Microsoft Defender for DevOps

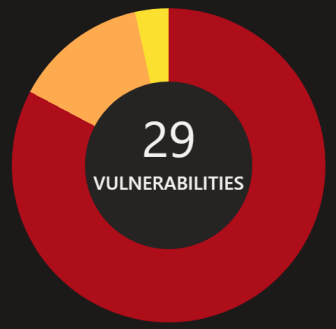
Houssem Dellai
CSA at Microsoft

Microsoft Defender for Cloud | DevOps security (preview)

Showing subscription 'Microsoft-Azure-0' | PREVIEW

Add environment | Refresh | DevOps workbook | Guides and Feedback | Getting Started | Configure

DevOps code scanning findings



High 24

Medium 4

Low 1

DevOps security results

8 Code scanning vulnerabilities

21 IaC scanning vulnerabilities

0 OSS vulnerabilities

0 Exposed Secrets

DevOps coverage

1 GitHub Connectors

1 Azure DevOps Connectors

400 Total

Github repositories 204

Azure DevOps repositories 196

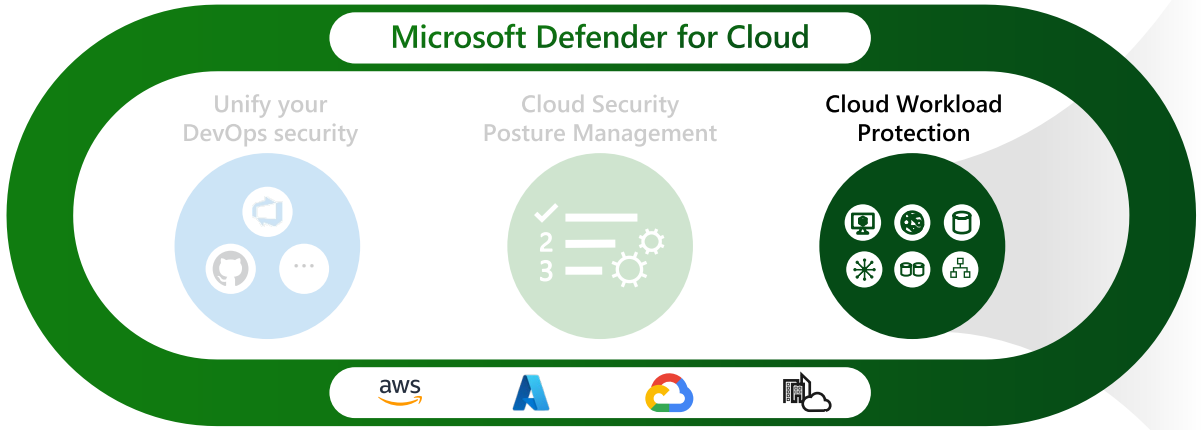
Search

Subscriptions == **All**

Resource Types == **Github Repository, Azure DevOps Repository**

Name	Pull request status	Total exposed secrets	OSS vulnerabilities	IaC scanning vulnera...	Total code scanning ...
WebAppWithDatabaseDemo-AzureRepo	Off	N/A - Unspecified	N/A	11	8
ARM-Template-DevOps-demo	Off	N/A - Unspecified	N/A	10	0
AKS-Demo-Cx	Off	N/A - Unspecified	N/A	0	0
AKS-Deployment	Off	N/A - Unspecified	N/A	0	0
AKS-Landing-Zone-Accelerator	N/A	N/A - Unspecified	0	0	0

Microsoft Defender for Cloud



Compute: Any server, Azure VMSS, Azure K8s, App Services, Unmanaged K8s

Service layer: Azure DNS, Key Vault, Network Layer V1, Resource Management

Databases and storage: Blob storage, File storage, Maria DB, Cosmos DB, Azure SQL, MySQL, Postgres SQL, SQL on VM

AWS workloads: Amazon EKS, Amazon EC2, SQL on VM, Unmanaged Kubernetes

GCP workloads: GKE clusters, Google Compute, SQL on VM, Unmanaged Kubernetes

On-premises workloads: Kubernetes, SQL on VM, Servers

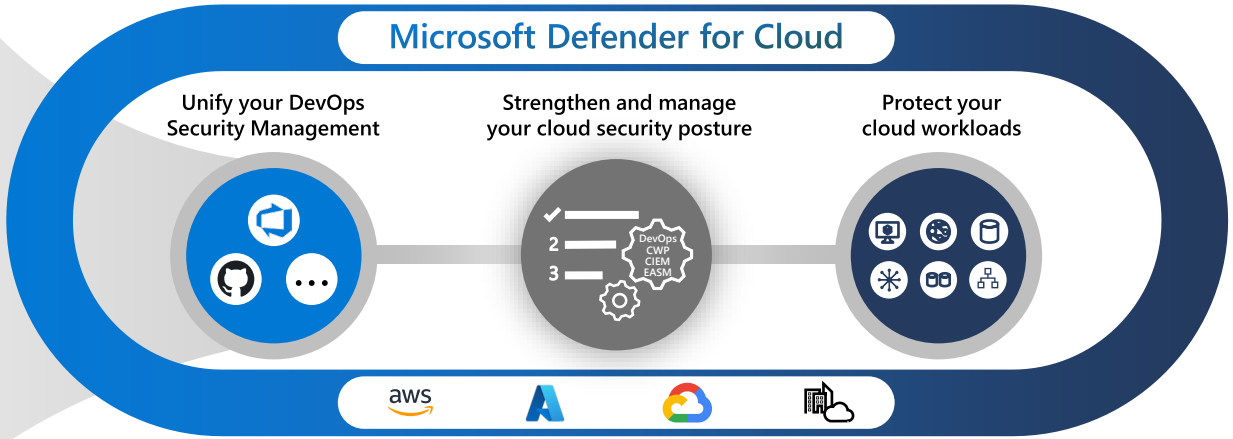
Microsoft Defender for DevOps

DevOps posture visibility
Code | Dependencies | Secrets | Container images | Infrastructure as code security insights

Infrastructure as code security
ARM | Bicep | Terraform | CloudFormation | And more

Code to cloud contextualization
Across multipipeline and multicloud environments

Integrated workflows
Pull request annotations | Developer ownership assignments



Name	Language	License
AntiMalware	code, artifacts	-
Bandit	python	Apache License 2.0
BinSkim	binary - Windows, ELF	MIT License
ESlint	JavaScript	MIT License
Template Analyzer	Infrastructure-as-code (IaC), ARM templates, Bicep files	MIT License
Terrascan	Infrastructure-as-code (IaC), Terraform (HCL2), Kubernetes (JSON/YAML), Helm v3, Kustomize, Dockerfiles, Cloudformation	Apache License 2.0
Trivy	container images, file systems, and git repositories	Apache License 2.0

Microsoft Defender for Cloud | Environment settings

Showing subscription 'Microsoft-Azure-0'

Search

Security alerts
Inventory
Cloud Security Explorer
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

Add environment | Refresh | Guides & Feedback | Cost estimator

- Amazon Web Services
- Google Cloud Platform
- GitHub (preview)
- Azure DevOps (preview)

GitHub (preview)

lti-cloud account management page. To switch back to the classic cloud connectors experience, click here.

Data sensitivity

Set the sensitivity of your organization's resources based on info type or sensitivity labels

Direct onboarding

Onboard non-Azure servers directly with Defender for Endpoint

1 Azure subscriptions

0 AWS accounts

0 GCP projects

1 GitHub connectors

1 AzureDevOps connectors

0 Total issues

GCP Projects 0 AWS Accounts 0

Search by name | Environments == All | Standards == All | Coverage == All | More (1)

Expand all

Name	Total resources	Connectivity status	Defender coverage

Create GitHub connection

GitHub connection | PREVIEW

Connector details | Select plans | 3 Authorize connection | 4 Review and create

Enter a descriptive name for the Defender for DevOps instance, choose a Subscription and Resource Group to store the connection information.

Name *: github

Subscription *: Microsoft-Azure-0

Resource group *: rg-azure-devops

Create new

Region *: West Europe

Defender for DevOps only supports Australia East, Central US and West Europe during preview

Next : Select plans >

Create GitHub connection

GitHub connection | PREVIEW

Connector details | Select plans | 3 Authorize connection | 4 Review and create

Select plans

Security posture management With continuous scans of your DevOps infrastructure and repositories, Defender for Cloud will help discover and prevent misconfigurations. You'll receive hardening recommendations, be able to view your resources in a unified asset inventory, and see your secure score.

Select the desired plan to enable for this connection. Each capability allows additional configuration and requires appropriate permissions to perform actions on the repositories.

Plan name & description	Configurations	Pricing	Plan status
DevOps Protect your DevOps environments and source code with advanced defenses.		Free (preview)	On / Off

< Previous | Next : Authorize connection >

Create GitHub connection

GitHub connection | PREVIEW

Connector details | Select plans | 3 Authorize connection | 4 Review and create

All resources with DevOps app installed will be visible.

Authorize Defender for DevOps

Give permission to the Defender for DevOps app to access your resources.

Authorize

Authorized

Install Defender for DevOps app

Install the Defender for DevOps app on your repositories.

Install

Installed

< Previous | Next : Review and create >

Microsoft Security DevOps

Microsoft | 4,817 installs | ★★★☆☆ (2) | Preview

Build tasks for performing security analysis.

Get it free

Microsoft Security DevOps for Azure DevOps

An extension for Azure DevOps that contributes a build task to run the Microsoft Security DevOps CLI.

- Installs the Microsoft Security DevOps CLI
- Installs the latest Microsoft security policy
- Installs the latest Microsoft and 3rd party security tools
- Automatic or user-provided configuration of security tools
- Execution of a full suite of security tools
- Normalized processing of results into the SARIF format
- Build breaks and more

Basic

Add the `MicrosoftSecurityDevOps` build task to your pipeline's yaml:

```
steps:
- task: MicrosoftSecurityDevOps@1
```

The `publish` input option is defaulted to true. If true, this will publish a SARIF formatted results file as a build artifact to `CodeAnalysisLogs/msdo.sarif`.

Categories

Azure Pipelines

Tags

Analysis AntiMalware Bandit BinSkim Build Break Defender ESLint Flawfinder Gosec Iac Microsoft Defender Microsoft Defender for Cloud Roslyn Analyzers SDL Security Static Analysis Template Analyzer Terrascan Trivy Windows Defender

Works with

Azure DevOps Services

Resources

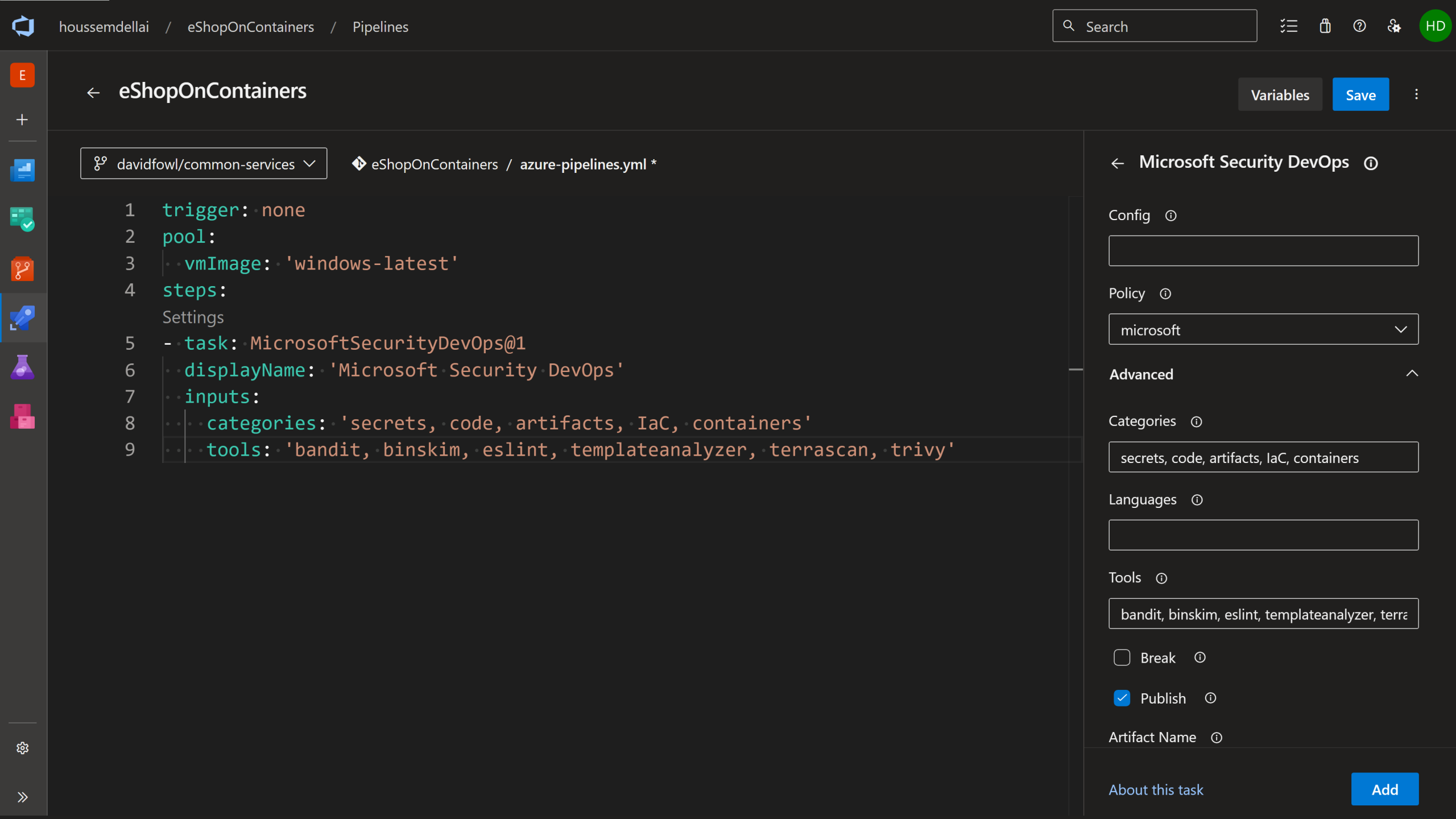
Support
Get Started
License

Project Details

microsoft/security-devops-azdevops

Integration into Azure DevOps pipelines

```
trigger  none
pool
  vmImage  'windows-latest'
steps
  task  MicrosoftSecurityDevOps@1
  displayName  'Microsoft Security DevOps'
  inputs
    categories  'secrets, code, artifacts, IaC, containers'
    tools  'bandit, binskim, eslint, templateanalyzer, terrascan, trivy'
```


houssemdellai / eShopOnContainers / Pipelines
Search
HD
eShopOnContainers
Variables
Save
davidfowl/common-services
eShopOnContainers / azure-pipelines.yml *
1 trigger: none
2 pool:
3 vmImage: 'windows-latest'
4 steps:
Settings
5 - task: MicrosoftSecurityDevOps@1
6 displayName: 'Microsoft Security DevOps'
7 inputs:
8 categories: 'secrets, code, artifacts, IaC, containers'
9 tools: 'bandit, binskim, eslint, templateanalyzer, terrascan, trivy'
Microsoft Security DevOps
Config
Policy
microsoft
Advanced
Categories
secrets, code, artifacts, IaC, containers
Languages
Tools
bandit, binskim, eslint, templateanalyzer, terra
Break
Publish
Artifact Name
About this task
Add

Jobs in run #Microsoft ...

WebAppWithDatabaseDemo-AzureRepo (2)

Jobs

- Job 2m 25s
  - Initialize job <1s
  - Checkout WebAppWit... 13s
  - Microsoft Security ... 2m 10s
  - Post-job: Checkout W... <1s
  - Finalize Job <1s
  - Report build status <1s

Microsoft Security DevOps

View raw log

```
761       Tool: ESLint: Rule: @microsoft/sdl/no-inner-html (Assignments to [innerHTML](https://developer.mozilla.org/en-US/docs/Web/API/Element/innerHTM
762       Do not write to DOM directly using innerHTML/outerHTML property
763   ##[warning]24. ESLint Warning @microsoft/sdl/no-inner-html - File: WebApp/wwwroot/lib/jquery/dist/jquery.js. Line: 10291. Column 2.
764       Tool: ESLint: Rule: @microsoft/sdl/no-inner-html (Assignments to [innerHTML](https://developer.mozilla.org/en-US/docs/Web/API/Element/innerHTM
765       Do not write to DOM directly using innerHTML/outerHTML property
766   ##[warning]25. ESLint Warning @microsoft/sdl/no-html-method - File: WebApp/wwwroot/lib/jquery/dist/jquery.js. Line: 10388. Column 4.
767       Tool: ESLint: Rule: @microsoft/sdl/no-html-method (Direct calls to method `html()` often (e.g. in jQuery framework) manipulate DOM without any
768       Do not write to DOM directly using jQuery html() method
769   ##[warning]26. ESLint Warning @microsoft/sdl/no-inner-html - File: WebApp/wwwroot/lib/jquery/dist/jquery.min.js. Line: 2. Column 84308.
770       Tool: ESLint: Rule: @microsoft/sdl/no-inner-html (Assignments to [innerHTML](https://developer.mozilla.org/en-US/docs/Web/API/Element/innerHTM
771       Do not write to DOM directly using innerHTML/outerHTML property
772   ##[warning]27. ESLint Warning @microsoft/sdl/no-html-method - File: WebApp/wwwroot/lib/jquery/dist/jquery.min.js. Line: 2. Column 85038.
773       Tool: ESLint: Rule: @microsoft/sdl/no-html-method (Direct calls to method `html()` often (e.g. in jQuery framework) manipulate DOM without any
774       Do not write to DOM directly using jQuery html() method
775   ##[warning]28. ESLint Warning @microsoft/sdl/no-html-method - File: WebApp/wwwroot/lib/jquery-validation/dist/jquery.validate.js. Line: 942. Column
776       Tool: ESLint: Rule: @microsoft/sdl/no-html-method (Direct calls to method `html()` often (e.g. in jQuery framework) manipulate DOM without any
777       Do not write to DOM directly using jQuery html() method
778   ##[warning]29. ESLint Warning @microsoft/sdl/no-html-method - File: WebApp/wwwroot/lib/jquery-validation/dist/jquery.validate.js. Line: 946. Column
779       Tool: ESLint: Rule: @microsoft/sdl/no-html-method (Direct calls to method `html()` often (e.g. in jQuery framework) manipulate DOM without any
780       Do not write to DOM directly using jQuery html() method
781   ##[warning]30. ESLint Warning @microsoft/sdl/no-html-method - File: WebApp/wwwroot/lib/jquery-validation/dist/jquery.validate.min.js. Line: 4. Colum
782       Tool: ESLint: Rule: @microsoft/sdl/no-html-method (Direct calls to method `html()` often (e.g. in jQuery framework) manipulate DOM without any
783       Do not write to DOM directly using jQuery html() method
784       Saved file D:\a\1\a\.gdn\msdo.sarif
785       Active results: 28
786       Skipped results: 0
787         Baselined results: 0
788         Suppressed results: 0
789         Results excluded by tool filters: 0
790         Results below minimum severity: 0
791         Results classified as Pass: 0
```

#20230725.1 • Set up CI with Azure Pipelines

ARM-Template-DevOps-demo (1)

Run new

This run is being retained as one of 3 recent runs by main (Branch).

View retention leases

Summary | Aqua Scanner Report | Artifactory | **Scans** | WhiteSource Bolt Build Report

Filter by keyword

Baseline: **New (+2)**

Level: **Error (+1)**

templateanalyzer 9

Path	Details	Actions	Baseline
TA-000015: AppServiceWebApp.OnlyFTPS 1			
azuredeploy.json	Enable FTPS enforcement for enhanced security.	Fix in VS Code	New
TA-000016: AppServiceWebApp.OnlyHTTPS 1			
TA-000017: AppServiceWebApp.UseLatestTLS 1			
TA-000019: AppServiceWebApp.UseManagedIdentity 1			
AZR-000186: Azure.SQL.DefenderCloud 1			

GitHub Action

security-devops-action

v1.7.2 Latest version

Use latest version

microsoft/security-devops-action (Preview)

Microsoft Security DevOps (MSDO) is a command line application which integrates static analysis tools into the development cycle. MSDO installs, configures and runs the latest versions of static analysis tools (including, but not limited to, SDL/security and compliance tools). MSDO is data-driven with portable configurations that enable deterministic execution across multiple environments. For tools that output results in or MSDO can convert their results to SARIF, MSDO imports into a normalized file database for seamlessly reporting and responding to results across tools, such as forcing build breaks.

Run locally. Run remotely.

MSDO Sample Workflow passing

This action runs the Microsoft Security DevOps CLI for security analysis:

- Installs the Microsoft Security DevOps CLI
- Installs the latest Microsoft security policy
- Installs the latest Microsoft and 3rd party security tools
- Automatic or user-provided configuration of security tools
- Execution of a full suite of security tools
- Normalized processing of results into the SARIF format

Verified creator

GitHub has verified that this action was created by **microsoft**.

Learn more about verified Actions.

Stars

Star 71

Contributors

Categories

Security Code Scanning Ready

Links

microsoft/security-devops-action

Open issues 14

Pull requests 0

Report abuse

https://github.com/marketplace/actions/security-devops-action

Integration into Github Actions

```yaml
permissions:
  security-events: write

steps:

- uses: actions/checkout@v3

- name: Run Microsoft Security DevOps
  uses: microsoft/security-devops-action@v1
  id: msdo
```

WebAppWithDatabaseDemo / .github / workflows / Microsoft_Defender_for_C in master

Cancel changes Commit changes...

Edit Preview Spaces 2 No wrap

```yaml
jobs:
  sample:
    name: Microsoft Security DevOps Analysis

    # MSDO runs on windows-latest.
    # ubuntu-latest and macos-latest supporting coming soon
    runs-on: windows-latest

    steps:

      # Checkout your code repository to scan
    - uses: actions/checkout@v3

      # Run analyzers
    - name: Run Microsoft Security DevOps Analysis
      uses: microsoft/security-devops-action@preview
      id: msdo

      # Upload alerts to the Security tab
    - name: Upload alerts to Security tab
      uses: github/codeql-action/upload-sarif@v2
      with:
        sarif_file: ${{ steps.msdo.outputs.sarifFile }}
```

Marketplace Documentation

Marketplace / Search results / security-devops-action

security-devops-action

By microsoft v1.7.2 71

Run security analyzers

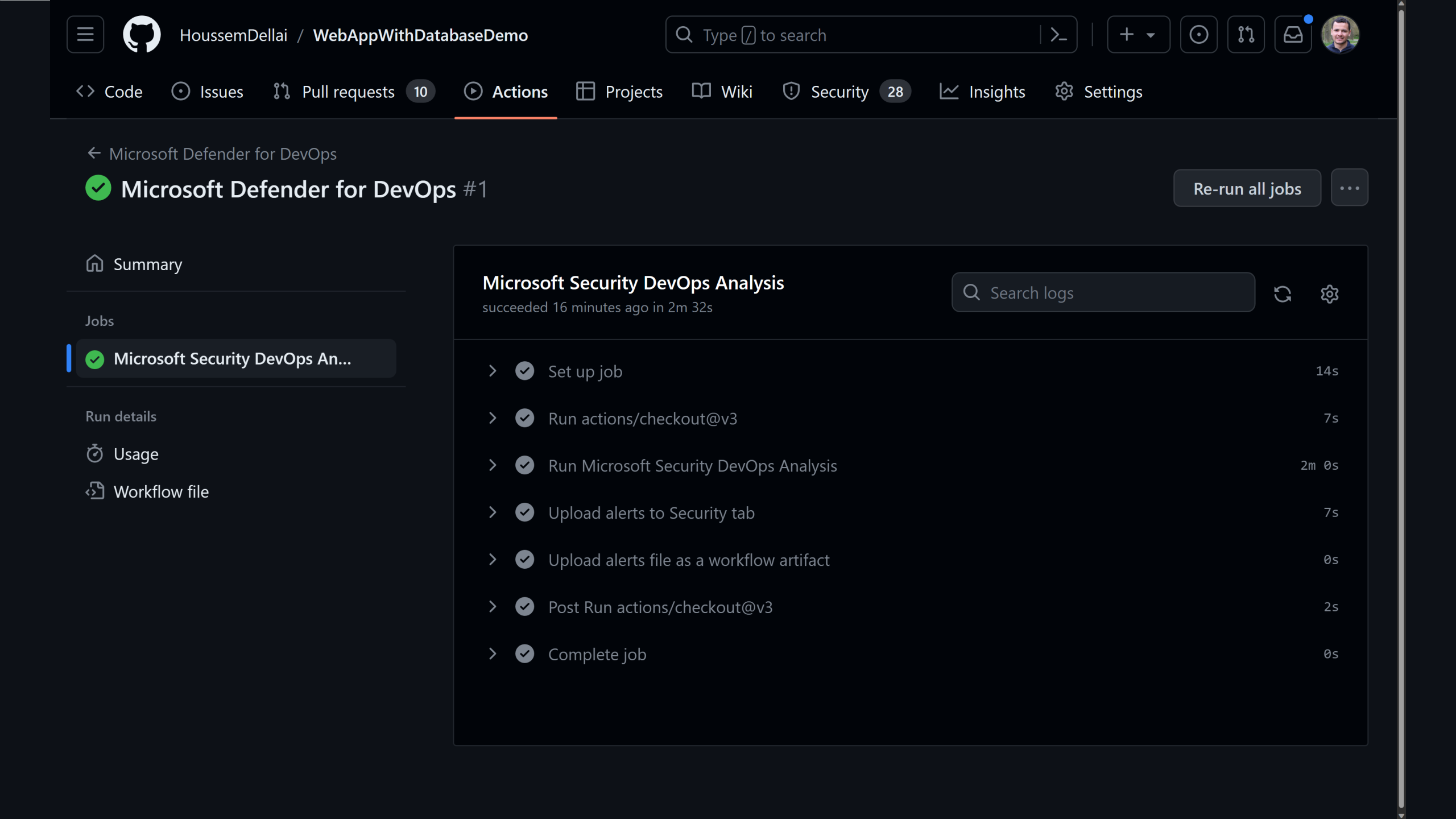
View full Marketplace listing

Installation

Copy and paste the following snippet into your .yml file.

Version: v1.7.2

```yaml
- name: security-devops-action
  uses: microsoft/security-devops-action@v1.7
  with:
    # A file path to a .gdnconfig file.
    config: # optional
    # The name of the well known policy to us
    policy: # optional, default is GitHub
    # A comma separated list of analyzer cate
    categories: # optional
```


HoussemDellai / WebAppWithDatabaseDemo
Type / to search
Code
Issues
Pull requests 10
Actions
Projects
Wiki
Security 28
Insights
Settings
Microsoft Defender for DevOps
Microsoft Defender for DevOps #1
Re-run all jobs
Summary
Jobs
Microsoft Security DevOps An...
Run details
Usage
Workflow file
Microsoft Security DevOps Analysis
succeeded 16 minutes ago in 2m 32s
Search logs
Set up job 14s
Run actions/checkout@v3 7s
Run Microsoft Security DevOps Analysis 2m 0s
Upload alerts to Security tab 7s
Upload alerts file as a workflow artifact 0s
Post Run actions/checkout@v3 2s
Complete job 0s

Overview

Reporting

Policy

Advisories

Vulnerability alerts

Dependabot

Code scanning 28

Secret scanning

Code scanning

ESLint is reporting errors

Tool status 4 + Add tool

is:open branch:master

28 Open ✓ 0 Closed Language Tool Branch Rule Severity Sort

Ensure that Azure Active Directory Admin is configured for SQL Server Error master

#28 opened 14 minutes ago • Detected by **terrascan** in **Terraform\webapp-db.tf**:39

App Service apps uses a managed identity. Error master

#26 opened 14 minutes ago • Detected by **templateanalyzer** in **AzureResourceGroupDeploy.../WebSiteSQLDatabase.json**:152

Azure SQL DB server minimum TLS version. Error master

#25 opened 14 minutes ago • Detected by **templateanalyzer** in **AzureResourceGroupDeploy.../WebSiteSQLDatabase.json**:98

Use AAD authentication with SQL databases. Error master

#24 opened 14 minutes ago • Detected by **templateanalyzer** in **AzureResourceGroupDeploy.../WebSiteSQLDatabase.json**:98

Enable auditing for Azure SQL DB server. Error master

#23 opened 14 minutes ago • Detected by **templateanalyzer** in **AzureResourceGroupDeploy.../WebSiteSQLDatabase.json**:1

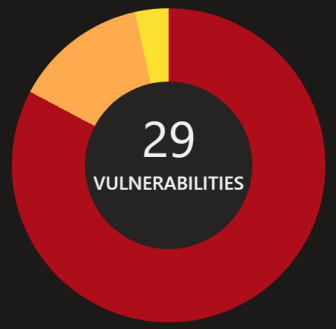
Use Advanced Threat Protection. Error master

Microsoft Defender for Cloud | DevOps security (preview)

Showing subscription 'Microsoft-Azure-0' | PREVIEW

Add environment | Refresh | DevOps workbook | Guides and Feedback | Getting Started | Configure

DevOps code scanning findings



High 24

Medium 4

Low 1

DevOps security results

8 Code scanning vulnerabilities

21 IaC scanning vulnerabilities

0 OSS vulnerabilities

0 Exposed Secrets

DevOps coverage

1 GitHub Connectors

1 Azure DevOps Connectors

400 Total

Github repositories 204

Azure DevOps repositories 196

Search

Subscriptions == **All**

Resource Types == **Github Repository, Azure DevOps Repository**

Name	Pull request status	Total exposed secrets	OSS vulnerabilities	IaC scanning vulnera...	Total code scanning ...
WebAppWithDatabaseDemo-AzureRepo	Off	N/A - Unspecified	N/A	11	8
ARM-Template-DevOps-demo	Off	N/A - Unspecified	N/A	10	0
AKS-Demo-Cx	Off	N/A - Unspecified	N/A	0	0
AKS-Deployment	Off	N/A - Unspecified	N/A	0	0
AKS-Landing-Zone-Accelerator	N/A	N/A - Unspecified	0	0	0

Findings

Code repositories should have infrastructure as code scanning findings resolved

Open query

Severity
Medium

Freshness interval
8 Hours

Tactics and techniques
Initial Access +1

Description

Remediation steps

Affected resources

Unhealthy resources (2) | Healthy resources (0) | Not applicable resources (194)

Search azure resources

Name	Subscription	Owner	Due date	Status	Last change date
webappwithdatabasedemo-	Microsoft-Azure-0				7/23/2023, 9:28:06 PM
arm-template-devops-demc	Microsoft-Azure-0				7/25/2023, 1:32:08 PM

Security checks

Findings

Search to filter items...

ID	Security check	Category	Applies to	Severity
4a188c1c-d2cb-f981-8...	Latest TLS version should be used in your web app.	Infrastructure as Code	1 of 2 resources	High
f445773a-5bea-b61e-e...	FTPS only should be required in your web app.	Infrastructure as Code	1 of 2 resources	High
1f484757-806e-fc50-86...	Ensure entire Azure infrastructure doesn't have access to Azure SQL ServerEn...	Infrastructure as Code	1 of 2 resources	High
66ce4bb5-f66c-e220-0...	App Service apps uses a managed identity.	Infrastructure as Code	1 of 2 resources	High
a0848f38-5ba3-770f-06...	Azure SQL DB server minimum TLS version.	Infrastructure as Code	1 of 2 resources	High
b9136fea-3266-2607-2...	Use AAD authentication with SQL databases.	Infrastructure as Code	1 of 2 resources	High
30c2bbc9-a91e-fa4d-e...	Use Advanced Threat Protection.	Infrastructure as Code	1 of 2 resources	High
f60a1858-eab5-eeeb-1...	Enable auditing for Azure SQL DB server.	Infrastructure as Code	1 of 2 resources	High

Trigger logic app | Assign owner | Change owner and set ETA