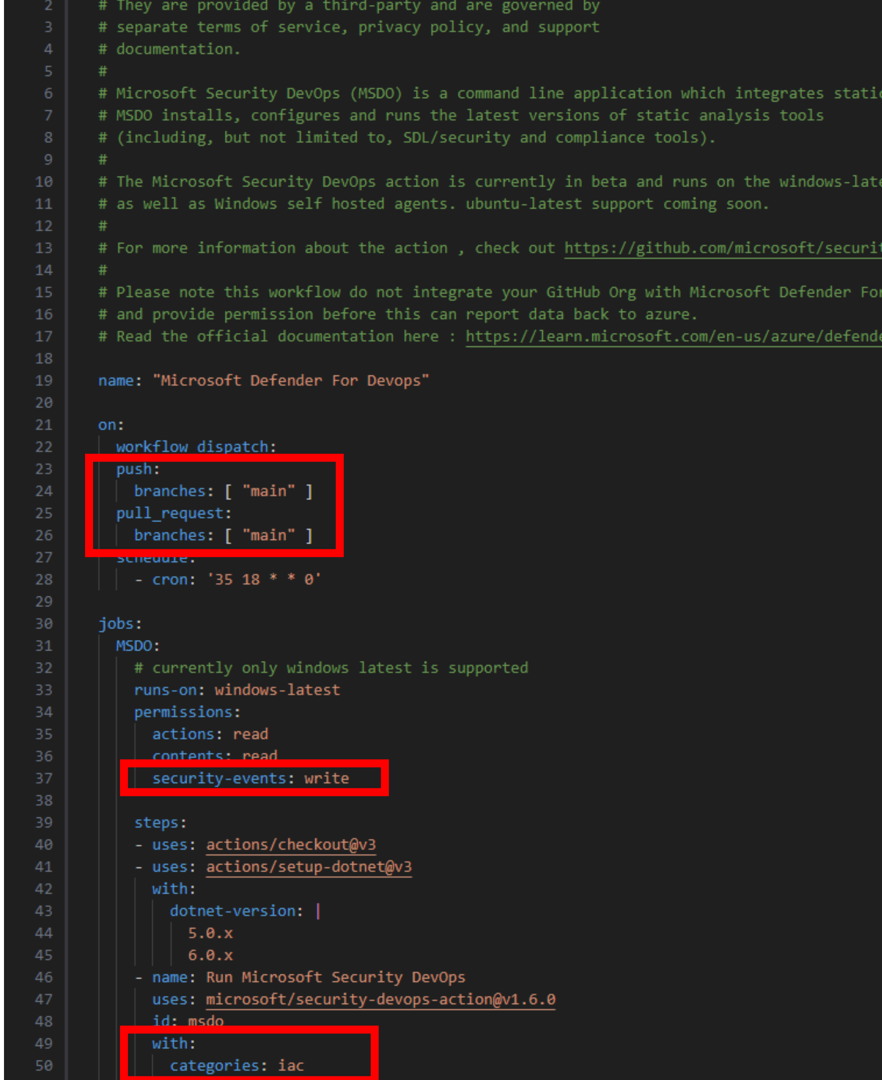
### With these permissions

- ✓ Identity (read)
- ✓ Work items (read and write)
- ✓ Build (read and execute)
- ✓ Code (read and write)
- ✓ PR threads
- ✓ Agent Pools (read)"
- ✓ Packaging (read)
- ✓ Extensions (read)
- ✓ Entitlements (read)
- ✓ Release (read)
- ✓ Security Files (read)
- ✓ Task Groups (read)
- ✓ Variable Groups (read)
- ✓ Service Endpoints (read)
- ✓ Project and team (read)
- ✓ Graph (read)
- ✓ MemberEntitlement Management (read)
- ✓ Notifications (diagnostics)
- ✓ Audit Read Log

< Previous | Next : Review and create >

# Defender for DevOps GitHub Action

- GitHub action template that scans a repository for known vulnerabilities and exposed secrets
- Uses open-source tool scanning
- Can be included as part of pull request process to identify vulnerabilities before merge



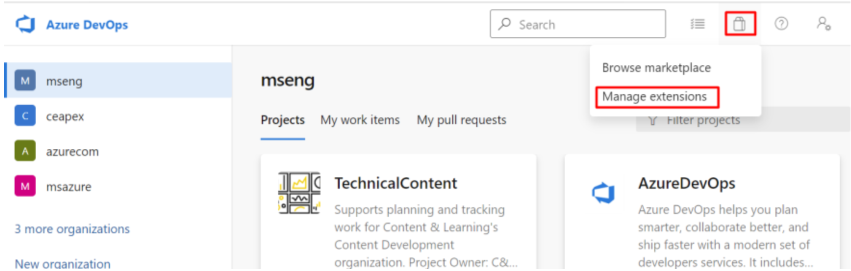
```yaml
# They are provided by a third-party and are governed by
# separate terms of service, privacy policy, and support
# documentation.
#
# Microsoft Security DevOps (MSDO) is a command line application which integrates stati
# MSDO installs, configures and runs the latest versions of static analysis tools
# (including, but not limited to, SDL/security and compliance tools).
#
# The Microsoft Security DevOps action is currently in beta and runs on the windows-late
# as well as Windows self hosted agents. ubuntu-latest support coming soon.
#
# For more information about the action , check out https://github.com/microsoft/securi
#
# Please note this workflow do not integrate your GitHub Org with Microsoft Defender Fo
# and provide permission before this can report data back to azure.
# Read the official documentation here : https://learn.microsoft.com/en-us/azure/defende

name: "Microsoft Defender For Devops"

on:
  workflow_dispatch:
  push:
    branches: [ "main" ]
  pull_request:
    branches: [ "main" ]
  schedule:
    - cron: '35 18 * * 0'

jobs:
  MSDO:
    # currently only windows latest is supported
    runs-on: windows-latest
    permissions:
      actions: read
      contents: read
      security-events: write

    steps:
    - uses: actions/checkout@v3
    - uses: actions/setup-dotnet@v3
      with:
        dotnet-version: |
          5.0.x
          6.0.x
    - name: Run Microsoft Security DevOps
      uses: microsoft/security-devops-action@v1.6.0
      id: msdo
      with:
        categories: iac
```

| Name | Language | License |
|---|---|---|
| AntiMalware | AntiMalware protection in Windows from Microsoft Defender for Endpoint, that scans for malware and breaks the build if malware has been found. This tool scans by default on windows-latest agent. | Not Open Source |
| Bandit | Python | Apache License 2.0 |
| BinSkim | Binary--Windows, ELF | MIT License |
| ESlint | JavaScript | MIT License |
| Template Analyzer | ARM template, Bicep file | MIT License |
| Terrascan | Terraform (HCL2), Kubernetes (JSON/YAML), Helm v3, Kustomize, Dockerfiles, Cloud Formation | Apache License 2.0 |
| Trivy | container images, file systems, git repositories | Apache License 2.0 |

# Demo 2

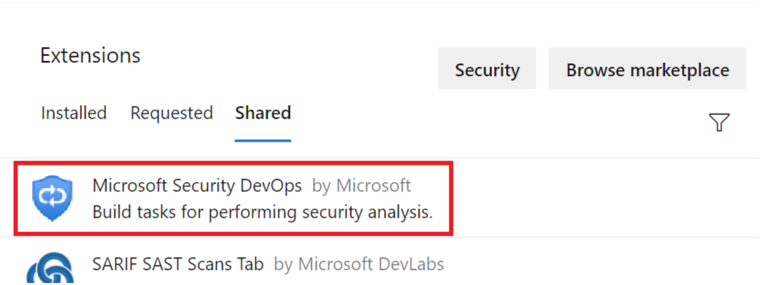
- Configure the Microsoft Security DevOps GitHub action
- Run action on existing code repository
- Analyse code scanning results

# Microsoft Security Azure DevOps extension



Supports planning and tracking work for Content & Learning's Content Development organization. Project Owner: C&...

Azure DevOps helps you plan smarter, collaborate better, and ship faster with a modern set of developers services. It includes...



Microsoft Security DevOps by Microsoft
Build tasks for performing security analysis.

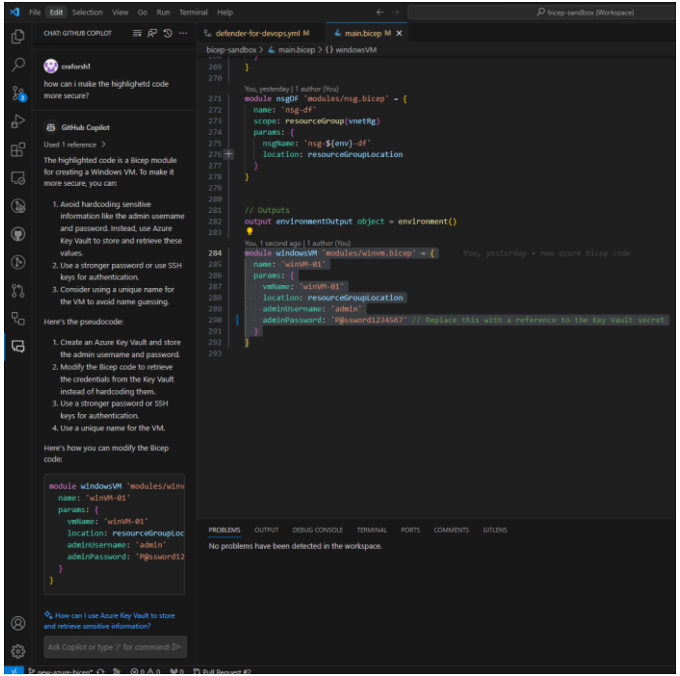
SARIF SAST Scans Tab by Microsoft DevLabs

[Enable pull request annotations in GitHub or in Azure DevOps - Microsoft Defender for Cloud | Microsoft Learn]

Secret scanning required as a step in the build process

# Remediate with GitHub Copilot

- AI code completion tool by GitHub and OpenAI to assist developers with coding by recommending next steps
- Can also be used to help find security vulnerabilities with **GitHub Copilot Chat Beta** by asking questions about how secure your code is and getting recommendations for fixes



craforsh1

how can i make the highlighetd code more secure?

GitHub Copilot

Used 1 reference >

The highlighted code is a Bicep module for creating a Windows VM. To make it more secure, you can:

1. Avoid hardcoding sensitive information like the admin username and password. Instead, use Azure Key Vault to store and retrieve these values.
2. Use a stronger password or use SSH keys for authentication.
3. Consider using a unique name for the VM to avoid name guessing.

Here's the pseudocode:

1. Create an Azure Key Vault and store the admin username and password.
2. Modify the Bicep code to retrieve the credentials from the Key Vault instead of hardcoding them.
3. Use a stronger password or SSH keys for authentication.
4. Use a unique name for the VM.

Here's how you can modify the Bicep code:

```
module windowsVM 'modules/winv
  name: 'winVM-01'
  params: {
    vmName: 'winVM-01'
    location: resourceGroupLoc
    adminUsername: 'admin'
    adminPassword: 'P@ssword12
  }
}
```

How can I use Azure Key Vault to store and retrieve sensitive information?

```
}

You, yesterday | 1 author (You)
module nsgDF 'modules/nsg.bicep' = {
  name: 'nsg-df'
  scope: resourceGroup(vnetRg)
  params: {
    nsgName: 'nsg-${env}-df'
    location: resourceGroupLocation
  }
}


// Outputs
output environmentOutput object = environment()

You, 1 second ago | 1 author (You)
module windowsVM 'modules/winvm.bicep' = {      You, yesterday • new azure bicep code
  name: 'winVM-01'
  params: {
    vmName: 'winVM-01'
    location: resourceGroupLocation
    adminUsername: 'admin'
    adminPassword: 'P@ssword1234567' // Replace this with a reference to the Key Vault secret
  }
}
```

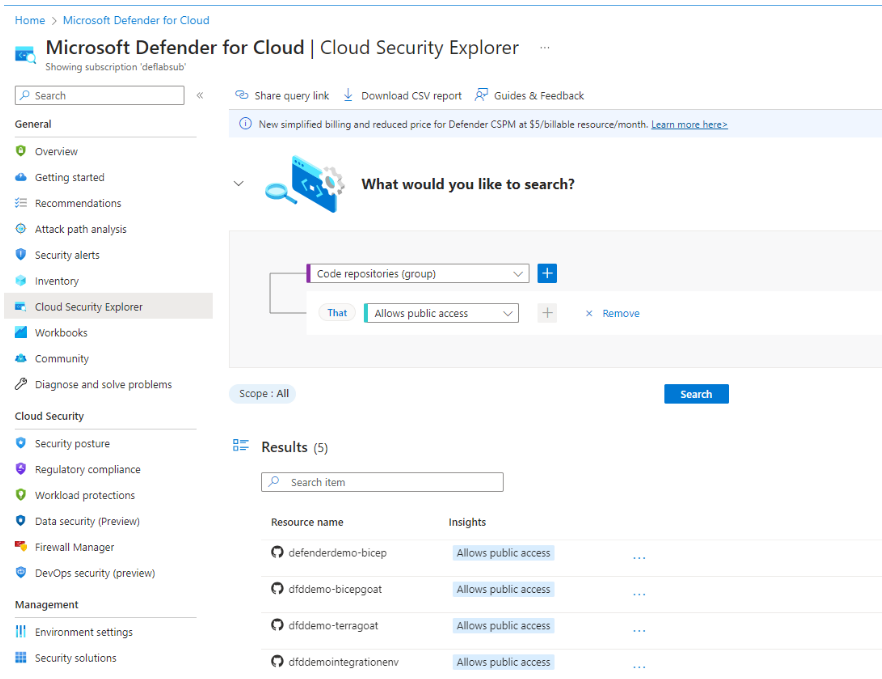
No problems have been detected in the workspace.

# Demo 3

- Run action on new code branch repository as part of a pull request
- Remediate security vulnerabilities

# Defender for Cloud Reporting

- Secure score recommendations – Defender for DevOps is not GA so doesnt affect the score
- Cloud Security Explorer – filter based on vulnerabilities, severity etc



New simplified billing and reduced price for Defender CSPM at $5/billable resource/month. Learn more here>

Code repositories (group)

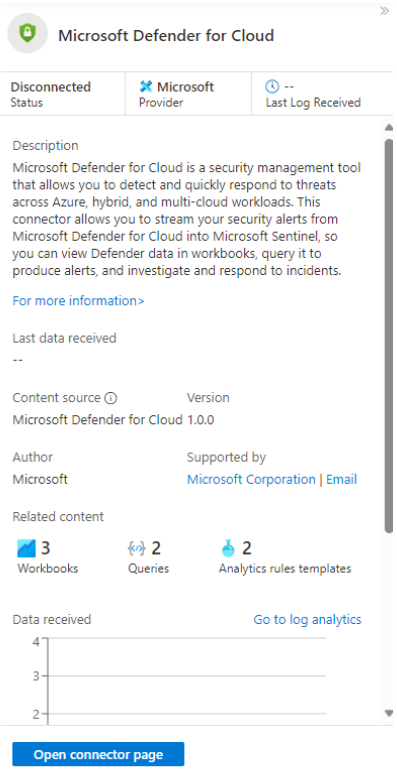
That Allows public access

Scope : All

| Resource name | Insights |
|---|---|
| defenderdemo-bicep | Allows public access |
| dfddemo-bicepgoat | Allows public access |
| dfddemo-terragoat | Allows public access |
| dfddemointegrationenv | Allows public access |

# Sentinel Connectors

- Microsoft Defender for Cloud – stream security alerts to sentinel
- Continuous threat monitoring for GitHub



**Microsoft Defender for Cloud**

| Disconnected | Microsoft | -- |
|---|---|---|
| Status | Provider | Last Log Received |

Description

Microsoft Defender for Cloud is a security management tool that allows you to detect and quickly respond to threats across Azure, hybrid, and multi-cloud workloads. This connector allows you to stream your security alerts from Microsoft Defender for Cloud into Microsoft Sentinel, so you can view Defender data in workbooks, query it to produce alerts, and investigate and respond to incidents.

For more information>

Last data received

--

| Content source ⓘ | Version |
|---|---|
| Microsoft Defender for Cloud | 1.0.0 |

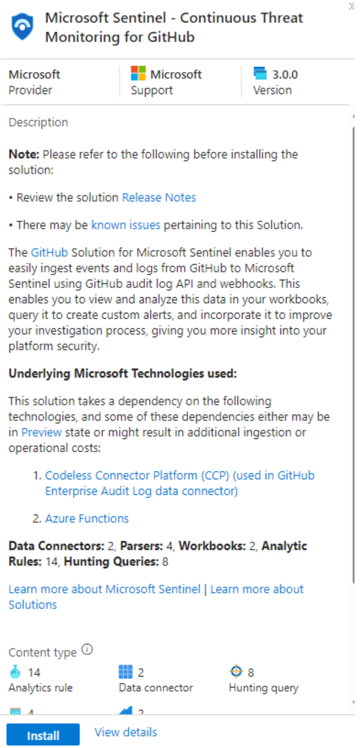
| Author | Supported by |
|---|---|
| Microsoft | Microsoft Corporation \| Email |

Related content

| 3 | 2 | 2 |
|---|---|---|
| Workbooks | Queries | Analytics rules templates |

Data received

Go to log analytics



**Microsoft Sentinel - Continuous Threat Monitoring for GitHub**

| Microsoft | Microsoft | 3.0.0 |
|---|---|---|
| Provider | Support | Version |

Description

**Note:** Please refer to the following before installing the solution:

• Review the solution Release Notes

• There may be known issues pertaining to this Solution.

The GitHub Solution for Microsoft Sentinel enables you to easily ingest events and logs from GitHub to Microsoft Sentinel using GitHub audit log API and webhooks. This enables you to view and analyze this data in your workbooks, query it to create custom alerts, and incorporate it to improve your investigation process, giving you more insight into your platform security.

**Underlying Microsoft Technologies used:**

This solution takes a dependency on the following technologies, and some of these dependencies either may be in Preview state or might result in additional ingestion or operational costs:

1. Codeless Connector Platform (CCP) (used in GitHub Enterprise Audit Log data connector)
2. Azure Functions

**Data Connectors:** 2, **Parsers:** 4, **Workbooks:** 2, **Analytic Rules:** 14, **Hunting Queries:** 8

Learn more about Microsoft Sentinel | Learn more about Solutions

Content type ⓘ

| 14 | 2 | 8 |
|---|---|---|
| Analytics rule | Data connector | Hunting query |
| 4 | 2 | |

# Defender for DevOps considerations

- **Polling period** between Azure and code repoistories is not real time. Sync time can be affected as more repos are onboarded due to API limits.
- **CodeQL** in GitHub advanced security supports C, C++, C#, Go, Java, JavaScript, Typescript, and Python.

    Code scanning occurs only in runtime for IaC, kubernetes.
- **Defender for cloud inventory** logs everything included deleted resources
- **Public preview** - contains some bugs (connector issues, syncing of data, resource tagging issues)

# Best practices in IaC - Secrets

- Avoid secrets where possible
- Create secure parameters for sensitive values

  @secure( ) param <value> string

  @secure( ) param <value> object
- Use dynamic secret lookup between resources
- Store secrets in a password vault

# Best practices in IaC - Vulnerabilities

- Use current versions of resource providers
- Use validation tools as part of the pipeline process
    - Bicep – linter, what-if
    - Terraform – validate, format, plan, tflint, Checkov
- Create a vulnerable sandbox with example code for learning and testing
    - Test vulnerable by design repos such as bicepgoat & terragoat

# Summary

- Microsoft is improving its security portfolio geared toward code-based vulnerability scanning and monitoring
- Best practices are **always** the best way to secure code – avoid secrets and vulnerabilities in code

- The future is tighter integration between all areas to improve code security

  Copilot 'X' products

  GitHub advanced security

  Defender for DevOps

  Sentinel

# Useful resources

- Shift-left and secure your code using Microsoft Defender for DevOps– Microsoft Security Community – YouTube
- Check out the getting started videos in DevOps security on Azure

Dont forget to scan the QR code and review my session!

- Vulnerable code repos:

  https://github.com/bridgecrewio/terragoat.git

  https://github.com/bridgecrewio/bicepgoat.git