

May 13th, 2023

#GlobalAzureAthens



Build DevSecOps practices on CI/CD pipelines

Gerasimos Alexiou

Senior DevOps engineer @ thesignalgroup.com

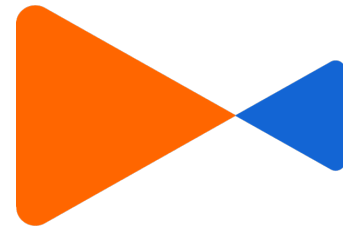
blog.geralexgr.com

linkedin.com/in/geralexgr

Dear Global Azure Athens
2023 sponsors,
your support made all the
difference — **thank you!**



#GlobalAzureAthens



kaizen
GAMING



Microsoft

Info Quest
TECHNOLOGIES



BlueStream
SOLUTIONS



Code.Hub

SIGNAL™

Agenda

- 1) Automation & CI/CD pipelines
- 2) DevSecOps
- 3) Best Practises

Automation & CI/CD

#GlobalAzureAthens



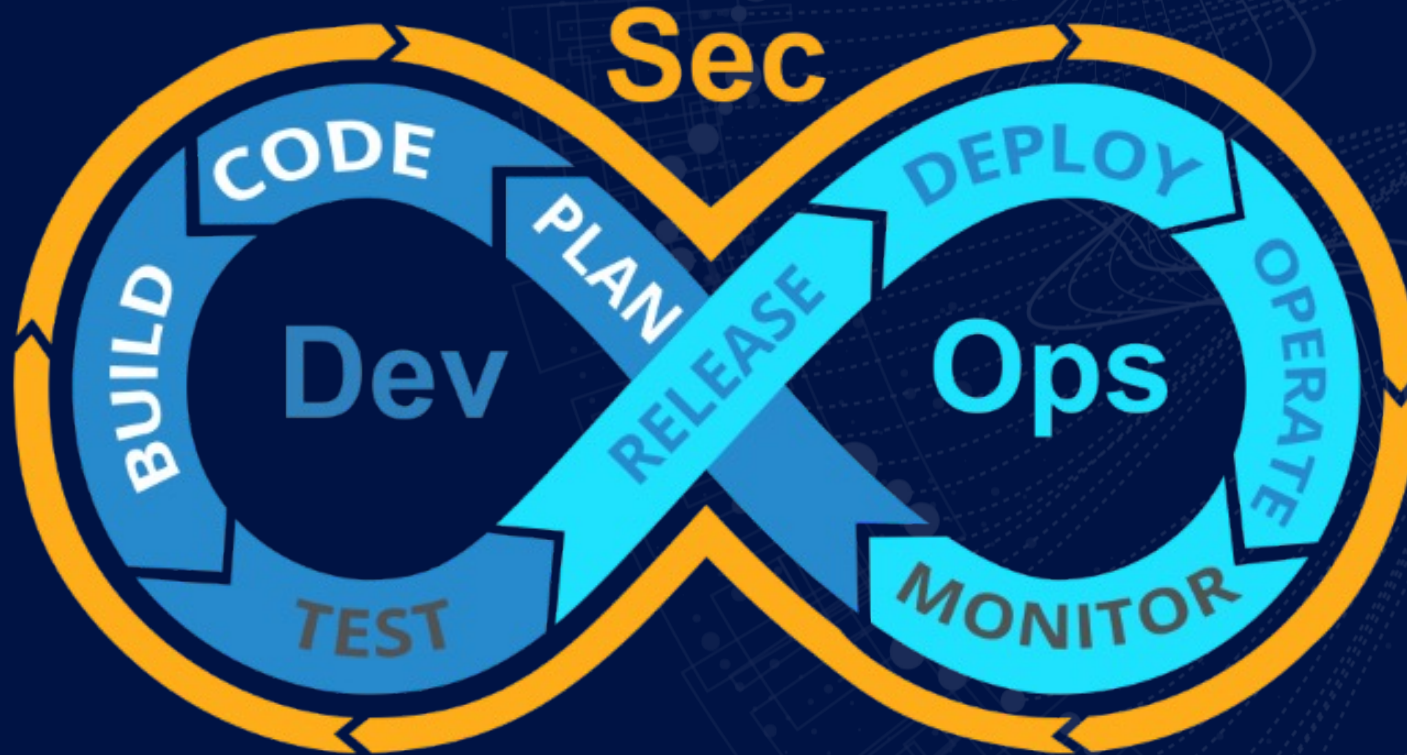
DevOps

Build & Deploy



DevSecOps

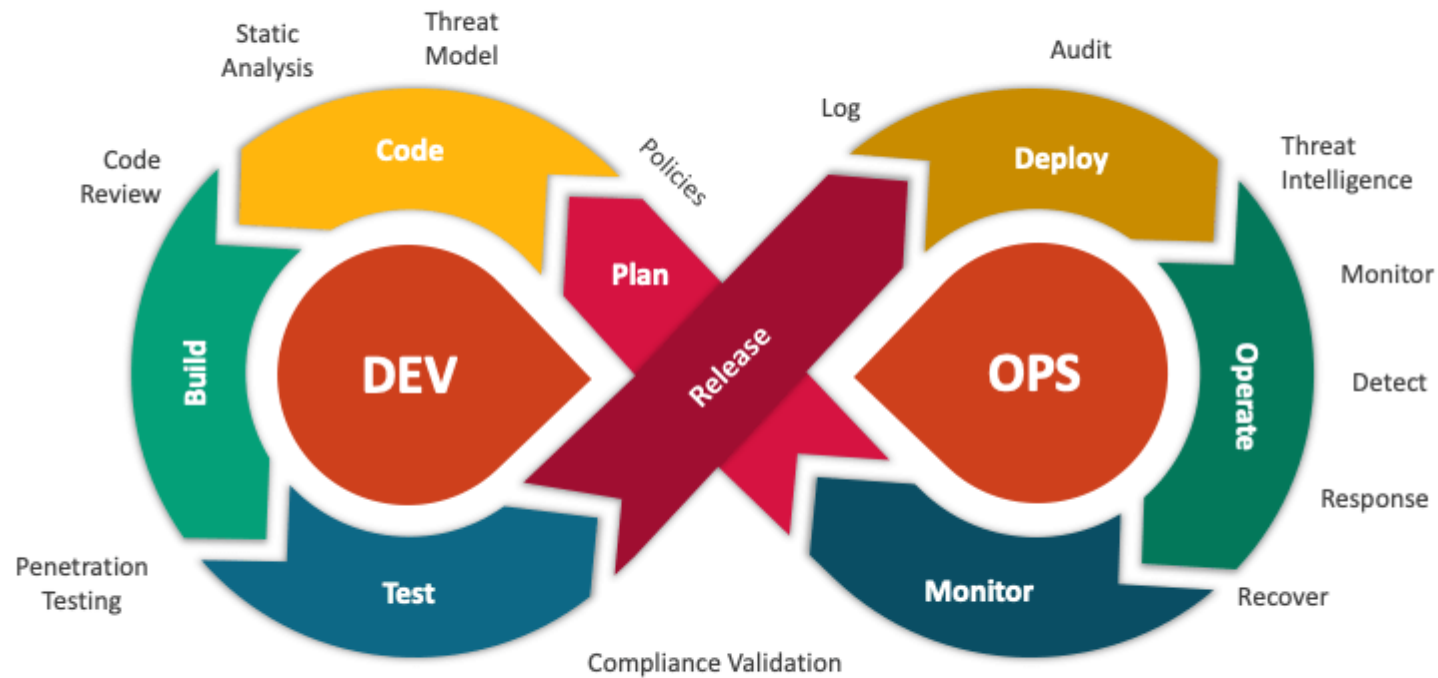
#GlobalAzureAthens



DevSecOps

Security additions

DEVSECOPS



DevSecOps

SecOps (SECURITY OPERATIONS)

Common Roles for your SecOps Team

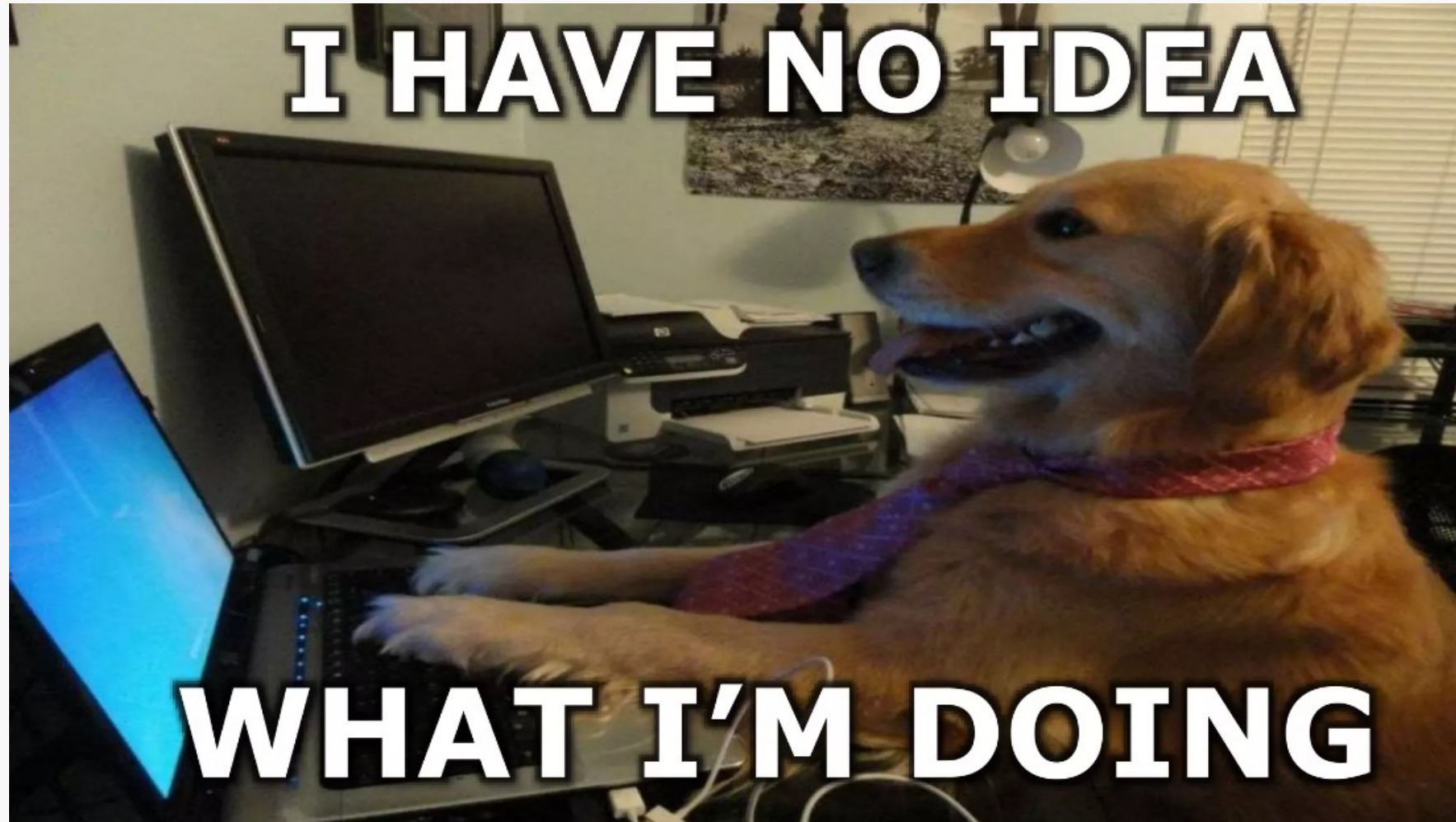


Source: bmc

DevOps



DevOps



DevSecOps



Demo time [devops]

build application → Release env

✓ Build Code

2 jobs completed

22s

✓ Deploy to DEV envi...

2 jobs completed

20s

✓ Deploy to QA envir...

2 jobs completed

20s

✓ Deploy to PROD en...

1 job completed

11s

DevSecOps

#GlobalAzureAthens

DevOps tools + Security practices = DevSecOps

➤ sonarqube scan

Skipped

✅ scan code

1 job completed

32s

➤ Build container image

Skipped

➤ Scan container image

Skipped

➤ Deploy application

Skipped

Demo time [devsecops]

Build application

+

- SonarQube
- Snyk
- Trivy
- Azure DevOps best practises

Release application

Tools

#GlobalAzureAthens

SonarQube → Trivy → Snyk → Production release

Quality Gates result → Code scanning →
Container scanning → Production release

SonarQube

#GlobalAzureAthens

- Code smells
- Bugs
- Vulnerabilities
- Coverage

SonarQube

A Quality Gate is a set of measure-based Boolean conditions. It helps you know immediately whether your project is production-ready. If your current status is not Passed, you'll see which measures caused the problem and the values required to pass.

Trivy

#GlobalAzureAthens

- OS packages and software dependencies in use (SBOM)
- Known vulnerabilities (CVEs)
- IaC issues and misconfigurations
- Sensitive information and secrets
- Software licenses

Snyk

#GlobalAzureAthens

- Unified Policy Engine
- IaC security
- Container security
- Compliance automation

Azure DevOps

- Agents topology
- Variables & Secrets
- Isolation (projects, pipelines)

≈

Demo time

#GlobalAzureAthens

Projects/AspNetWebApi
Globalazure-devsecops.yml

<https://github.com/geralexgr/ado-course/tree/globalazuregreece-2023>



#GlobalAzure

Recap

- DevOps & DevSecOps
- Tools
- Mindset

Questions?



Please evaluate !



A big **thank you** to our
sponsors!



Microsoft

InfoQuest
TECHNOLOGIES



BlueStream
SOLUTIONS



Code.Hub

SIGNAL

<https://bit.ly/GA23Evaluation>

#GlobalAzureAthens