consorzio interuniversitario nazionale per l'informatica

SESAR LAB

ITA DATA 2024

Assurance in DevSecOps Pipelines

Alex Della Bruna, Marco Anisetti, Giandonato Inverso

19th September 2024

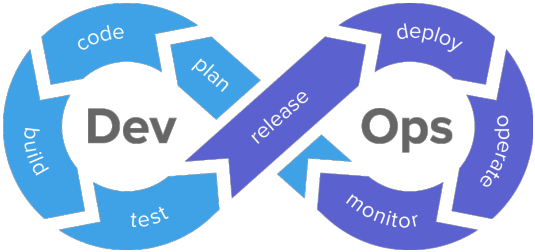
UNIVERSITÀ DEGLI STUDI DI MILANO

DevOps Pipelines

A classic DevOps pipeline commonly consists of three main stages

- Upload ⟶ developer pushes code updates
- Build and test ⟶ CI/CD pipeline builds and tests the code
- Deployment ⟶ code is deployed to the operation environment

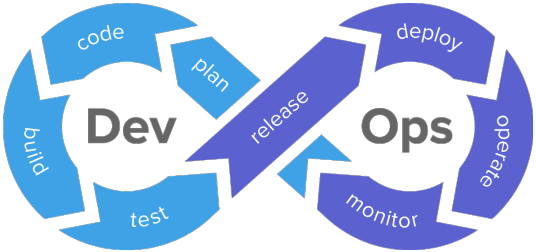
⟶ great for traditional development lifecycles



DevOps Pipelines

A classic DevOps pipeline commonly consists of three main stages

- Upload ⟶ developer pushes code updates
- Build and test ⟶ CI/CD pipeline builds and tests the code
- Deployment ⟶ code is deployed to the operation environment

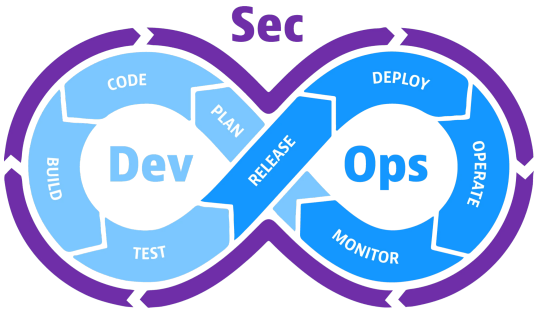


⟶ great for traditional development lifecycles, but it does not take into account security

DevSecOps Pipelines

A DevSecOps pipeline adds security capabilities to the traditional DevOps pipeline

- Static code analysis ⟶ code is scanned for vulnerabilities
- Composition analysis ⟶ software components are scanned for vulnerabilities
- Dynamic testing ⟶ application is executed under simulated attacks

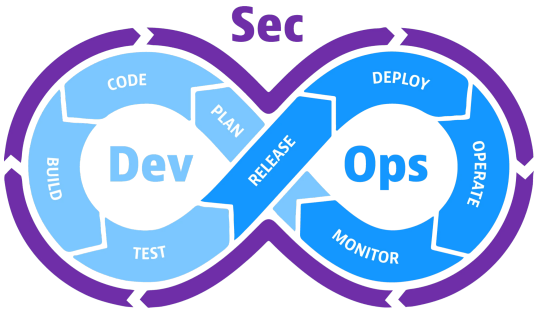


⟶ security is integrated into the development lifecycle

DevSecOps Pipelines

A DevSecOps pipeline adds security capabilities to the traditional DevOps pipeline

- Static code analysis ⟶ code is scanned for vulnerabilities
- Composition analysis ⟶ software components are scanned for vulnerabilities
- Dynamic testing ⟶ application is executed under simulated attacks



⟶ security is integrated into the development lifecycle, but is it enough?

What If...

What if the operation environment...

- is vulnerable?
- is not the same as the one used for testing ?
- becomes vulnerable after the deployment?

⟶ DevSecOps pipelines are great, but they do not consider the real-world environment

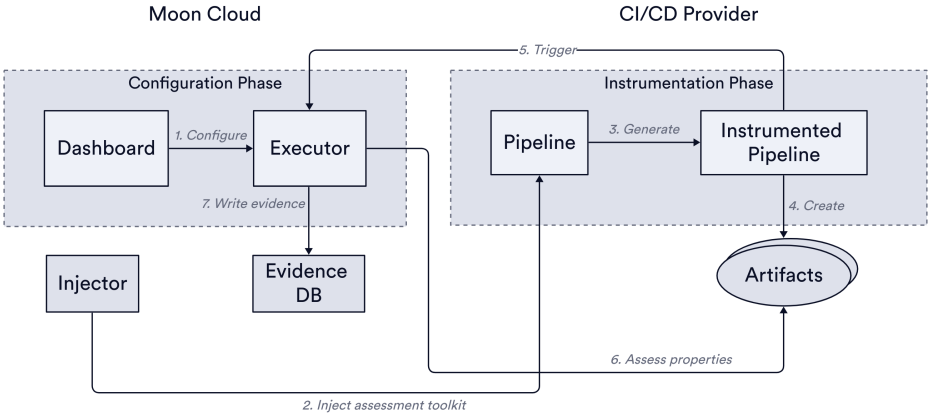
⟶ **Assurance in DevSecOps pipelines**

Assurance

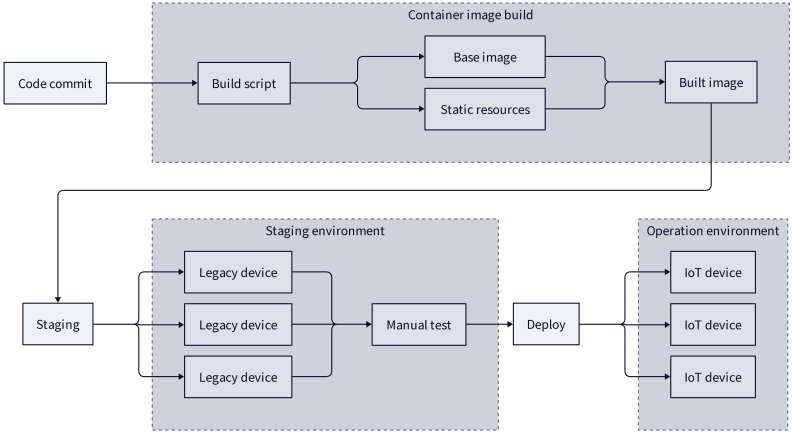
"Security assurance is the process of asserting non-functional properties of a system to ensure that it meets the given non-functional requirements over time"

C. A. Ardagna and N. Bena. *"Non-Functional Certification of Modern Distributed Systems: A Research Manifesto".* ***In: Proc. of IEEE SSE 2023. Chicago, IL, USA, July 2023***

Assurance in DevSecOps Pipelines

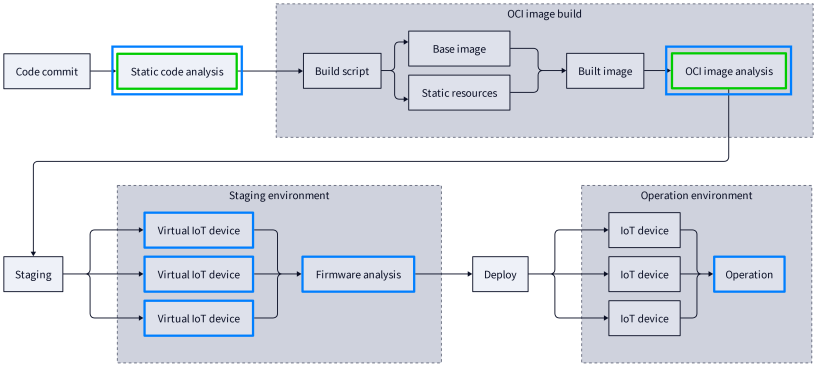


Cloud-Edge-IoT Scenario - From DevOps...



Cloud-Edge-IoT Scenario - ... To Assurance DevSecOps

DevSecOps Assurance DevSecOps



Conclusions

Assurance takes DevSecOps to the next level bridging the gap between development and compliance

- Compliance-focused traceability of security events
- High modularity by decoupling between the pipeline and the assurance platform

Future work

- Deeper integration with the assurance platform
- Extension to other development approaches

Assurance in DevSecOps Pipelines

Thank you for listening!
Any questions?

Alex Della Bruna: alex.dellabruna@studenti.unimi.it
Marco Anisetti: marco.anisetti@unimi.it
Giandonato Inverso: giandonato.inverso@studenti.unimi.it