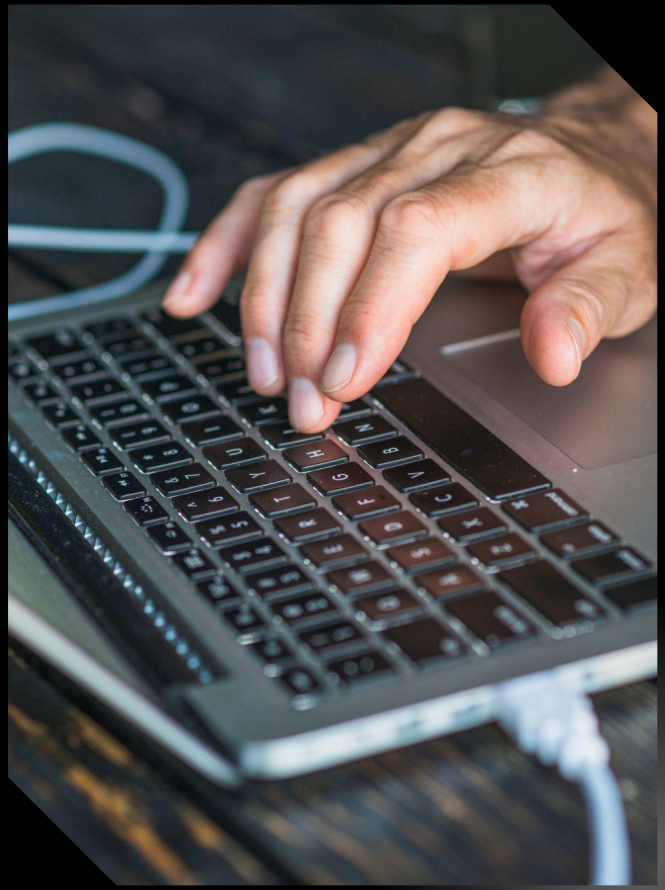
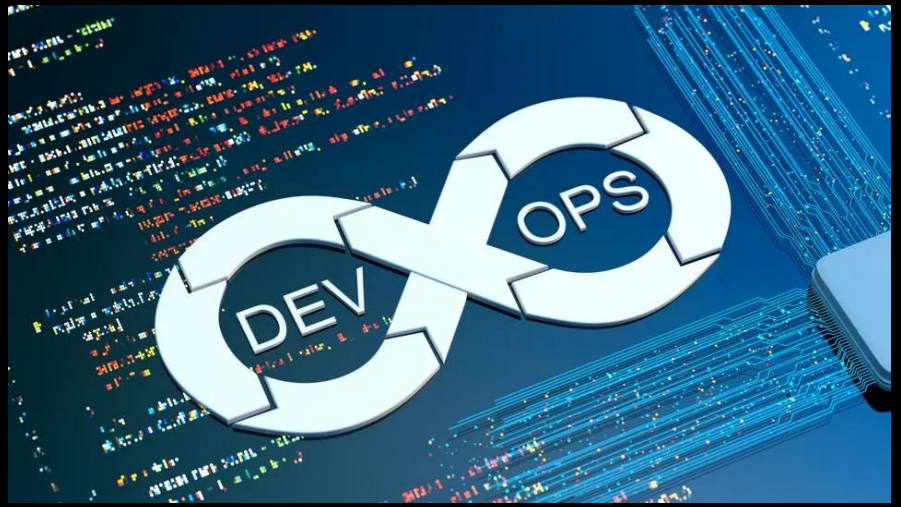


DevSecOps: Bridging DevOps and Security

By Djelloul Bouida

DevOps!

DevOps is the direct descendant of agile software development



DevOps!

DevOps is a combination of software development (dev) and operations (ops).

It is defined as a software engineering methodology .....

DevOps!

Focus: Speed and agility in development and operations.

Security: Often handled separately at the end of the development cycle.

Issues: Late-stage security issues can cause delays and higher costs.

Devops

Dev

Plan
Develop

Dev

Build
Test
Release

Ops

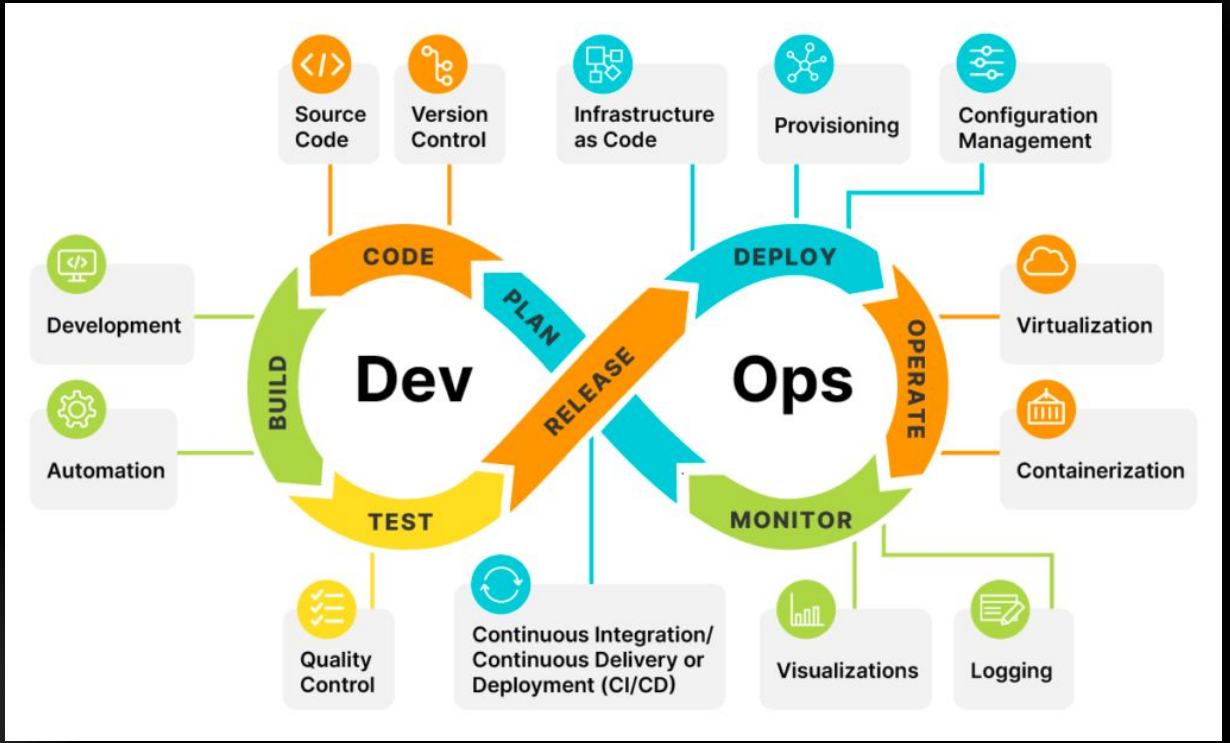
Deliver
Deploy
Operate

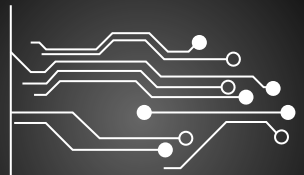
Ops

Monitor
Feedback



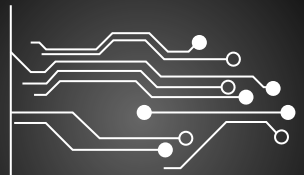

Devops


Source Code
Version Control
Infrastructure as Code
Provisioning
Configuration Management
CODE
PLAN
DEPLOY
Development
Automation
BUILD
Dev
RELEASE
Ops
OPERATE
Virtualization
Containerization
TEST
MONITOR
Quality Control
Continuous Integration/ Continuous Delivery or Deployment (CI/CD)
Visualizations
Logging



DevSecops

stands for **development**, **security**, and **operations**.
It's an approach to culture, automation, and platform design that integrates security as a shared responsibility throughout the entire IT lifecycle.



DevSecops

Add a **security** layer to the Devops approach

DevSecops

Focus: Speed and agility in development and operations

Focus: Integrates security from the beginning and throughout the lifecycle.

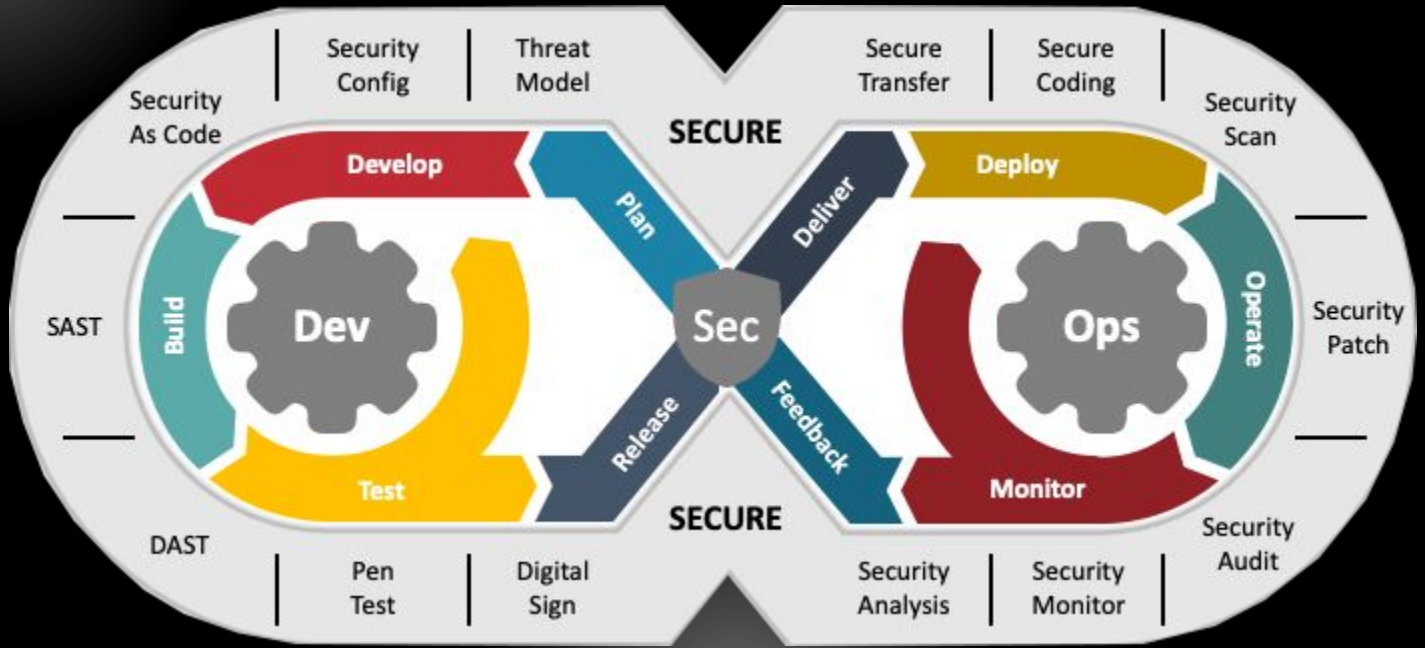
Security: Often handled separately at the end of the development cycle.

Security: Continuous and automated, part of every stage from planning to deployment.

Issues: Late-stage security issues can cause delays and higher costs.

Benefits: Early detection and resolution of security issues, smoother and faster development cycles.

DevSecops

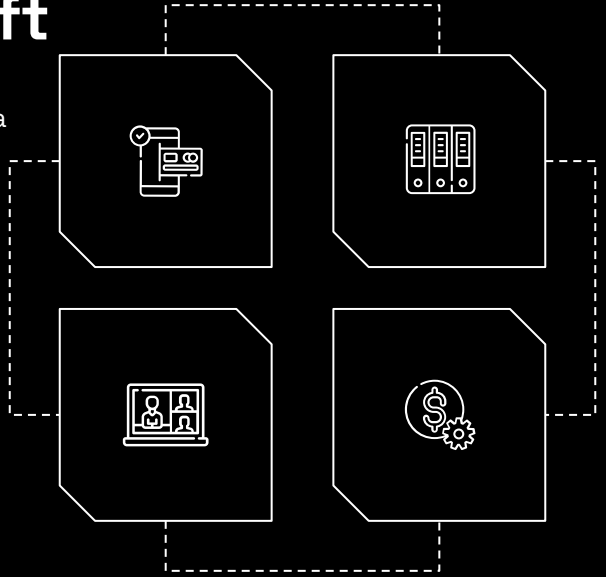

Security As Code
Security Config
Threat Model
SECURE
Secure Transfer
Secure Coding
Security Scan
Develop
Plan
Deliver
Deploy
SAST
Build
Dev
Sec
Ops
Operate
Security Patch
Test
Release
Feedback
Monitor
SECURE
DAST
Pen Test
Digital Sign
Security Analysis
Security Monitor
Security Audit

Challenges in Adopting DevSecOps

Cultural Shift

Need for development and operations teams to adopt a security-first mindset.

Overcoming resistance to change.



Training and Skill Development

Continuous education and training programs to keep teams updated on the latest security practices and tools.

Tool Integration

Ensuring compatibility and seamless integration with existing tools and workflows

Core Practices of DevSecOps

Security as Code

Writing security policies as code to automate security testing and enforcement.
Example tools: **Terraform, Ansible**.

Continuous Monitoring

Implementing real-time monitoring for threats and vulnerabilities.
Example tools: **Prometheus, Grafana.**

Collaboration and Communication:

Encouraging cross-functional teams to work together, ensuring security considerations are included in all stages.
Using platforms like **Slack**

Implementation Strategies

Start Small

Begin with pilot projects to test and refine DevSecOps practices.
Example: Implement automated security testing in a small, non-critical project.

Automate Security Processes

Integrate security tools into the CI/CD pipeline to automate testing and compliance.
Example tools: Tekton, Jenkins, GitLab CI/CD, CircleCI.

Educate and Train

Conduct regular training sessions and workshops to keep teams up-to-date with the latest security threats and mitigation strategies.
Encourage certification programs for team members.

Tools and Technologies

Security Testing Tools

Static Code Analysis: **SonarQube, Checkmarx.**
Dynamic Analysis: **OWASP ZAP, Burp Suite.**
Dependency Scanning: **Snyk, Black Duck.**

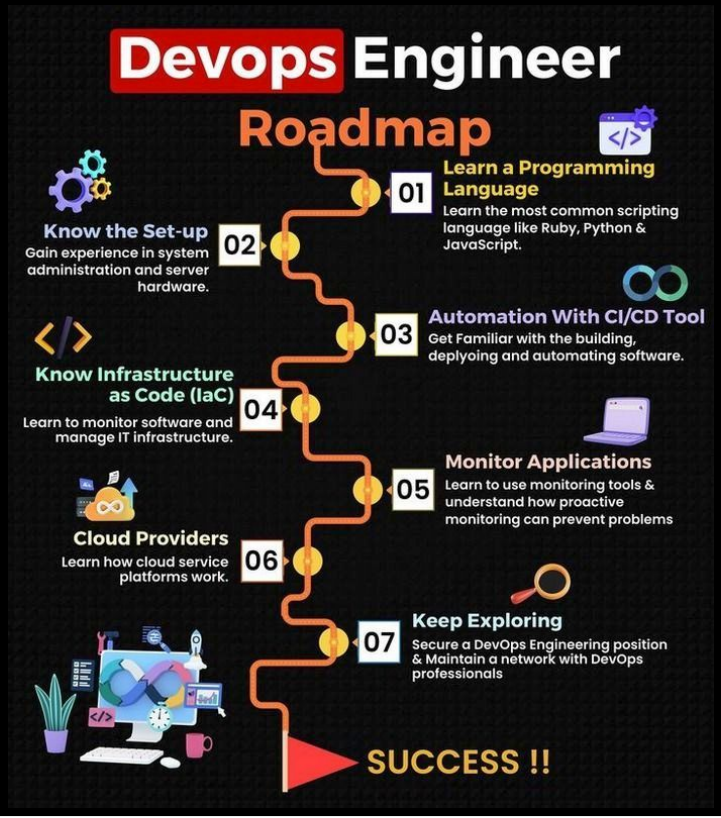
CI/CD Integration

Tools to integrate security testing into CI/CD pipelines.
Example tools: **Tekton, Jenkins, GitLab CI/CD, CircleCI.**

Monitoring and Logging

Tools for continuous monitoring and logging to detect and respond to security incidents.
Examples: **ELK Stack (Elasticsearch, Logstash, Kibana), Splunk, Prometheus, Loki Stack.**

DevOps Roadmap



DevSecOps Roadmap

DevOps Roadmap +++

Get Acquainted with Key Security Concepts

Familiarize yourself with security fundamentals: **risk management**, **threat modeling**, **security architectures**.

Hands-On Security Tooling

Delve into tools like static application security testing **(SAST)**, dynamic application security testing **(DAST)**, and container security solutions. Knowing how to integrate these into CI/CD pipelines is crucial.


ANY
QUESTIONS?

https://www.linkedin.com/in/bouida

bouida@hdconsulting-dz.com