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

Pouyan Khabazi

Co-founder @EightFence

Microsoft® Most Valuable Professional

EIGHTFENCE

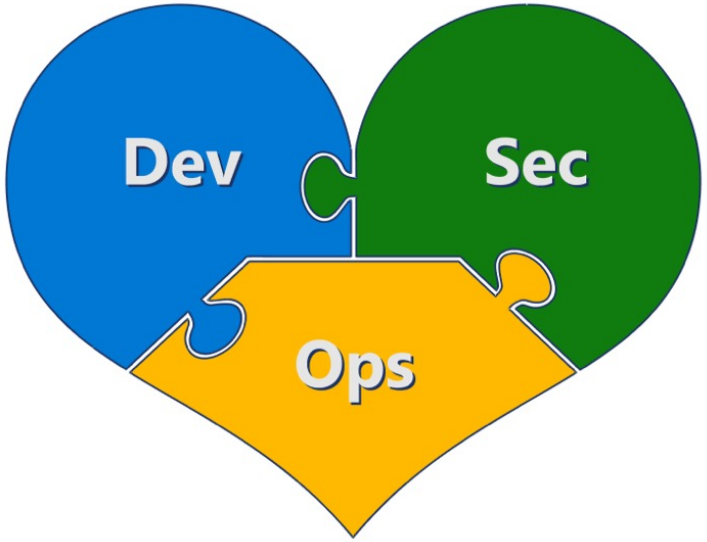
Part of Codeinceps Group

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

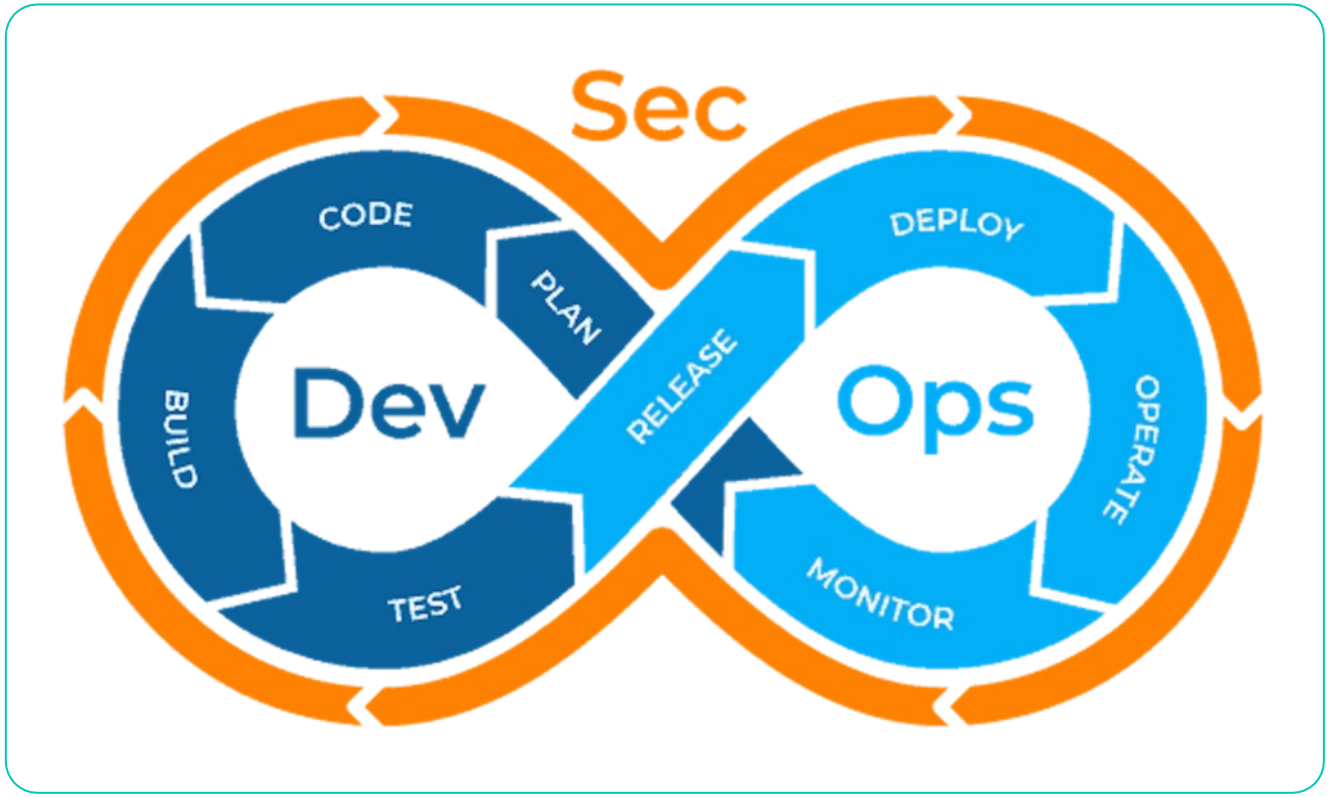
Quality and Performance
meets the quality, speed, scalability, reliability, and other expectations

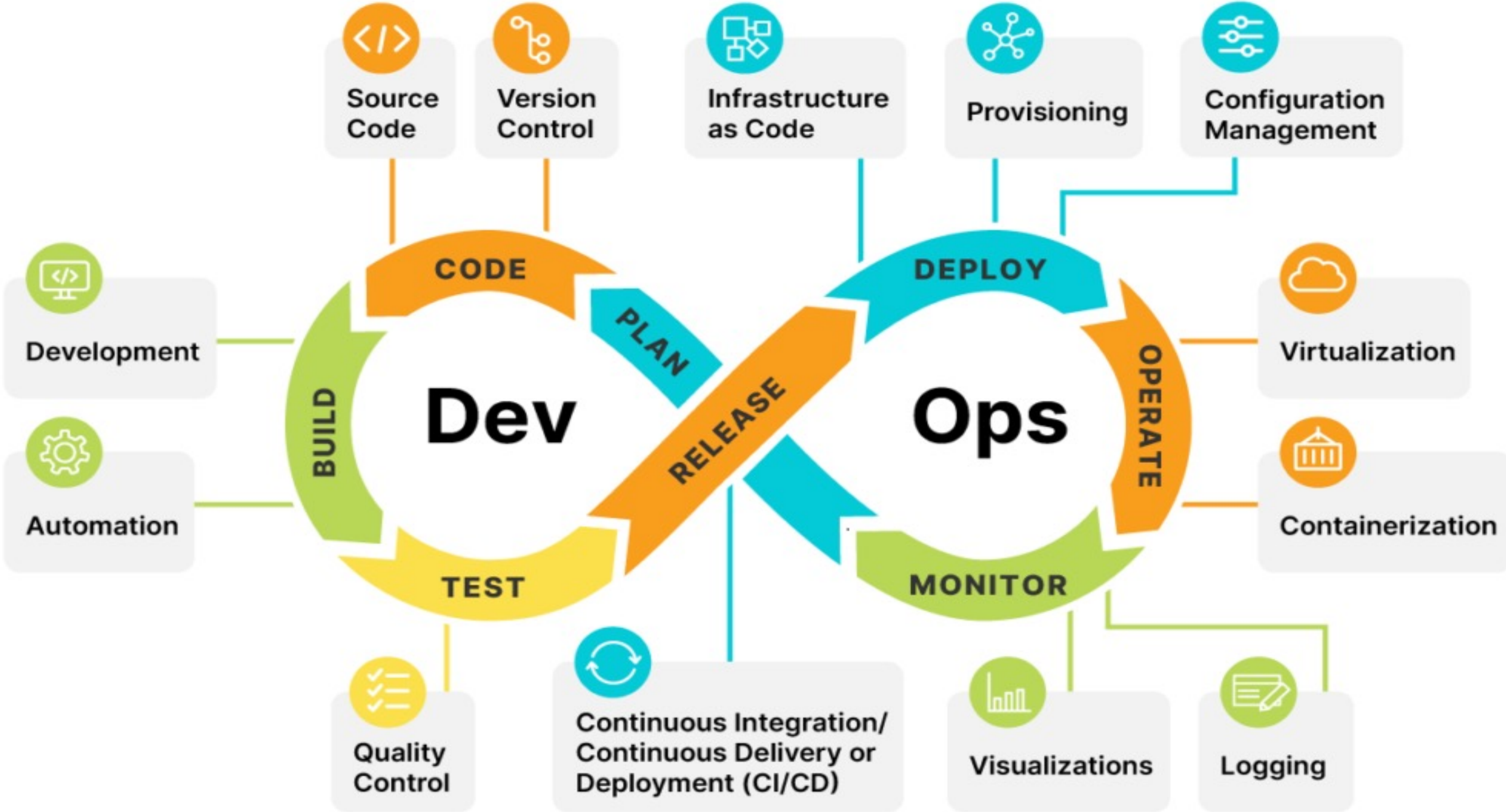
Innovation is the lifeblood of an organization in the digital age and needs to be both enabled and protected

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.

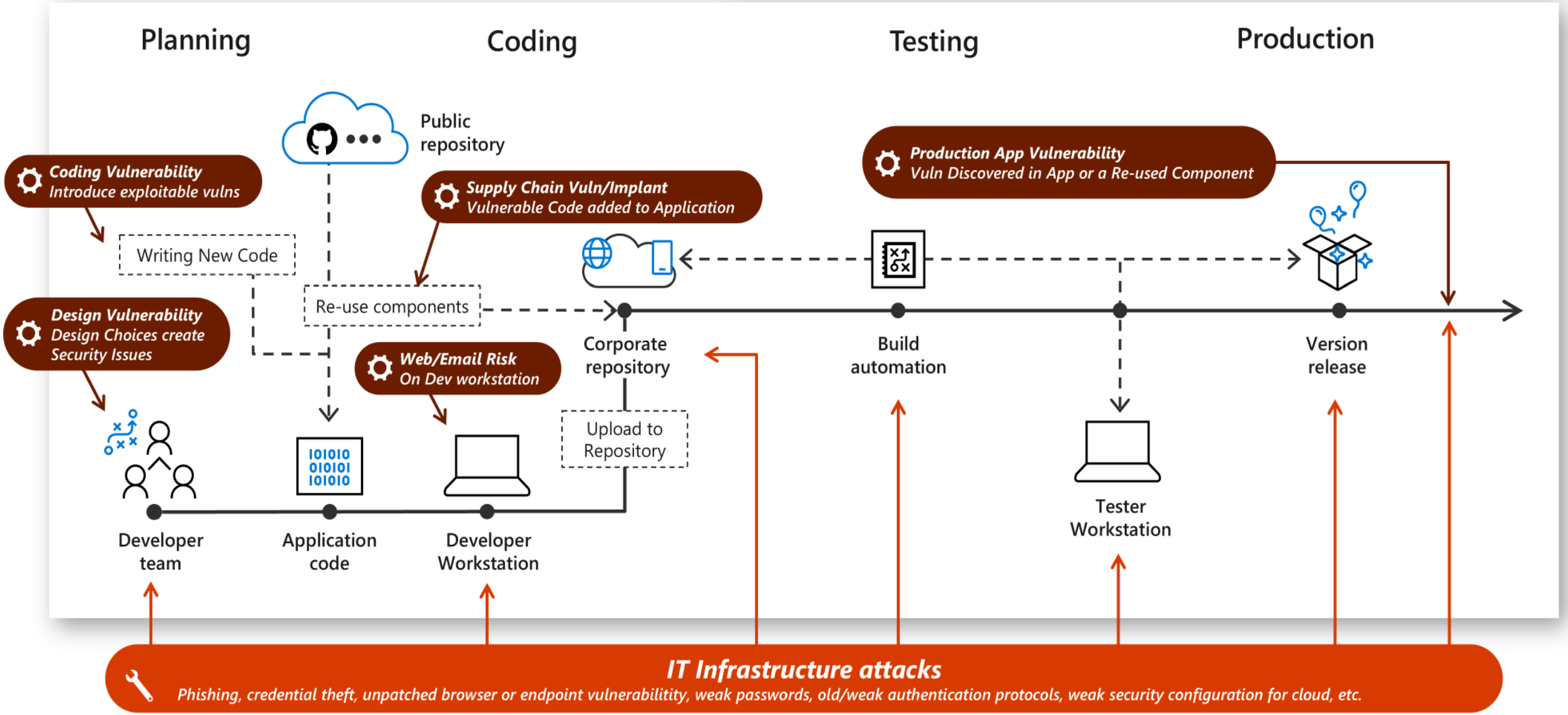
Integrating **security** into the process creates a **DevSecOps** process.




Source Code
Version Control
Infrastructure as Code
Provisioning
Configuration Management
Development
Automation
CODE
PLAN
BUILD
TEST
RELEASE
DEPLOY
OPERATE
MONITOR
Dev
Ops
Virtualization
Containerization
Quality Control
Continuous Integration/ Continuous Delivery or Deployment (CI/CD)
Visualizations
Logging

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



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

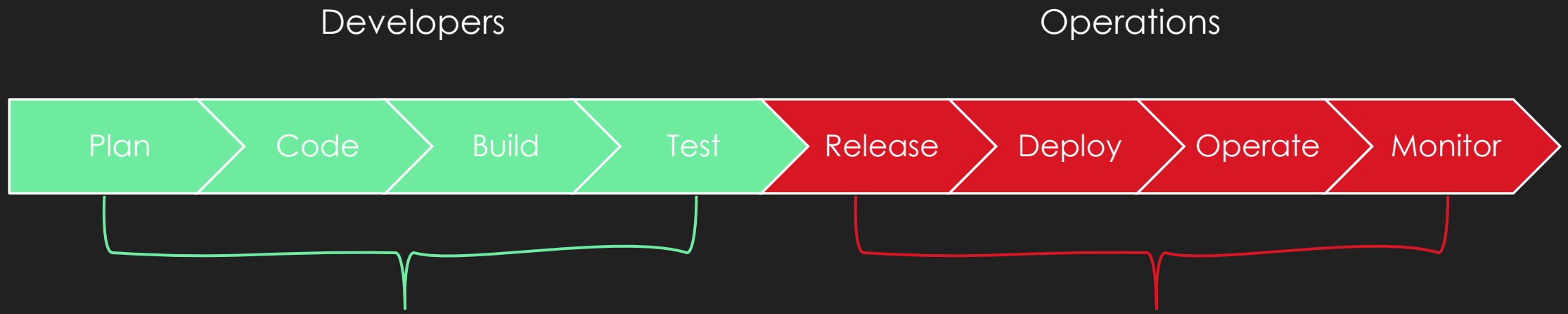
"Driving security into **every aspect** of the development **lifecycle** is difficult to achieve without **visibility** into what **Developers** are building"

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




Shift security Left

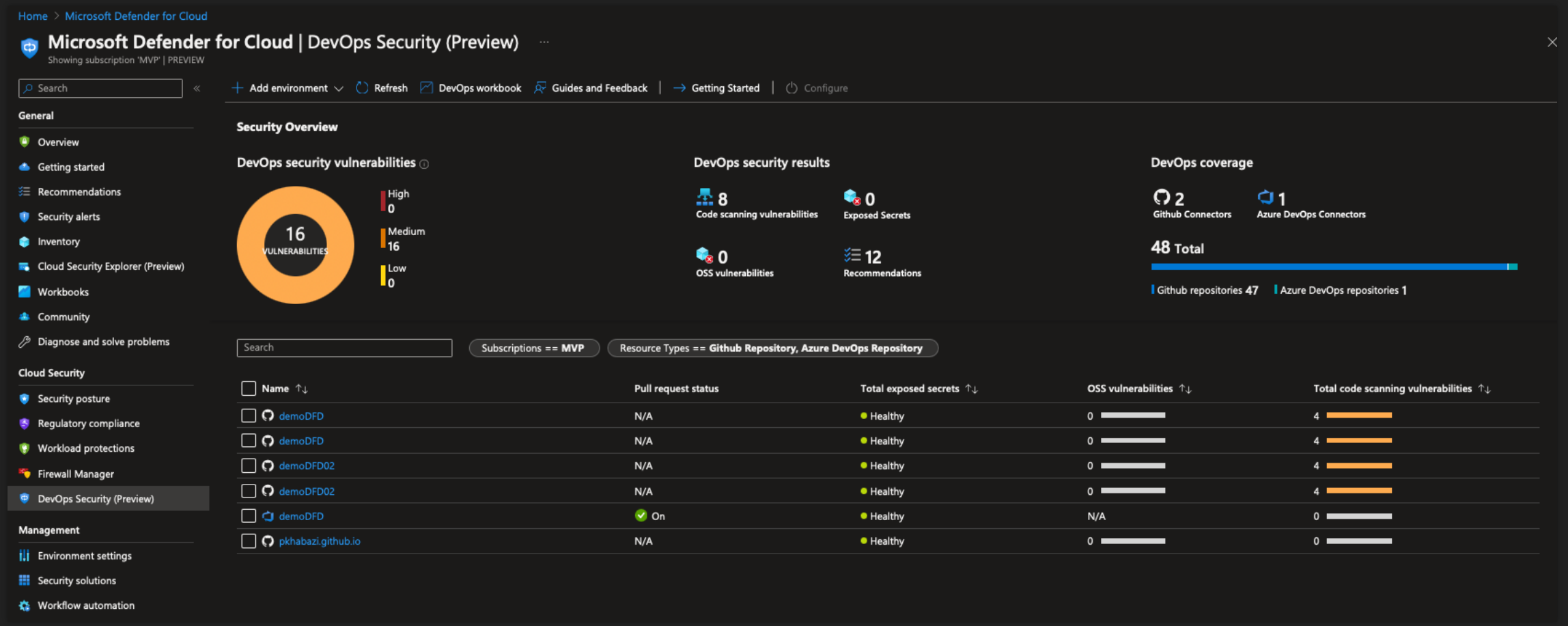
Defender for DevOps Can Help

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

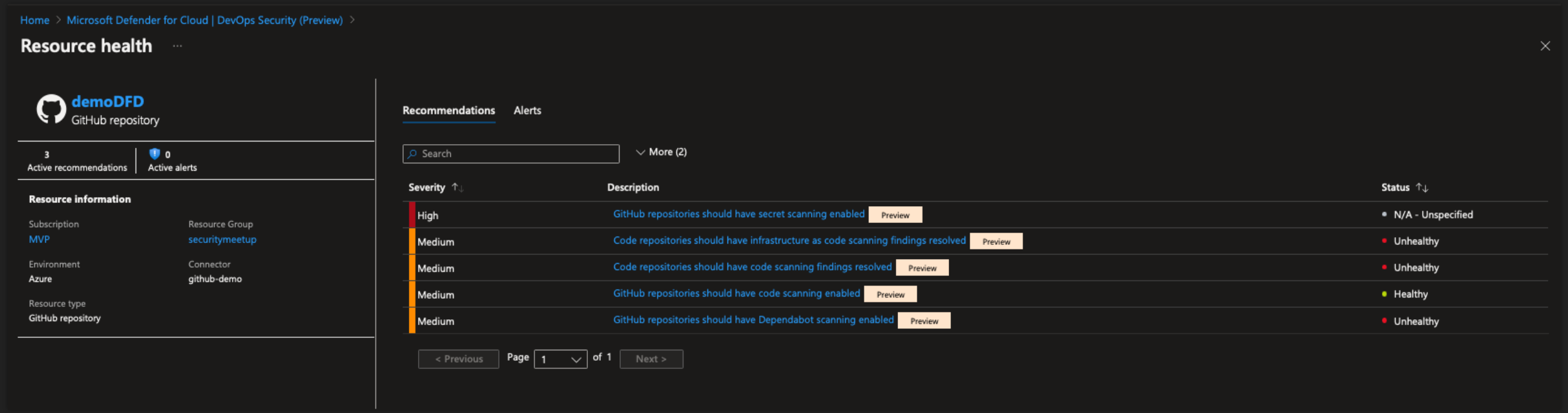
Microsoft Defender for DevOps

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.

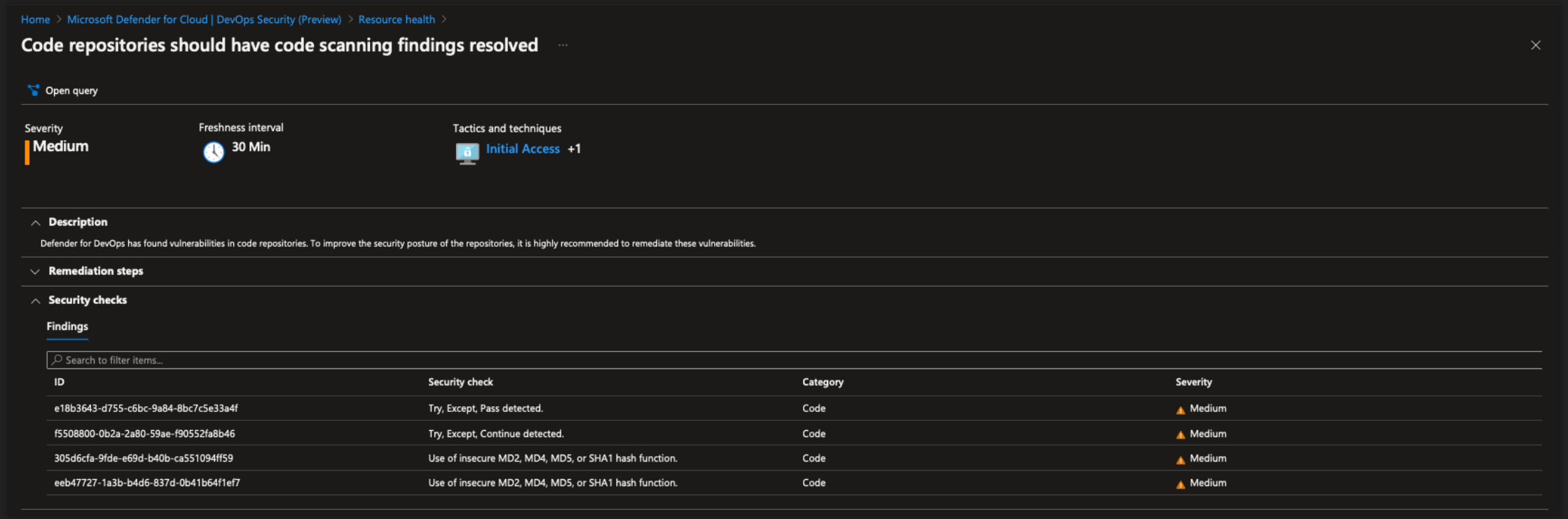
Overview


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
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
16
VULNERABILITIES
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

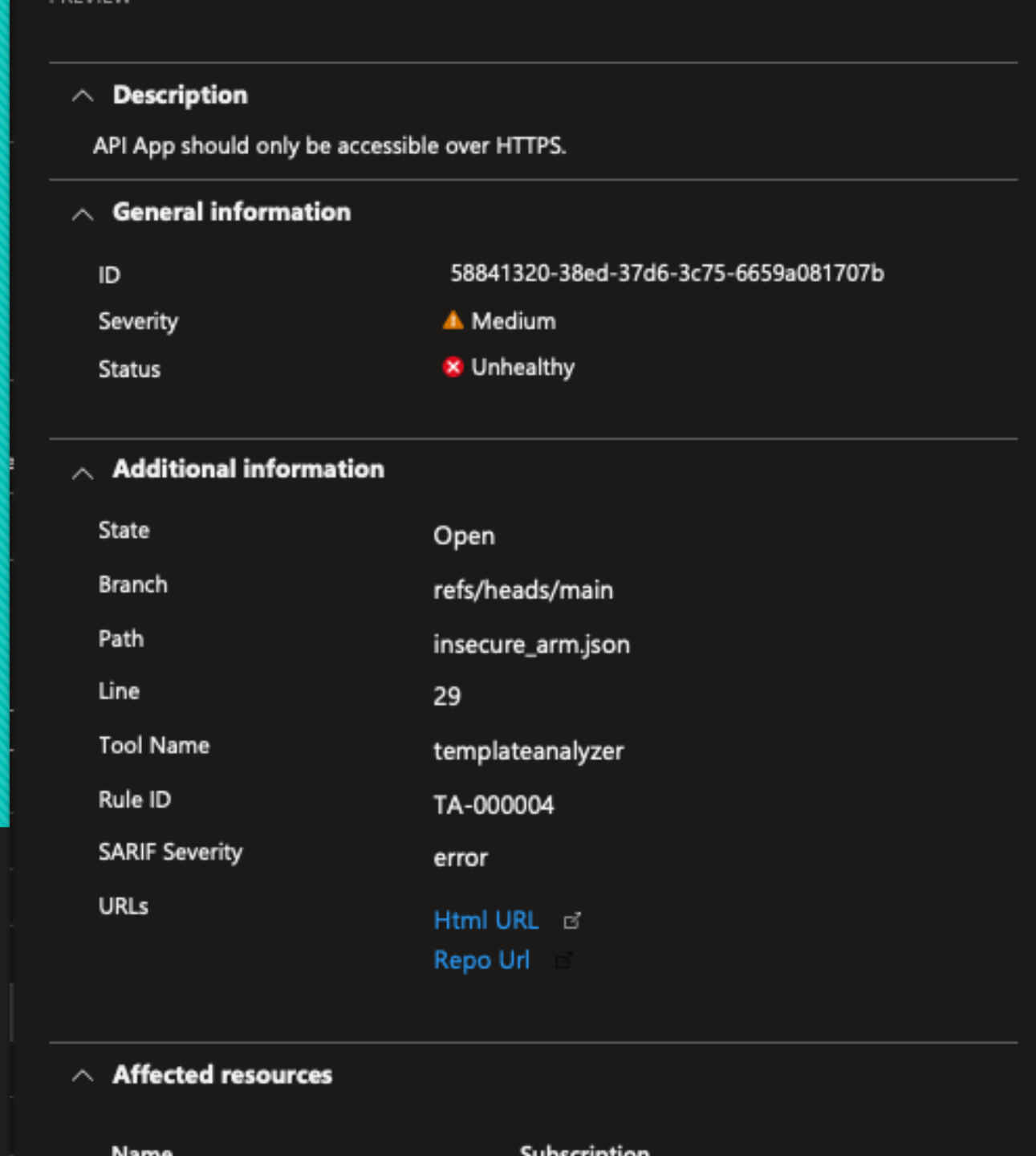
Resource health



Detailed overview



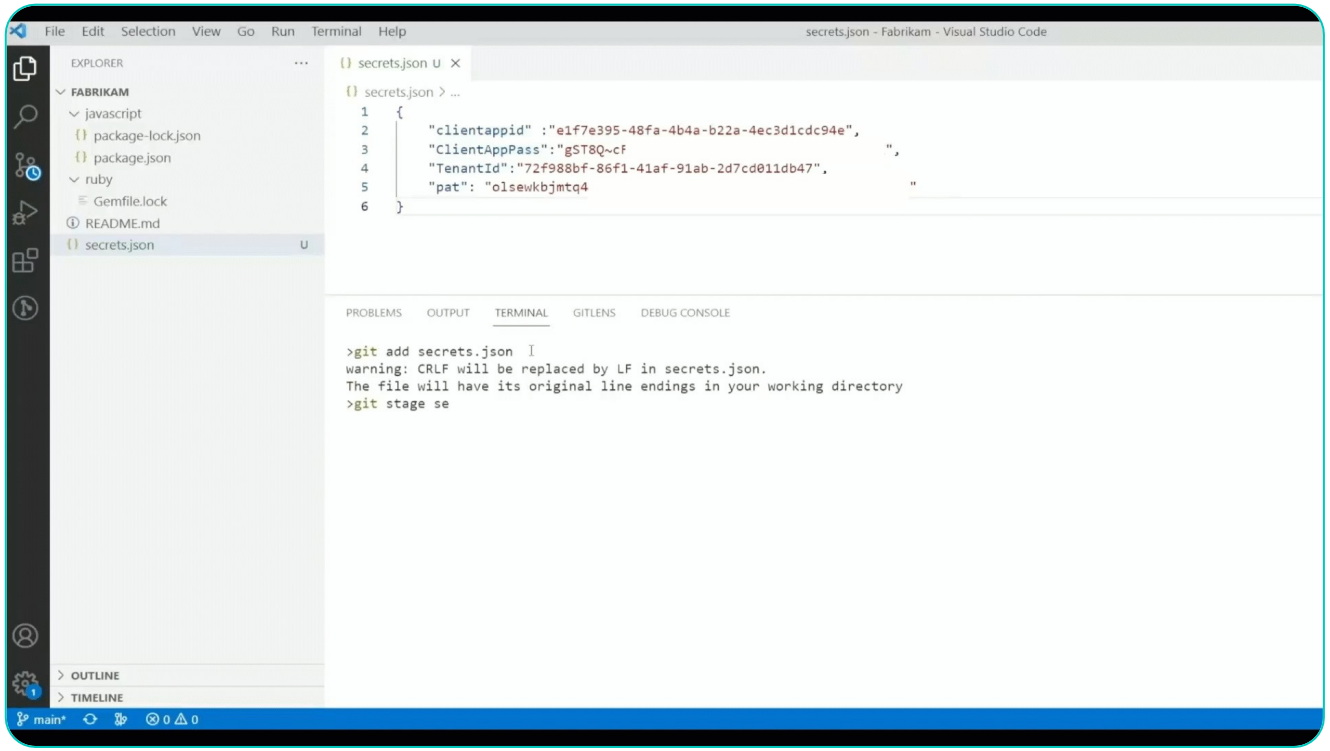
Direct link to vulnerability



Two layers

- Platform vulnerability
- Code vulnerability

GitHub Advanced security



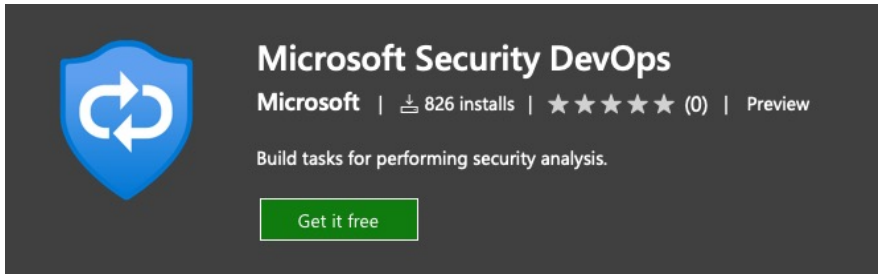
GitHub workflow

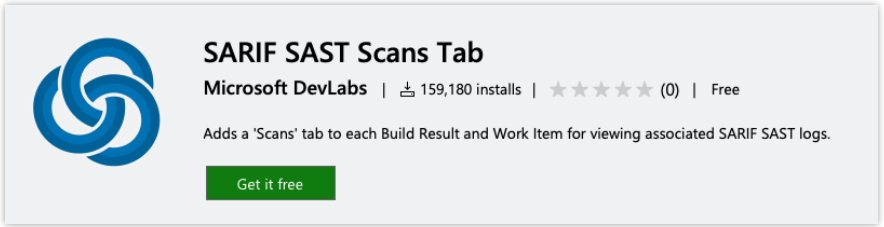
```yaml
    # Install dotnet, used by MSDO
  - uses: actions/setup-dotnet@v3
    with:
      dotnet-version: |
        5.0.x
        6.0.x

    # 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.sarifFile }}

    # 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.sarifFile }}
```

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





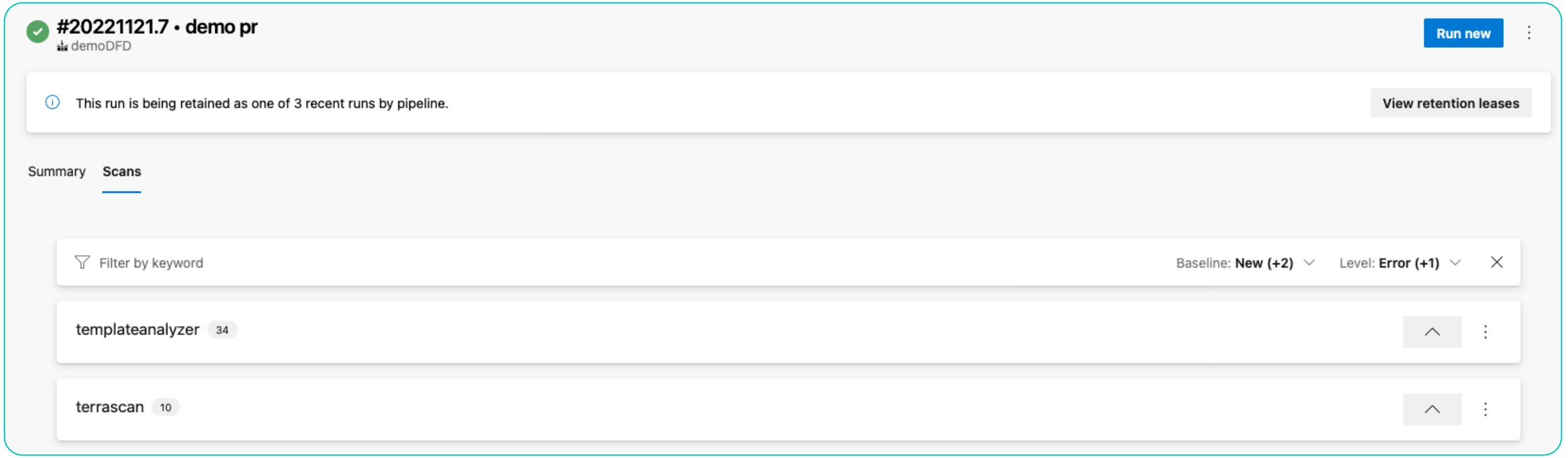
DevOps pipeline

```yaml
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



DevOps Secret scan

demo pr

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

Overview Files Updates Commits

All required checks succeeded

View 2 checks

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-cccccccc'
2 + $ApplicationId = 'eb834708-2844-4a16-b760-3222222'
3 + $Password = '4Ui8Q~NsWDOx4566434354354hjiok;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...

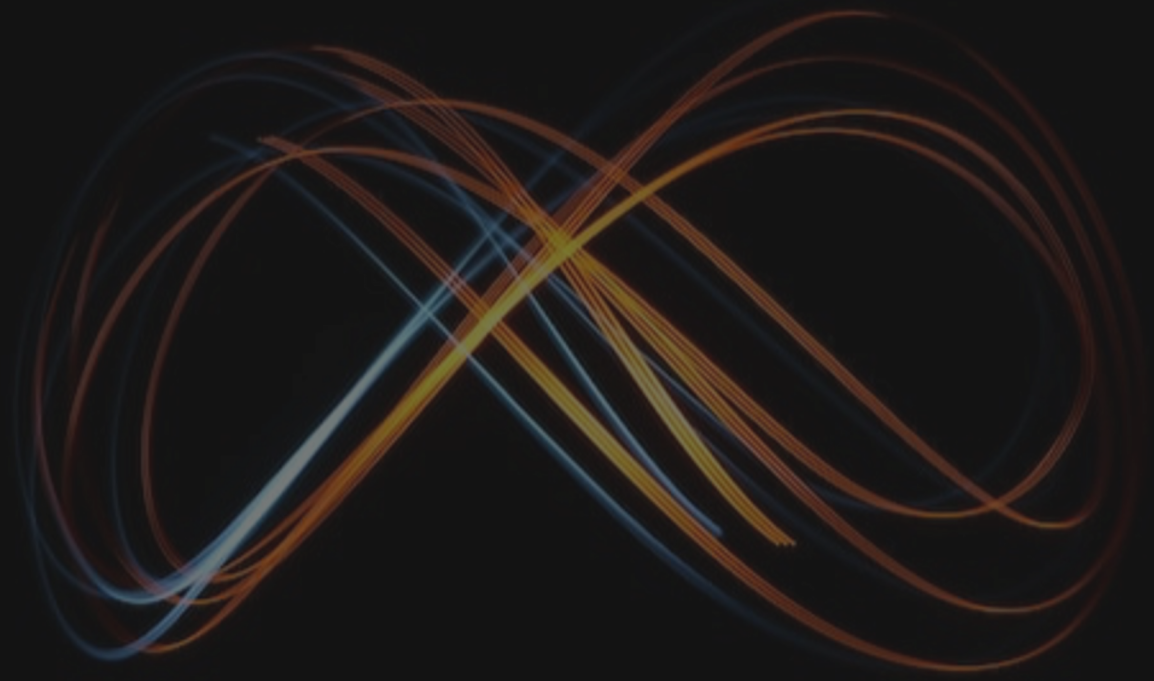
Demo

Missing features:

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

Open questions

- Pricing
- GA Time



Infinite mindset to cloud security