DevSecOps

Wie bringe ich den Security Gedanken in meinen DevOps-Prozess?

Yannick Tresch

DMoove Solutions GmbH

yannick.tresch@dmoove.com

Die DMoove

DMoove

DMoove

- Cloud Consulting
- Managed Services
  - DevOps Tools
  - Monitoring
- Kostenoptimierung on AWS
  - Up to 55% savings on EC2
- Partner: AWS, GitLab, Centreon, Microsoft

DMOOVE

Introduction to DevSecOps

DMOOVE

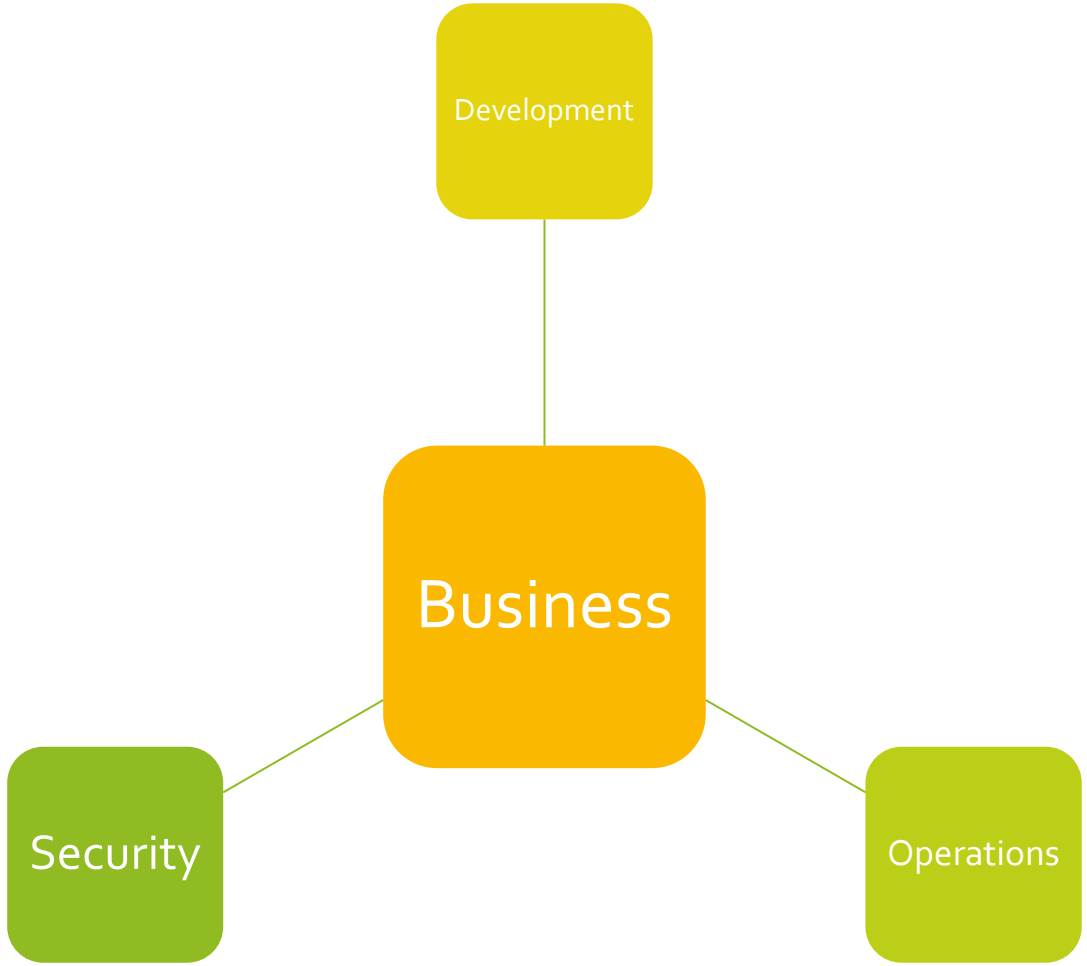
What is DevOps?

Cultural Philosophy

Practices

Tools

Whats important?



DMOOVE

What is DevSecOps?

DevSecOps is

- Team effort, not a single security unit
- Automated and continous security

DevSecOps role

- Not here for code audits
- Implement proccesses to automate code validation and audit of code and atrifacts during CI/CD proccess

So how should we perform DevSecOps?

- Implement security as code
- Keep security in your mind while developing
- Implement iterative solutions and not „the best answer“
- Not only scanners but real attacks on services
  - Learn how to defend
  - Learn how to attack
- Automate defense procedures

Target:
Ensure data security

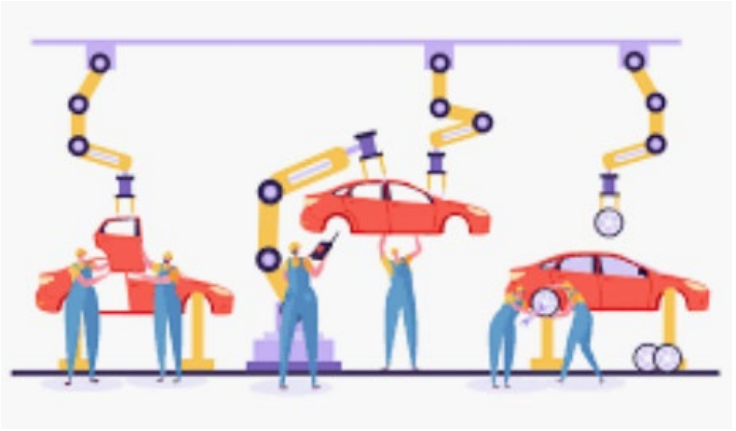
DevSecOps

DMOOVE

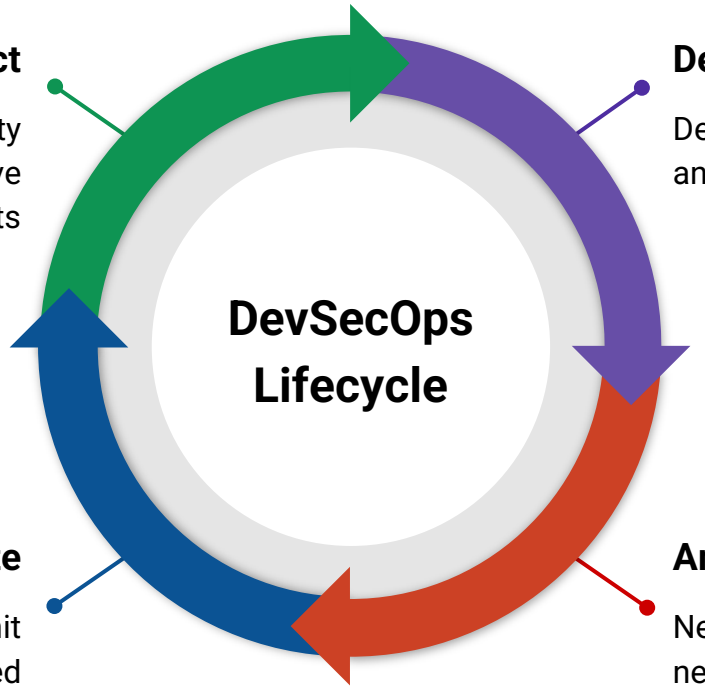
New problems need new solutions

The CI pipeline is your software assembly line. It must be:

- Standardized
- Protected
- Measured
- Inspected



DevSecOps lifecycle



Protect

Detect and defend security attacks within cloud-native environments

Develop

Developers create new features and commit new code

Mitigate

Fix vulnerabilities and submit new commit with fixes included

Analyze

New commits are scanned for new security findings

DMOOVE

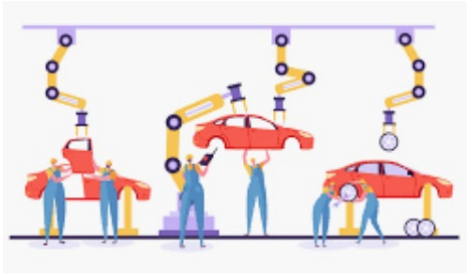
Application Security Testing and Remediation

Shift-left

DMOOVE

Managing vulerabilites

What happens when you find 10k vulnerabilities at the end of the SDLC?



What if you empower Dev to deal with each one at the point where it is introduced?

What means shift-left?

Implementing a successful “shift left” is straightforward; however, steps are often overlooked. Security scans and associated results are:

- Run as early and as often as possible into the development lifecycle
- Built into CI with results showing up within the developer workflow
- Run on the delta code change making results available within minutes
- Easy to understand and include actionable next steps to resolve

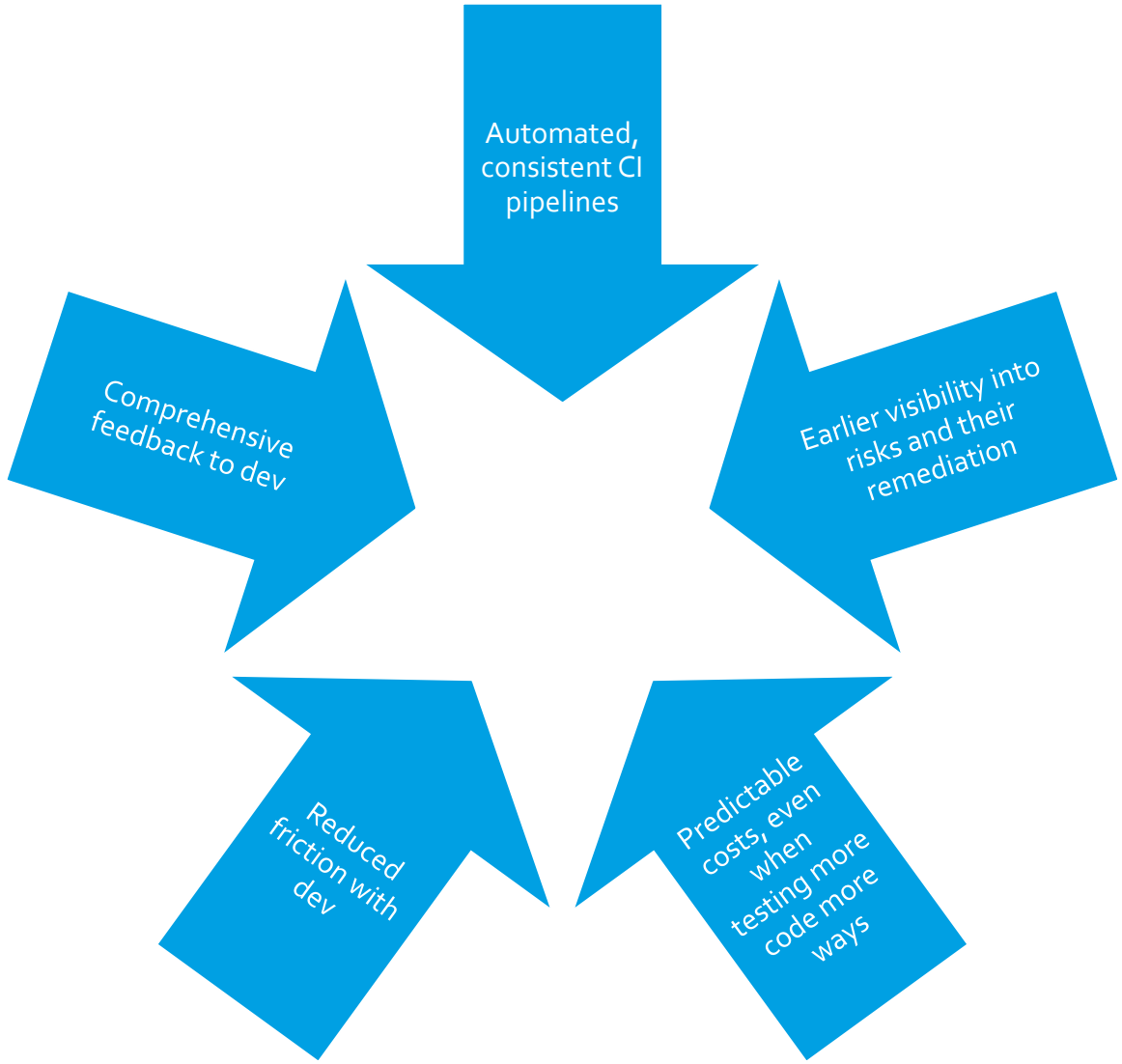
DMOOVE

Advantages for the developer

Contextual	Congruent with DevOps processes	Integrated with DevOps tools	Efficient and automated
• Within CI/CD dev workflow - accountable person • Security dashboard for Security	• Iterative within dev, tests every code change • Immediate cause/effect of code changes	• Create issues • Auto remediation • Production feedback	• Eliminate work wherever possible • No context-switching • Less tracking/triaging and more value-added security

DMOOVE

Advantages for the security engineer



Security Testing

DMOOVE

Tooling for security testing

Static Application Security Testing (SAST)

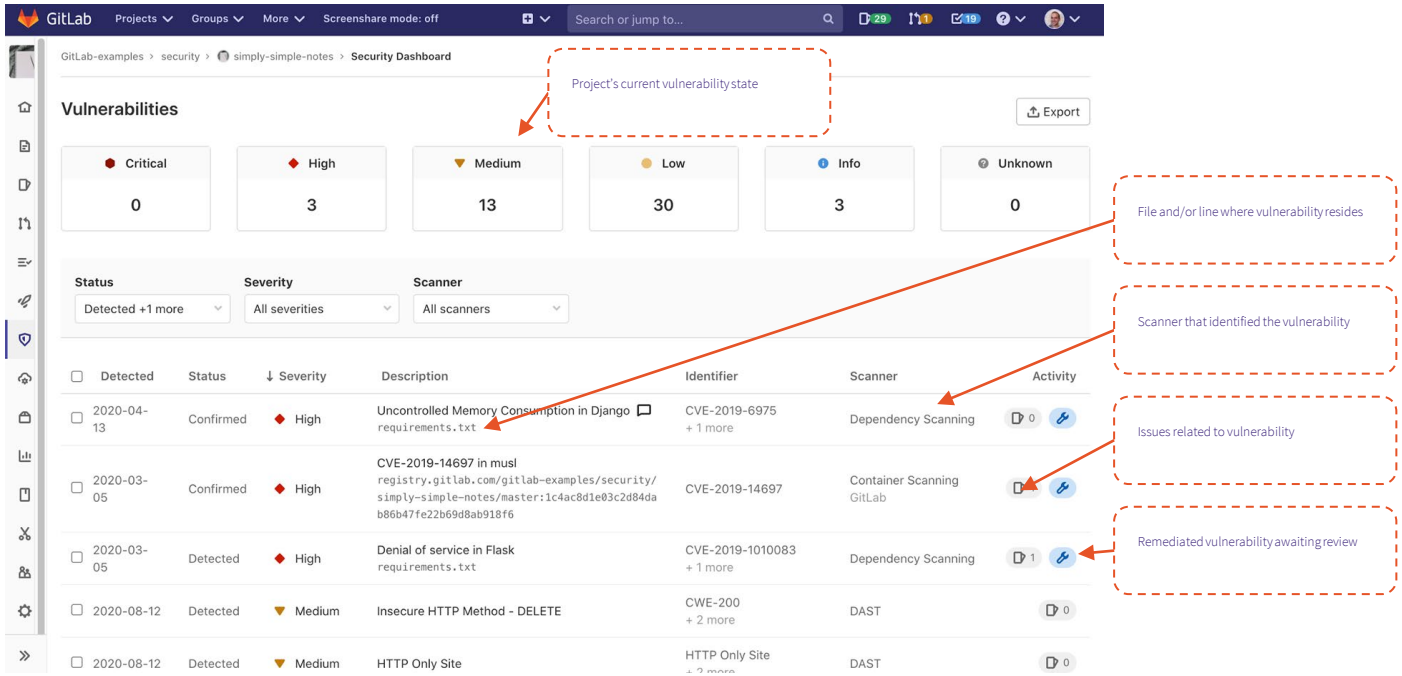
- In SAST, application is tested from inside out.
  - This type testing is a developer's approach of testing.

Dynamic Application Security Testing (DAST)

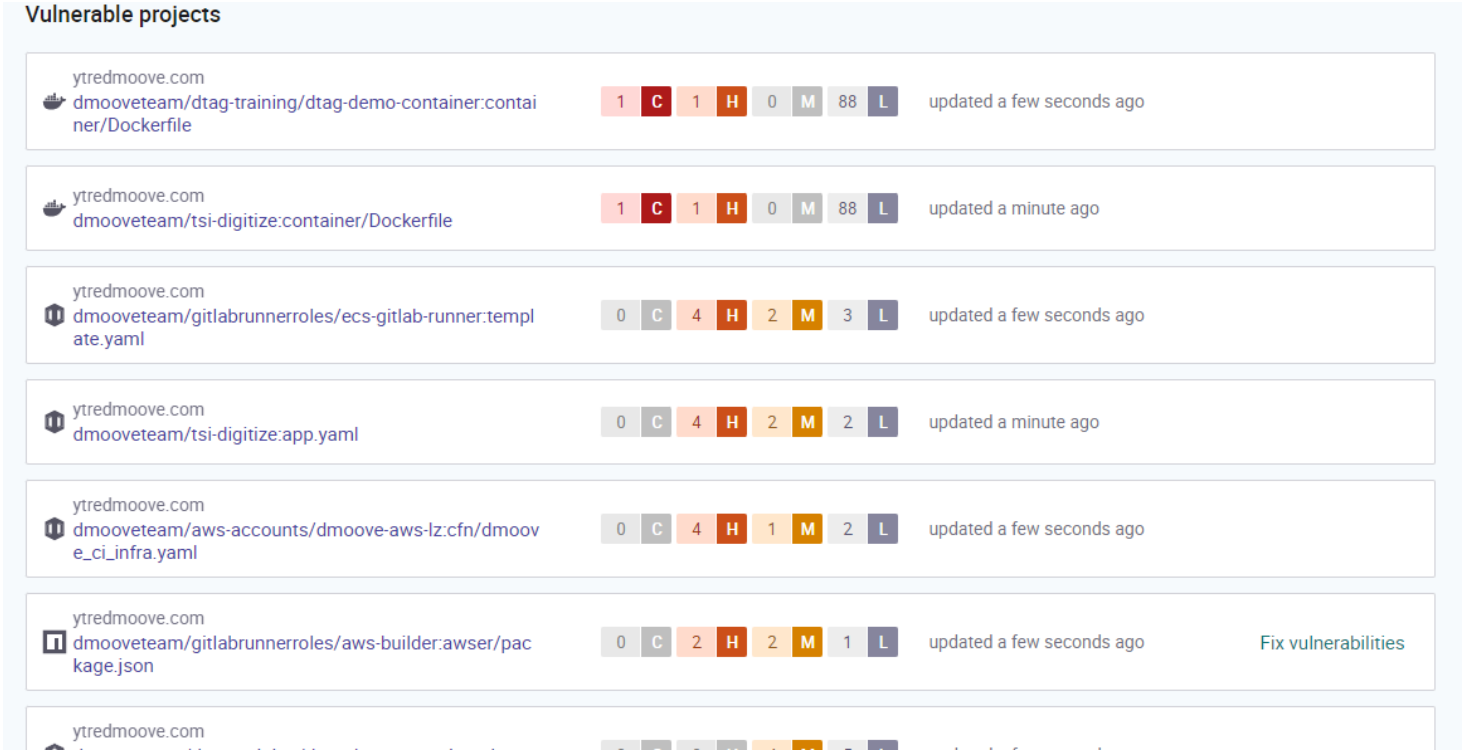
- In DAST, application is tested from outside in.
  - This type testing is a hacker's approach of testing.

Dependency scanners

- Scans source code for dependencies.



Today: Providing increased visibility into security risk



Whitesource Alternative: Snyk

Fragen?

LinkedIn: Yannick Tresch
E-Mail: yannick.tresch@dmoove.com