

Innovation is the lifefblood of
an organization in the digital
age and needs to be both
enabled and protected!

Pouyan Khabazi

Co-founder @EightFence



Part of Codeinceps Group



pkm-technology.com

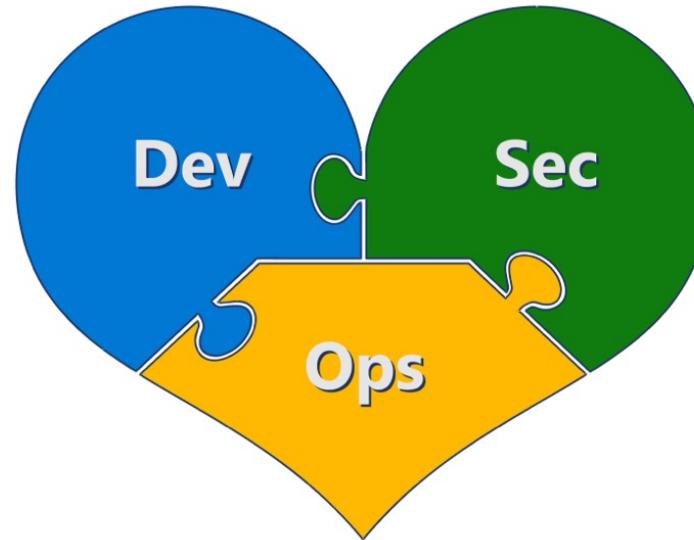


@pkhabazi



@pkhabazi

Responsive to Needs
Meets business and customer requirements for market relevance



Safe and Secure
Provides confidentiality, integrity, & availability + regulatory compliance

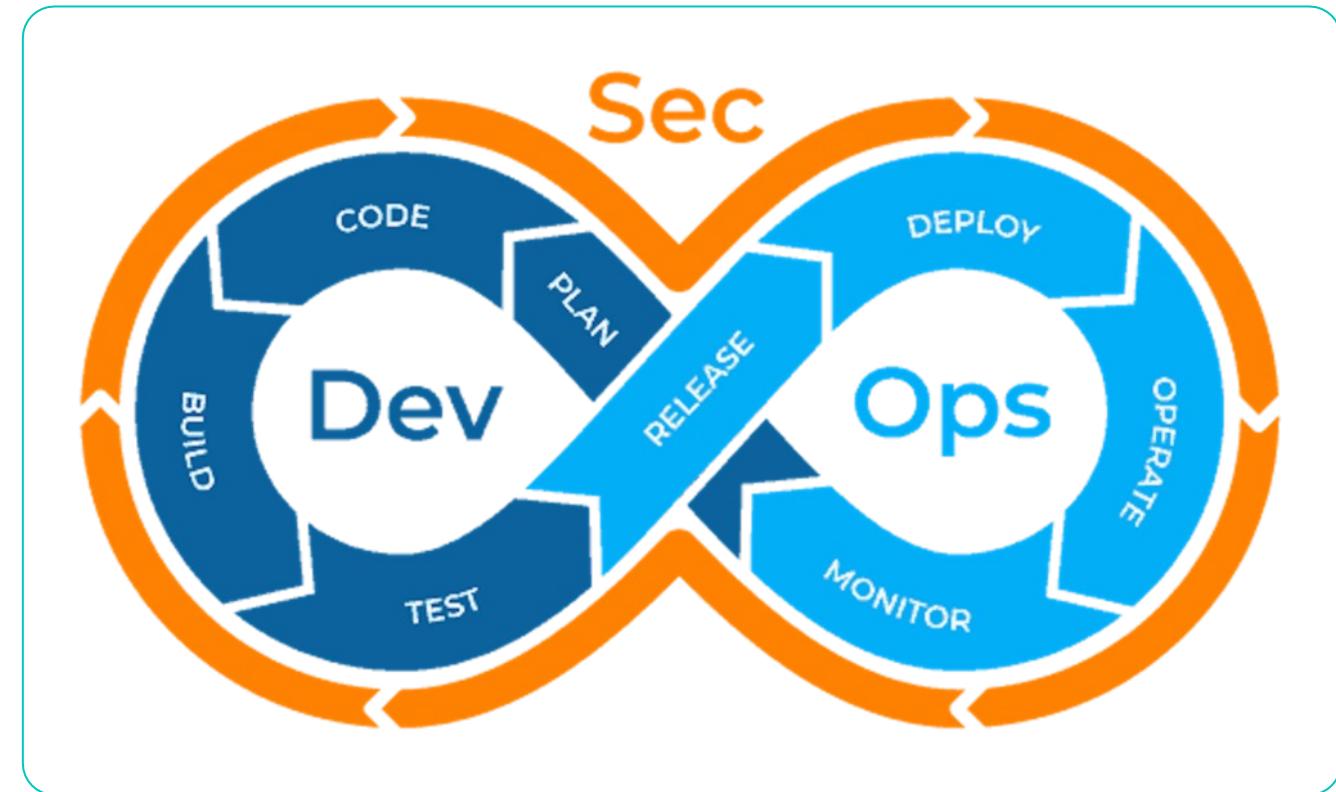
Quality and Performance
meets the quality, speed, scalability, reliability, and other expectations

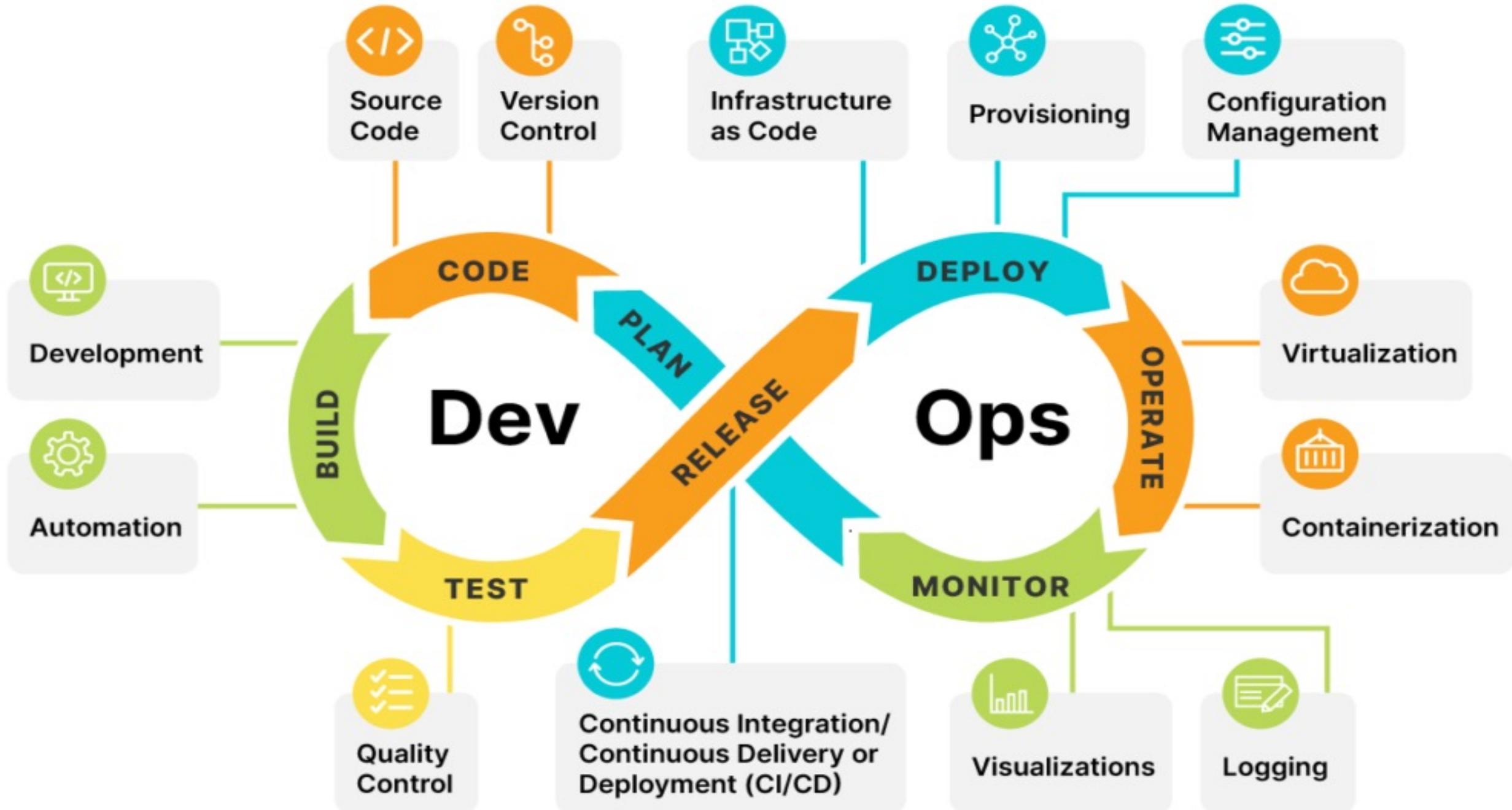
Innovation is the lifeblood of an organization in the digital age and needs to be both enabled and protected

What is DevSecOps?

Technology innovation is frequently developed in the context of a **rapid lean and agile** development approach that combines development and operations together into a **DevOps** process.

Integrating **security** into the process creates a **DevSecOps** process.





Attacker Opportunities

Note: Attackers may conduct a multi-stage attack that increases their illicit access with stolen credentials, stolen keys, implanting malware, implanting backdoors in code, and more

Planning

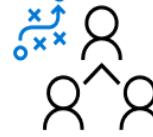


Public
repository

Coding Vulnerability
Introduce exploitable vulns

Writing New Code

Design Vulnerability
Design Choices create Security Issues



Developer
team



Application
code

Coding

Supply Chain Vuln/Implant
Vulnerable Code added to Application



Corporate
repository



Developer
Workstation

Upload to
Repository

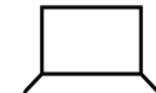
Web/Email Risk
On Dev workstation

Testing

Production App Vulnerability
Vuln Discovered in App or a Re-used Component



Build
automation



Tester
Workstation

Production



Version
release

IT Infrastructure attacks



Phishing, credential theft, unpatched browser or endpoint vulnerability, weak passwords, old/weak authentication protocols, weak security configuration for cloud, etc.

DevSecOps controls



Plan and Develop

- Threat modelling
- IDE Security plugins
- Pre-commit hooks
- Secure coding standards
- Peer review

Commit the code

- Static application security testing
- Security unit and functional tests
- Dependency management
- Secure pipelines

Build and test

- Dynamic application security testing
- Cloud configuration validation
- Infrastructure scanning
- Security acceptance testing

Go to production

- Security smoke tests
- Configuration checks
- Live Site Penetration testing

Operate

- Continuous monitoring
- Threat intelligence
- Penetration testing
- Blameless postmortems

Challenges for Security Operators

“Driving security into **every aspect** of the development **lifecycle** is difficult to achieve without **visibility** into what **Developers** are building”

Challenges for Developers

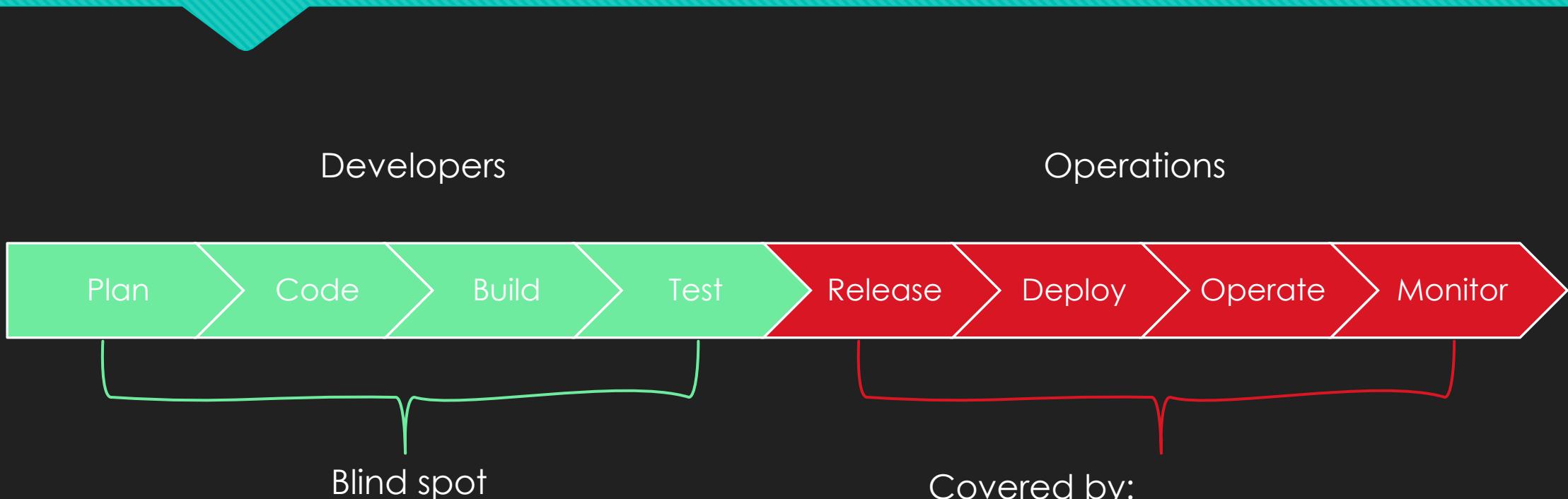
Developers often use **multiple solutions** to achieve **holistic** security coverage while writing code.

Developers need this information **at development time** and on pull requests so they can use the tools with which they are most familiar.

Additionally, Developers are **not the security experts**.

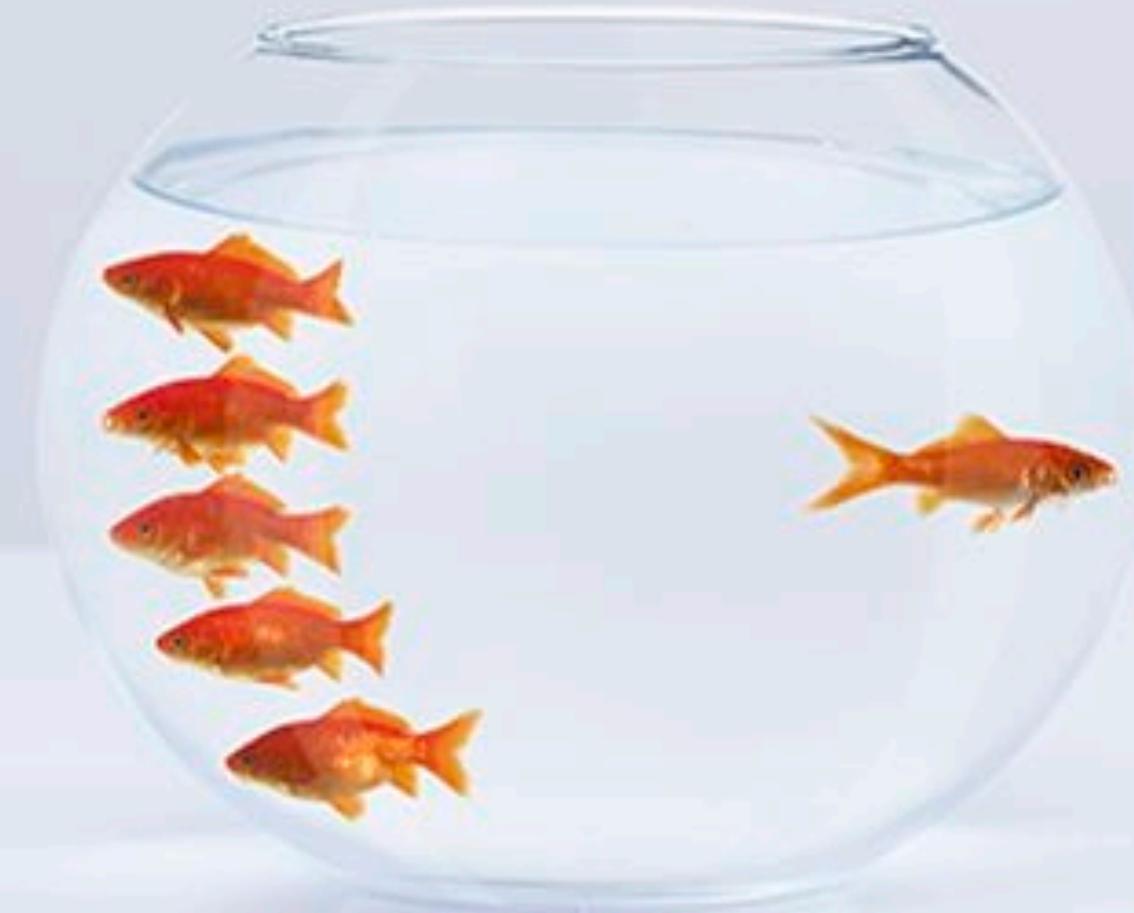


Security coverage



Covered by:

- DevOps / GitHub
- Defender for Cloud (Server, SQL, container etc)
- Azure Firewall/WAF
- Sentinel



Shift security Left

Defender for DevOps Can Help

1. Unified visibility into DevOps security posture
2. Strengthen cloud resource configurations throughout the development lifecycle
3. Prioritize remediation of critical issues in code



Microsoft Defender for DevOps

Microsoft Defender for DevOps adds additional security capabilities to the robust Microsoft Defender for Cloud service for security posture management and threat protection for code, code management systems, and deployment pipelines.



Vulnerabilities in Code

*Keep dependencies up-to-date with automated pull requests
Detect and monitor for leaked credentials and secrets*



Secure and Compliant Infrastructure-as-Code (IaC)

*Deploy and enforce policy to ensure uniformity and best practices
Find and fix issues before they are deployed, prevent drift*



Security Monitoring

*Respond to suspicious activities in code, pipelines, and the developer cloud
Assess the impact of vulnerabilities and risk clearly and easily*



Continuous Cloud Security and Compliance

*Assess and view state of pre-production resources
Compare posture to security and compliance standards
Leverage attack graphs & attack simulation*



Secure Cloud-Native Workloads

Multi-cloud integration, Containers, Serverless, APIs

Overview

Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | DevOps Security (Preview)

Showing subscription 'MVP' | 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

Security Overview

DevOps security vulnerabilities

Severity	Count
High	0
Medium	16
Low	0

DevOps security results

8 Code scanning vulnerabilities	0 Exposed Secrets
0 OSS vulnerabilities	12 Recommendations

DevOps coverage

2 Github Connectors	1 Azure DevOps Connectors
---------------------	---------------------------

48 Total

Github repositories 47 Azure DevOps repositories 1

Search Subscriptions == MVP Resource Types == Github Repository, Azure DevOps Repository

Name	Pull request status	Total exposed secrets	OSS vulnerabilities	Total code scanning vulnerabilities
demoDFD	N/A	Healthy	0	4
demoDFD	N/A	Healthy	0	4
demoDFD02	N/A	Healthy	0	4
demoDFD02	N/A	Healthy	0	4
demoDFD	On	Healthy	N/A	0
pkhabazi.github.io	N/A	Healthy	0	0

Cloud Security

- Security posture
- Regulatory compliance
- Workload protections
- Firewall Manager
- DevOps Security (Preview) (Selected)

Management

- Environment settings
- Security solutions
- Workflow automation

Resource health

Home > Microsoft Defender for Cloud | DevOps Security (Preview) >

Resource health

... X

demoDFD
GitHub repository

3 Active recommendations | 0 Active alerts

Resource information

Subscription	Resource Group
MVP	securitymeetup
Environment	Connector
Azure	github-demo
Resource type	GitHub repository

Recommendations Alerts

Search More (2)

Severity ↑	Description	Status ↑↓
High	GitHub repositories should have secret scanning enabled Preview	• N/A - Unspecified
Medium	Code repositories should have infrastructure as code scanning findings resolved Preview	● Unhealthy
Medium	Code repositories should have code scanning findings resolved Preview	● Unhealthy
Medium	GitHub repositories should have code scanning enabled Preview	● Healthy
Medium	GitHub repositories should have Dependabot scanning enabled Preview	● Unhealthy

< Previous Page 1 ▼ of 1 Next >

Detailed overview

Home > Microsoft Defender for Cloud | DevOps Security (Preview) > Resource health >

Code repositories should have code scanning findings resolved

[Open query](#) X

Severity	Freshness interval	Tactics and techniques
Medium	30 Min	Initial Access +1

[Description](#)
Defender for DevOps has found vulnerabilities in code repositories. To improve the security posture of the repositories, it is highly recommended to remediate these vulnerabilities.

[Remediation steps](#)

[Security checks](#)

Findings

Search to filter items...

ID	Security check	Category	Severity
e18b3643-d755-c6bc-9a84-8bc7c5e33a4f	Try, Except, Pass detected.	Code	Medium
f5508800-0b2a-2a80-59ae-f90552fa8b46	Try, Except, Continue detected.	Code	Medium
305d6cfa-9fde-e69d-b40b-ca551094ff59	Use of insecure MD2, MD4, MD5, or SHA1 hash function.	Code	Medium
eeb47727-1a3b-b4d6-837d-0b41b64f1ef7	Use of insecure MD2, MD4, MD5, or SHA1 hash function.	Code	Medium

Direct link to vulnerability

PREVIEW

^ **Description**

API App should only be accessible over HTTPS.

^ **General information**

ID	58841320-38ed-37d6-3c75-6659a081707b
Severity	⚠ Medium
Status	✖ Unhealthy

^ **Additional information**

State	Open
Branch	refs/heads/main
Path	insecure_arm.json
Line	29
Tool Name	templateanalyzer
Rule ID	TA-000004
SARIF Severity	error
URLs	Html URL <input type="checkbox"/> Repo Url <input type="checkbox"/>

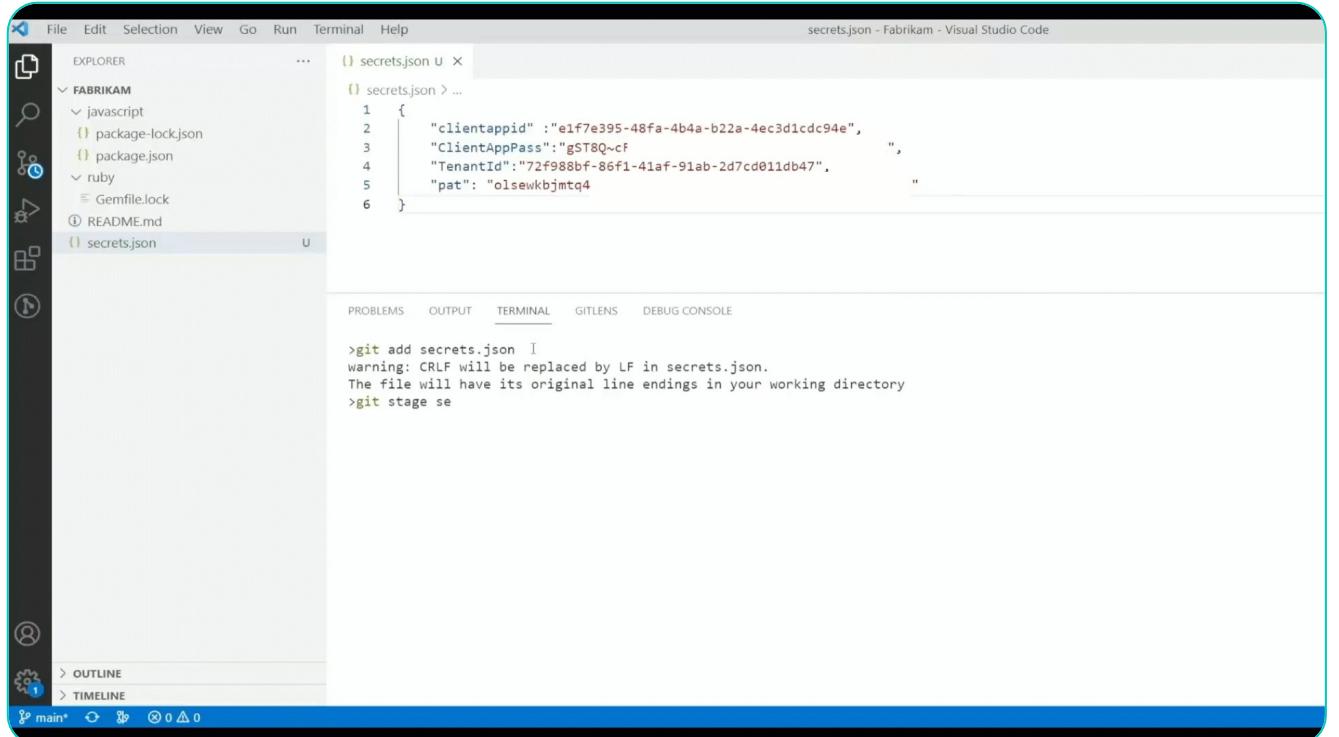
^ **Affected resources**

Name	Subscription
------	--------------

Two layers

- Platform vulnerability
- Code vulnerability

GitHub Advanced security



A screenshot of the Visual Studio Code interface. The Explorer sidebar shows a project structure with folders for FABRIKAM, javascript, ruby, and files like package-lock.json, package.json, Gemfile.lock, README.md, and secrets.json. The secrets.json file is open in the main editor area, displaying the following JSON content:

```
1 {  
2   "clientappid": "e1f7e395-48fa-4b4a-b22a-4ec3d1cdc94e",  
3   "ClientAppPass": "gST8Q~cf",  
4   "TenantId": "72f988bf-86f1-41af-91ab-2d7cd011db47",  
5   "pat": "olsewkbjmtq4"  
6 }
```

The terminal at the bottom shows the following git commands being run:

```
>git add secrets.json  
warning: CRLF will be replaced by LF in secrets.json.  
The file will have its original line endings in your working directory  
>git stage se
```

GitHub workflow

```
# Install dotnet, used by MSDO
- uses: actions/setup-dotnet@v3
  with:
    dotnet-version: |
      5.0.x
      6.0.x

# 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.sariffFile }}

# Upload alerts file as a workflow artifact
- name: Upload alerts file as a workflow artifact
  uses: actions/upload-artifact@v3
  with:
    name: alerts
    path: ${{ steps.msdo.outputs.sariffFile }}
```

GitHub - Under the hood

Name	Language	License
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

DevOps Plugins



Microsoft Security DevOps
Microsoft | 826 installs | ★★★★★ (0) | Preview
Build tasks for performing security analysis.
[Get it free](#)



SARIF SAST Scans Tab
Microsoft DevLabs | 159,180 installs | ★★★★★ (0) | Free
Adds a 'Scans' tab to each Build Result and Work Item for viewing associated SARIF SAST logs.
[Get it free](#)

DevOps pipeline

```
steps:  
- task: UseDotNet@2  
  displayName: 'Use dotnet'  
  inputs:  
    version: 3.1.x  
  
- task: UseDotNet@2  
  displayName: 'Use dotnet'  
  inputs:  
    version: 5.0.x  
  
- task: UseDotNet@2  
  displayName: 'Use dotnet'  
  inputs:  
    version: 6.0.x  
  
- task: MicrosoftSecurityDevOps@1  
  displayName: 'Microsoft Security DevOps'
```

Name	Language	License
Bandit	Python	Apache License 2.0
BinSkim	Binary--Windows, ELF	MIT License
ESlint	JavaScript	MIT License
Credscan	Credential Scanner (also known as CredScan) is a tool developed and maintained by Microsoft to identify credential leaks such as those in source code and configuration files common types: default passwords, SQL connection strings, Certificates with private keys	Not Open Source
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

DevOps – Under the hood

DevOps result blade

 #20221121.7 • demo pr
 demoDFD

Run new ⋮

ⓘ This run is being retained as one of 3 recent runs by pipeline. View retention leases

Summary Scans ⋮

Filter by keyword Baseline: New (+2) Level: Error (+1) X

templateanalyzer 34 ^ ⋮

terrascan 10 ^ ⋮

DevOps Secret scan

demo pr

Active | 51 | Pouyan Khabazi testingPR into main 0/1 comments resolved

Overview Files Updates Commits

All required checks succeeded

No merge conflicts Last checked Yesterday

Description

move files

Add a comment...

Pouyan Khabazi reactivated the pull request

Pouyan Khabazi abandoned the pull request

password.ps1
/samples/password.ps1

```
1 + $TenantId = '1da6230b-391f-4a71-bd8e-ccccccc'
2 + $ApplicationId = 'eb834708-2844-4a16-b760-3222222'
3 + $Password = '4Ui8Q~NsWD0x4566434354354hjick;knv7tfcre5dckdTJG7otbzrAagG'
4 +
5 + $SecuredPassword = $Password | ConvertTo-SecureString -AsPlainText -Force
6 + $Credential = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $ApplicationId, $SecuredPassword
```

Microsoft Defender for DevOps Yesterday

High severity

Information: General Password.

Issue ID: CSCAN-GENERAL0060

Remediation: A potential secret was detected. Validate file contains secrets, remove, rotate credential, and use approved store. For a on secret remediation see <https://aka.ms/CredScanDocs>

Write a reply...



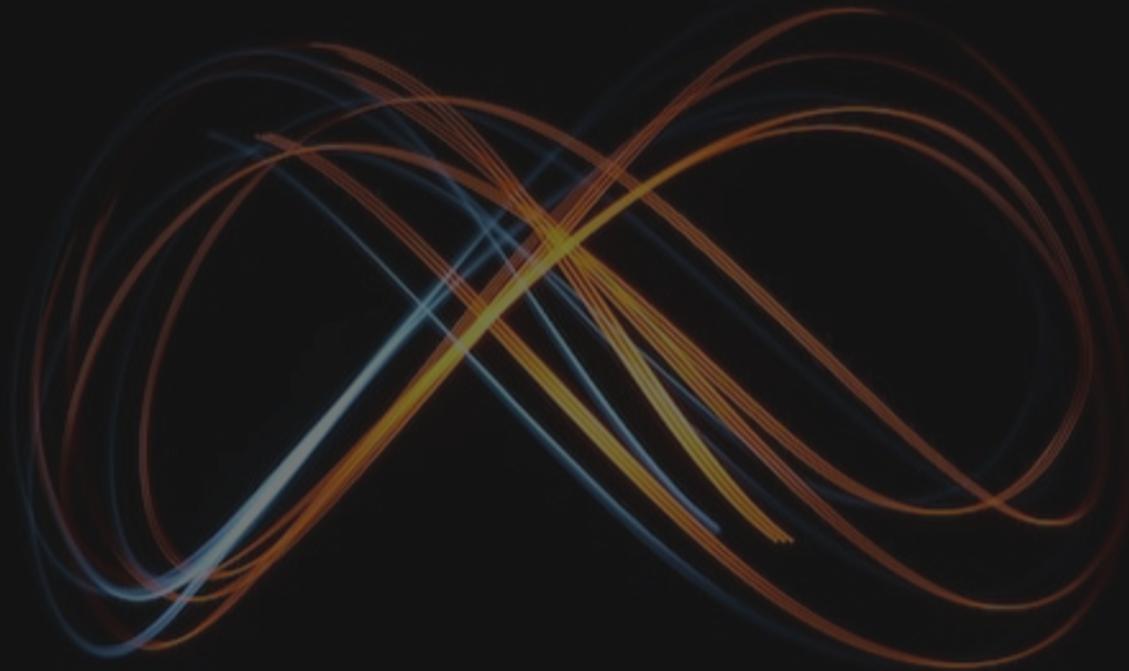
Demo

Missing features:

- IDE security plug-ins and pre-commit hooks
- Sentinel Integration

Open questions

- Pricing
- GA Time



Infinite mindset to cloud security