Best practices for Securing CI/CD Pipelines

or how to get Security right

I am Victoria

Security girl at Microsoft Norway

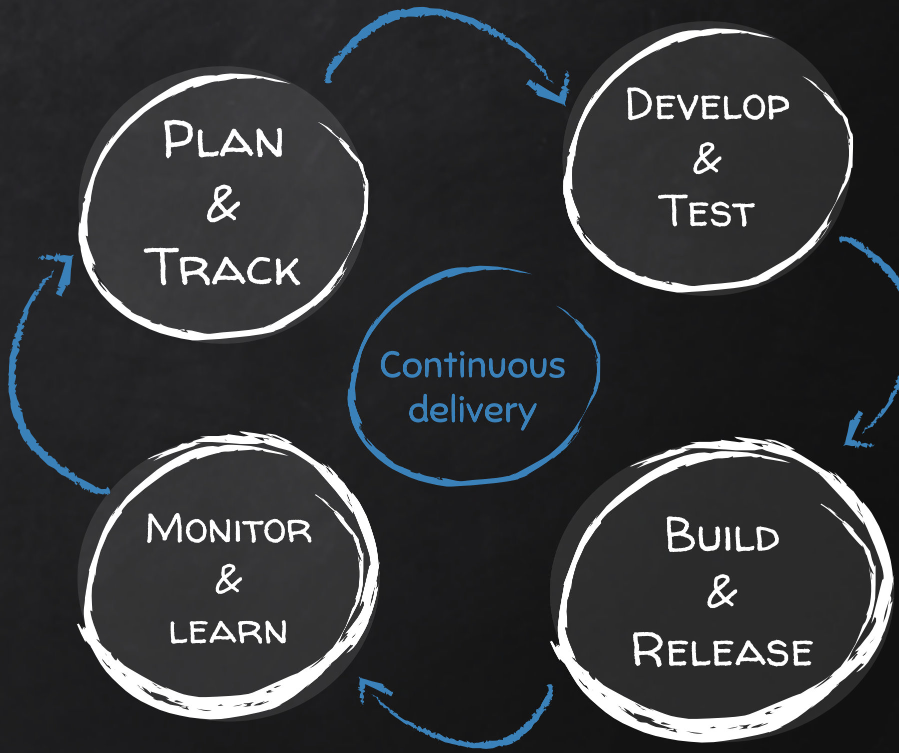
Find me at @texnokot

or victoria.almazova@microsoft.com

100:10:1

DevOps

DevOps is the union of people, process, and technology to enable continuous delivery of value to your end users



Plan & Track

Develop & Test

Build & Release

Monitor & Learn

Continuous delivery

@Microsoft

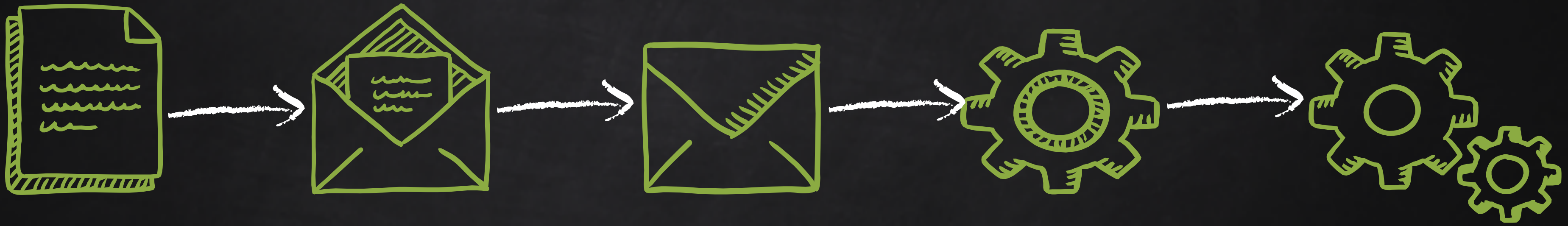
AUTOMATION

Why not to automate security then?

Every breath you take,
every move you make, every bond
you break, every step you take
I'll be watching you

Some security guy named "Sting"

DELIVERING THE PRODUCT



Development

Commit

Acceptance

Production

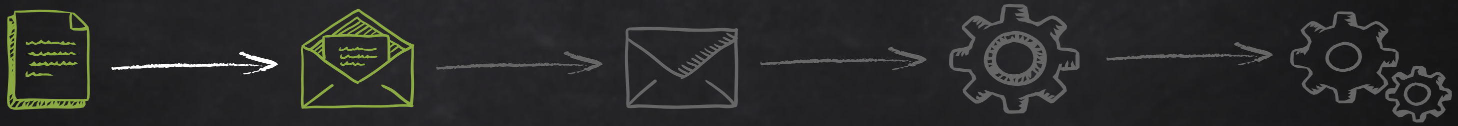
Operations

Development stage

Goal: fix security from the first line of a code

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

Commit stage



Goal: provide fast feedback to developers

- Static code analysis
- Security unit tests
- Dependency management

Acceptance stage

Goal: comprehensive check of the application and infrastructure

- Infrastructure as Code
- Security scanning
- Cloud configuration
- Security acceptance testing

Production stage

Goal: Ensure that setup follows security traditions

- Security smoke tests
- Configuration checks
- Penetration testing

Operations

Goal: continuous security and lessons learned

- Continuous monitoring
- Threat intelligence
- Vulnerability assessment
- Blameless postmortems

...EVERY STEP YOU TAKE... I’LL BE WATCHING YOU

Development

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

Commit

- ✗ Static code analysis
- ✗ Security unit tests
- ✗ Dependency management

Acceptance

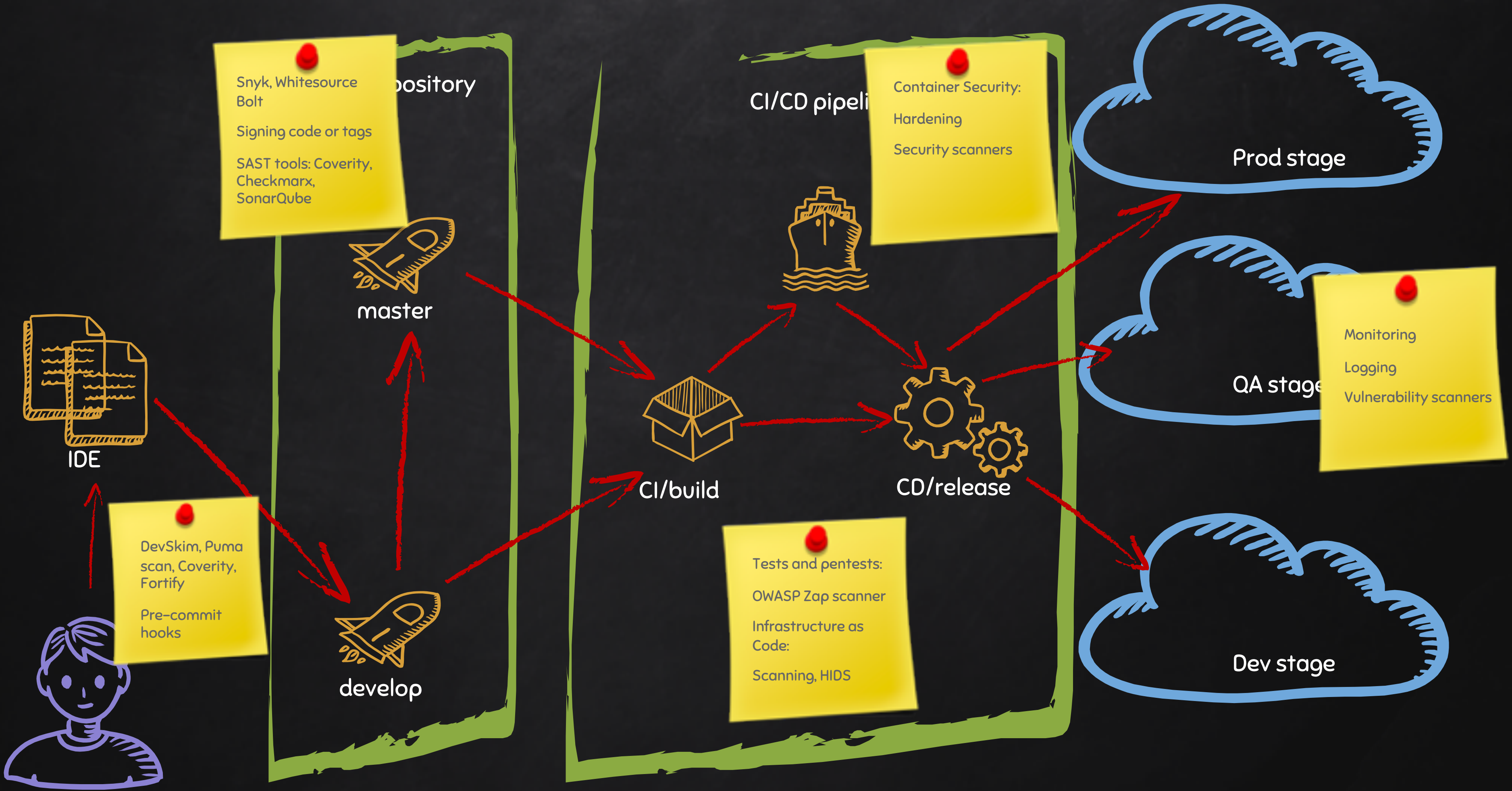
- ✗ IaC
- ✗ Security scanning
- ✗ Cloud configuration
- ✗ Security acceptance testing

Production

- ✗ Security smoke tests
- ✗ Configuration checks
- ✗ Penetration testing

Operations

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



Pre-Commit

Commit (Continuous Integration)

Acceptance (Continuous Delivery)

Production (Continuous Deployment)

Operations

[illegible]

Secure DevOps Toolchain

Building a DevSecOps Program (CALMS)

Culture

[illegible]

Automation

[illegible]

Lean

[illegible]

Measurement

[illegible]

Sharing

[illegible]

Start Your DevOps Metrics Program

[illegible]

First Steps in Automation

[illegible]

SANS AppSec

SANS APPSEC CURRICULUM

[illegible]

SANS

WE DO DEVOPS ALREADY
JUST WITHOUT AGILE, CI, SECURITY, STANDUPS OR ANY OF THAT HIPSTER STUFF
imgflip.com
memes.com

Resources

- SANS poster: https://www.sans.org/security-resources/posters/secure-devops-toolchain-swat-checklist/60/download
- The OWASP Foundation: https://www.owasp.org/index.php/Main_Page
- And me ☺ at github: https://github.com/texnokot/
- And of course twitter: https://twitter.com/texnokot

THANKS!

Any questions?

You can find me at
@texnokot
victoria.almazova@microsoft.com