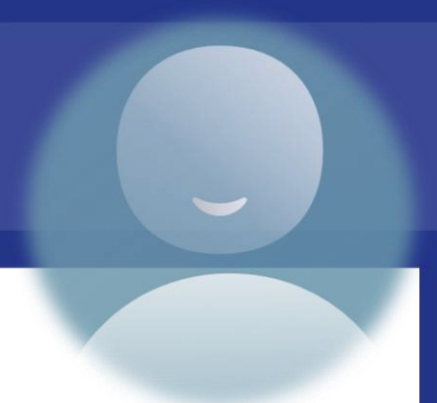




CONF42 DEVSECOPS 2024

DECEMBER 5 • ONLINE



DevSecOps as an approach to building and deploying secure apps by “shifting left”

Peter De Tender

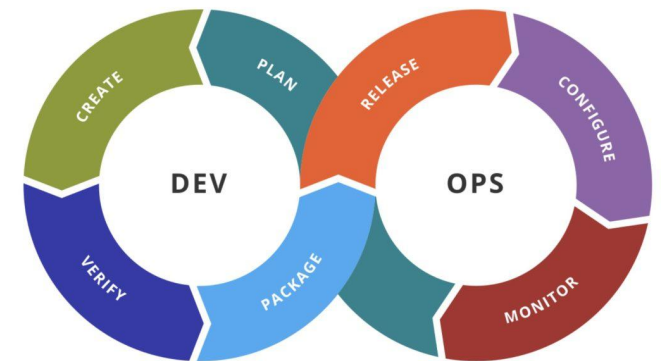
Microsoft Technical Trainer

Microsoft Corp, Redmond, WA

<https://aka.ms/pdtit>

<https://linkedin.com/in/pdtit>

petender@microsoft.com



What will be covered



DEVOPS



SHIFT LEFT
MENTALITY



DEVSECOPS
TOOLING



DEMOS

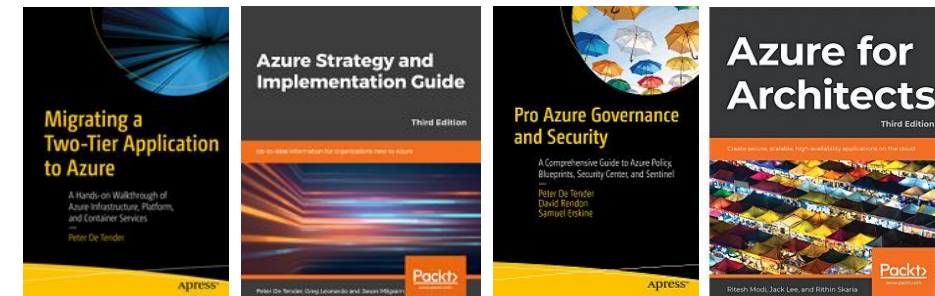


Q & A



About Me : Peter De Tender

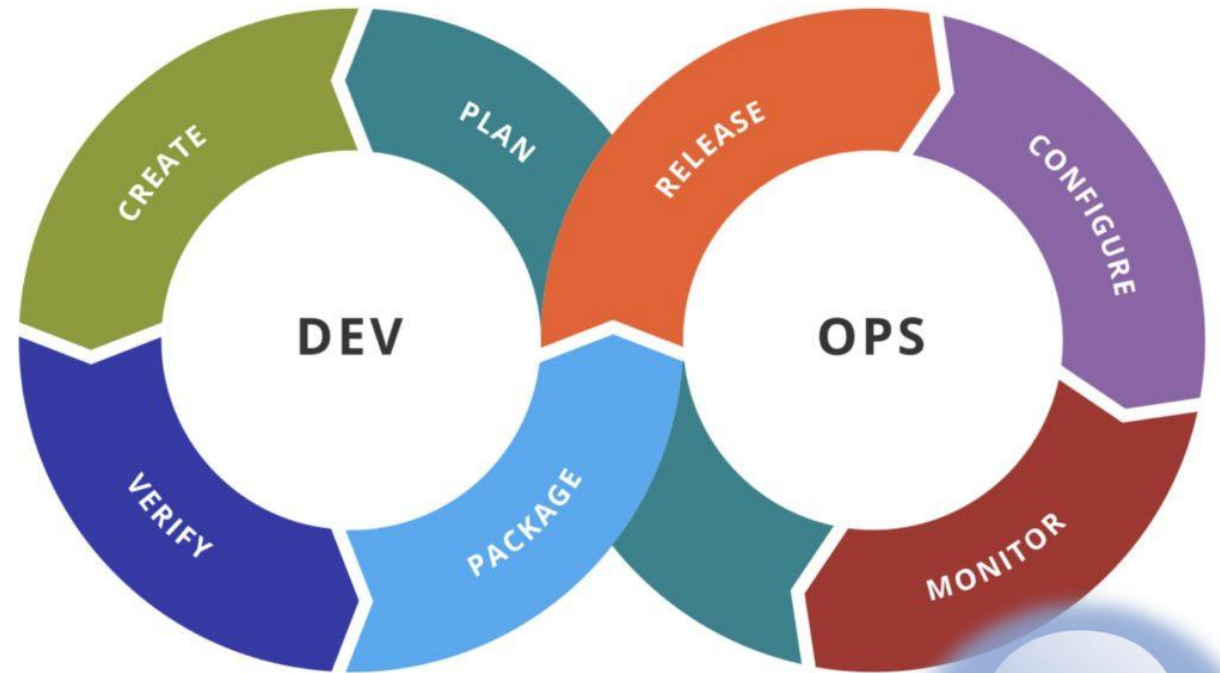
- Azure Technical Trainer and Cloud Advocacy v-team @ Microsoft with focus on Azure Architecting and Microsoft DevOps Solutions
- Former Azure MVP (6y)
- Technical Writer & Book publisher



Concepts of DevOps

Microsoft's Definition:

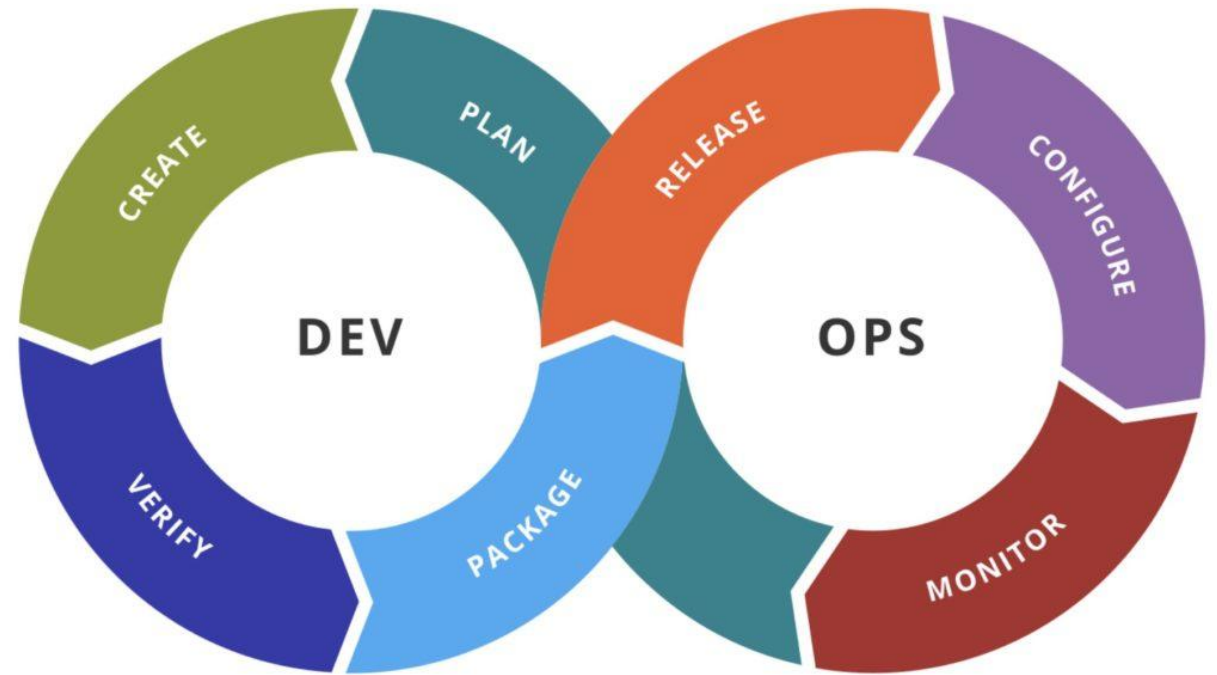
*The Union of People,
Processes and Products,
to enable continuous
delivery of value to our
end users*



Concepts of DevOps

Peter's Definition:

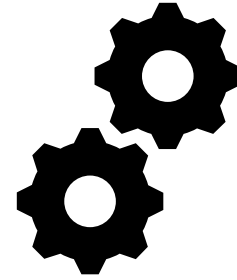
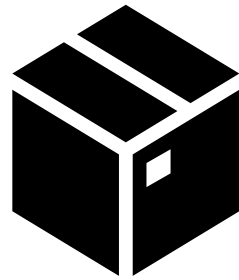
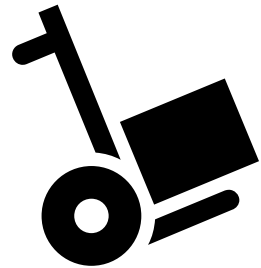
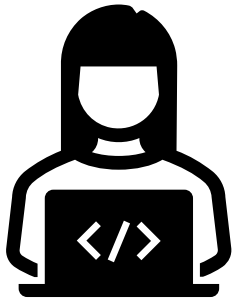
Integrating a culture of delivering value to your end users, relying on team collaboration and workload automation



60% - Culture 40% - Tools



Automate Everything



DEV

VALIDATE

PACKAGE

RUN

OPERATE

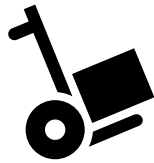
Automate Everything!!

Secure Everything



DEV

- Threat Modeling
- Secure Coding Standards
- Credentials & Secrets management
- Peer Review



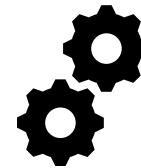
VALIDATE

- Code Analysis
- Credentials & Secrets management
- Approvals
- Unit Testing
- Container Vulnerability Scanning



PACKAGE

- Secured IaC
- Secured Containers
- Quality Gates
- Cloud Configuration
- Security & Pen-testing



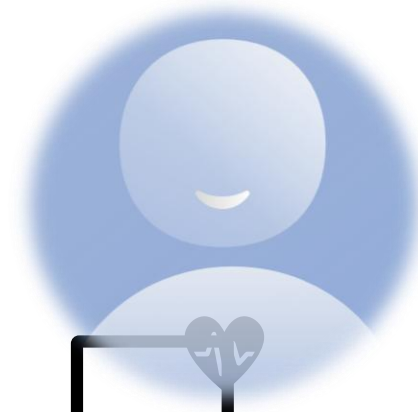
RUN

- Cloud Platform Security
- RBAC permissions model
- Credentials & Secrets management



OPERATE

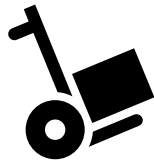
- Security Monitoring
- Threat Detection
- Mitigation



Secure Everything – by shifting left



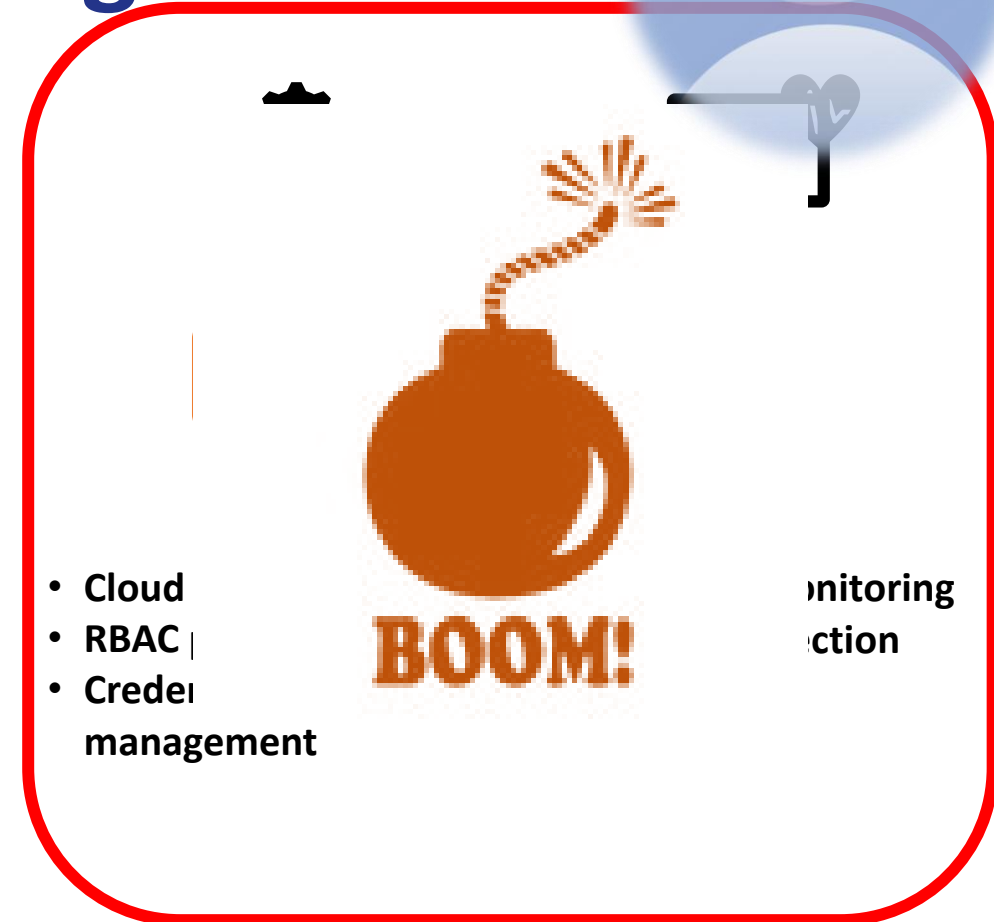
- Threat Modeling
- Secure Coding Standards
- Credentials & Secrets management
- Peer Review



- Code Analysis
- Credentials & Secrets management
- Approvals
- Unit Testing
- Container Vulnerability Scanning



- Secured IaC
- Secured Containers
- Quality Gates
- Cloud Configuration
- Security & Pen-testing



- Cloud
- RBAC |
- Credential management

Monitoring
ction

Demo

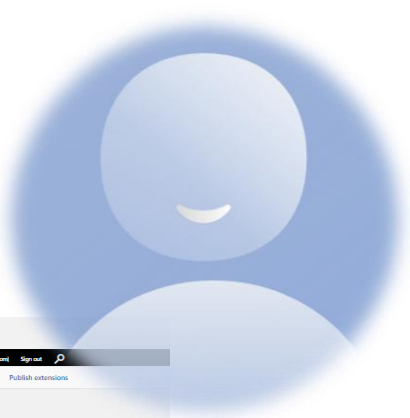
Approvals & Pull requests



Demo

Code Analysis

Credentials & Secrets Management



The screenshot shows the Visual Studio Marketplace interface with a search for 'security'. The results are displayed in a grid of 24 items, each with a logo, name, version, and a brief description. The items include:

- Snyk Security Scan
- ADO Security Scanner
- Security Scan
- Container Security
- Security Scan
- Serverless Security
- Hdr Security Integr
- Metasploit Security
- Codified Security
- REST API Static Security
- AI-R Security Assess
- Beagle Security Test
- azure-novosecure-ai
- SonarQube
- Secure DevOps Kit
- API Management Security
- Secure Development
- Kiwan FIS Extension
- Alcide Kubernetes
- OWASP Zed Attack Framework
- Secure area and Remote
- Appknox
- WhiteSource Bolt
- Konduito Vulnerability
- Veracode
- SD Elements Integr
- Qualys Container Security
- NeuVector
- Konduito Vulnerability
- WhiteSource for Azure

Azure DevOps Security: Your Personal Access Tokens (PAT) have been found in a public GitHub repository.

We are notifying you that Azure DevOps security team has identified that one of your Personal Access Tokens (PAT) named SonarCloud associated with user petender@microsoft.com have been found exposed in the following public GitHub repository.

<https://github.com/JLPacherie/sicm-workspace/blob/5635a9782e0d02c8b058271824ba43196f3d543c/libraries/Servers/SNR-002.json>

We encourage you to take immediate action by revoking this leaked token and mitigate any risks associated with this leakage. Please see the public documentation on how to revoke a personal access token.

[Authenticate with personal access tokens - Azure DevOps | Microsoft Docs](#)

We will go ahead and revoke this personal access token by **Jan 28 2021** if the PAT is still found active.

You can create a new personal access token and use that for business continuity in place of the revoked token. Please see the public documentation on how to create a new personal access token.

[Authenticate with personal access tokens - Azure DevOps | Microsoft Docs](#)

As a good security practice, if you are using other tokens, please ensure that they are not checked into any public or private repositories.

Reach out to Azure DevOps Security SMEs (<mailto:azdevsecsme@microsoft.com>) if you have any questions or concerns.

Azure DevOps Security Team





Secure Everything – by shifting left

Some Container Vulnerability Scanning Solutions (No preference!!)

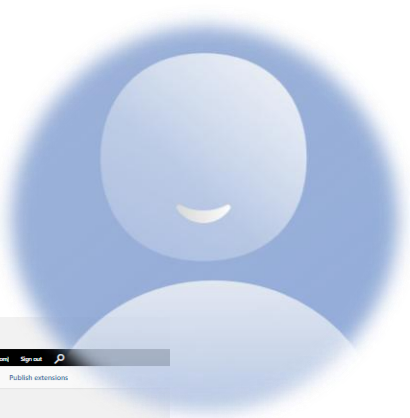
1. AquaSec (<https://www.aquasec.com/products/container-vulnerability-scanning/>)
2. Qualys (<https://www.qualys.com/apps/container-security/>)
3. Clair (<https://github.com/quay/clair>)
4. Anchore (<https://anchore.com/opensource/>)
5. Docker Bench Security (<https://github.com/docker/docker-bench-security>)
6. Snyk (<https://snyk.io>)
7. And so many other ones 😊



Demo

Container Vulnerability Scanning

Azure Key Vault Secret Store



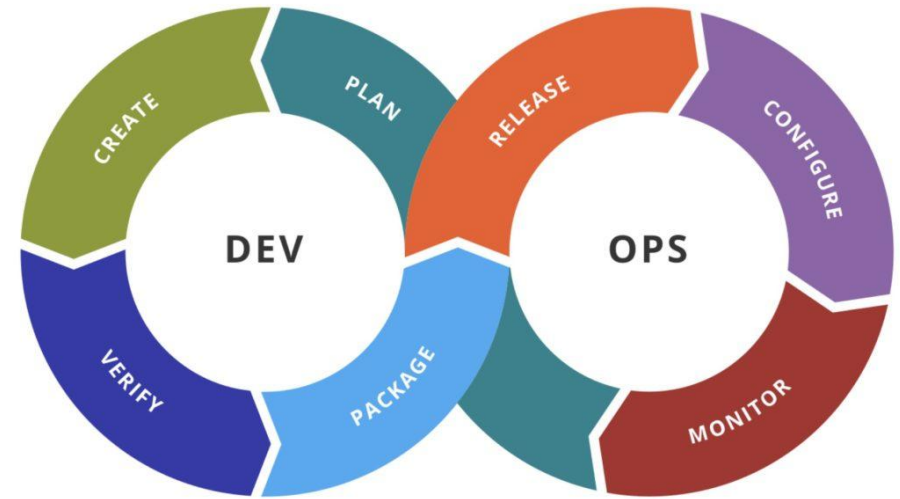
The screenshot shows the Visual Studio Marketplace interface with a search for 'security'. The results are displayed in a grid of 24 items, each with a logo, name, version, and a brief description. The items include:

- Snyk Security Scan
- ADO Security Scanner
- Security Scan
- Container Security
- Security Scan
- Serverless Security
- Hdr Security Integri
- Metasploit Security
- Codified Security
- REST API Static Secu
- AI-R Security Assess
- Beagle Security Test
- azure-novosecure-ai
- SonarQube
- Secure DevOps Kit
- API Management Sc
- Secure Development
- Kiwan FIS Extension
- Alicide Kubernetes A
- OWASP Zed Attack P
- Secure area and Res
- Appknox
- WhiteSource Bolt
- Konduito Vulnerabil
- Veracode
- SD Elements Integri
- Qualys Container Sci
- NeuVector
- Konduito Vulnerabil
- WhiteSource for Azu

Concepts of DevSecOps

Peter's Definition:

*Developing a culture of delivering value to your end users, relying on team collaboration, workload automation and **end-to-end security integration***



What got covered



DEVOPS



SHIFT LEFT
MENTALITY



DEVSECOPS
TOOLING



DEMOS



Q & A

Thank you

petender@microsoft.com

[@pdtit](#)

<http://aka.ms/pdtit>

