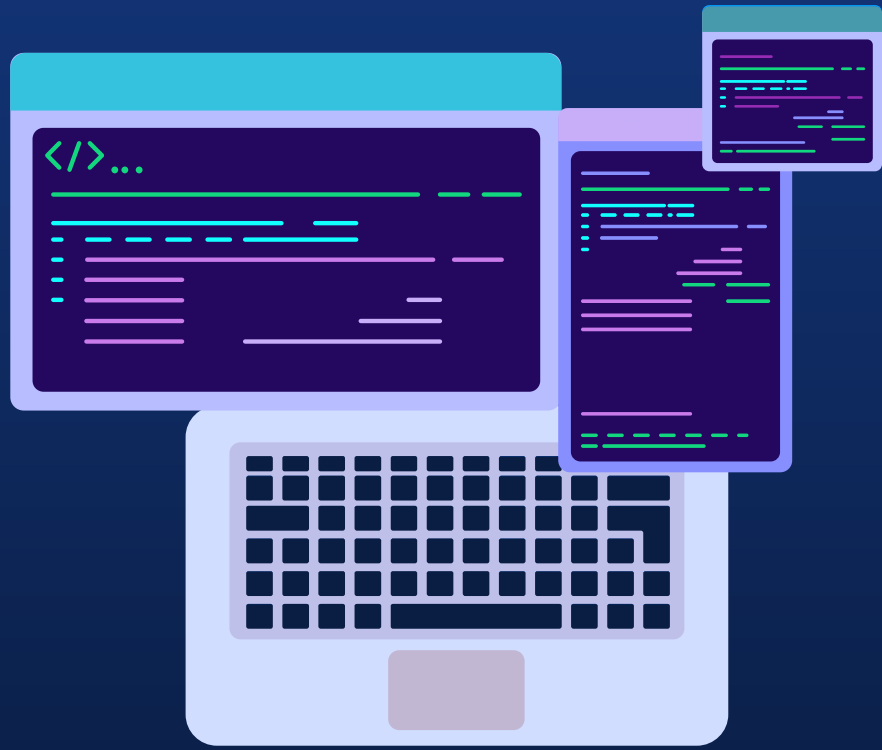
DevSecOps

Session asynchrone

INFO5 - Leila Michelard



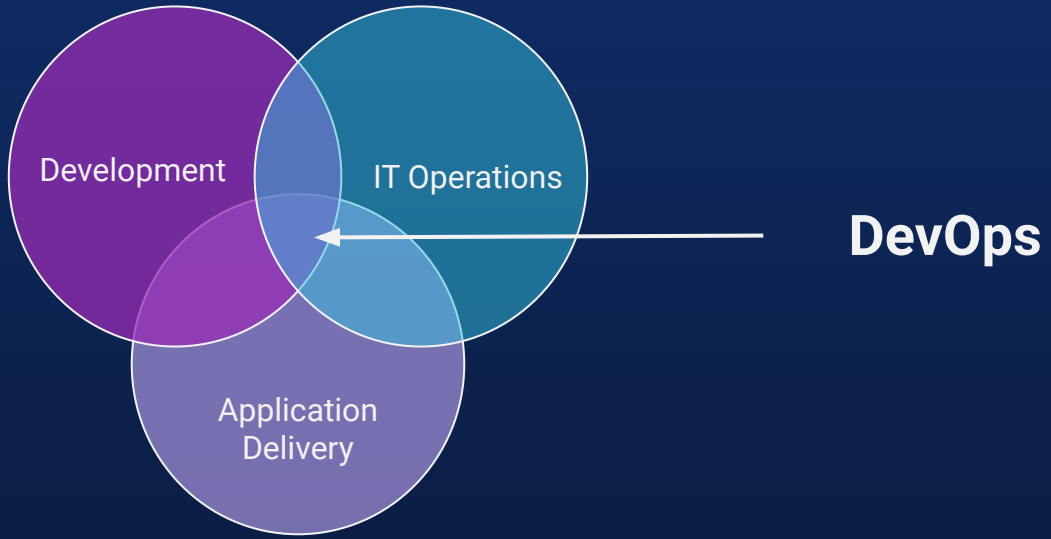
Sommaire

01

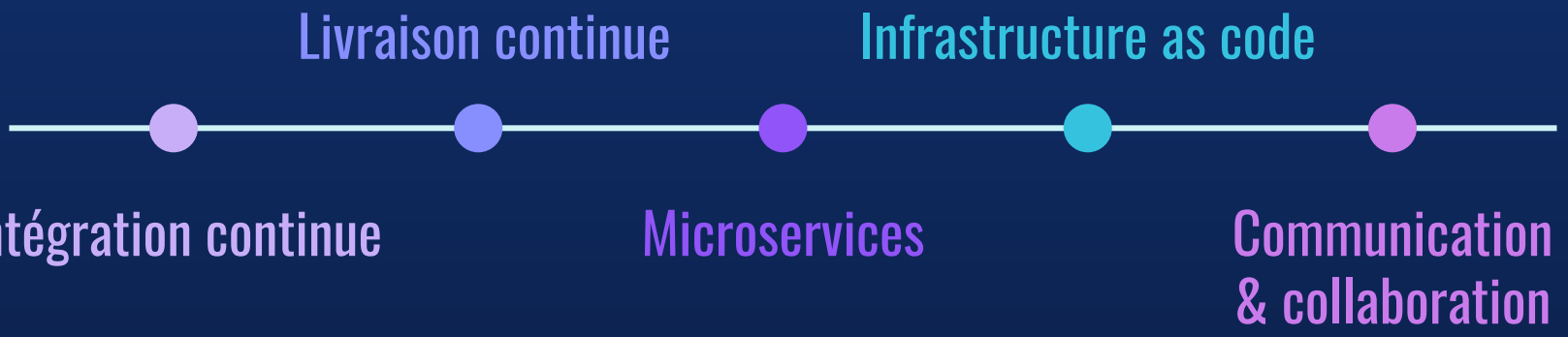
DevOps, qu’est ce que c’est ?

DevOps, c’est quoi ?

Méthode Agile qui vise à unifier le développement logiciel (Dev) et l’administration de système et d’architecture (Ops)



La Pratique DevOps



Avantages et inconvénients de DevOps

Rapidité

Livraison rapide

Fiabilité

Évolutivité

Collaboration améliorée

Nouvelle méthode

02

Et la sécurité dans tout ça ?

Et la sécurité ?

Cyberattaques

Complicité interne (hameçonnage)

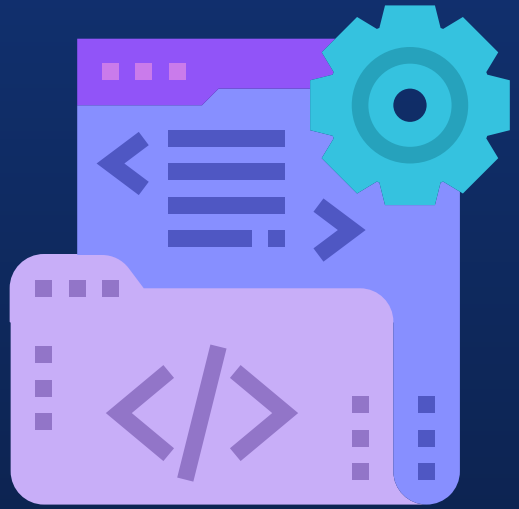
Ajouter une étape *sécurité* ?

Oui mais réduit à néant les avantages du DevOps

DevSecOps

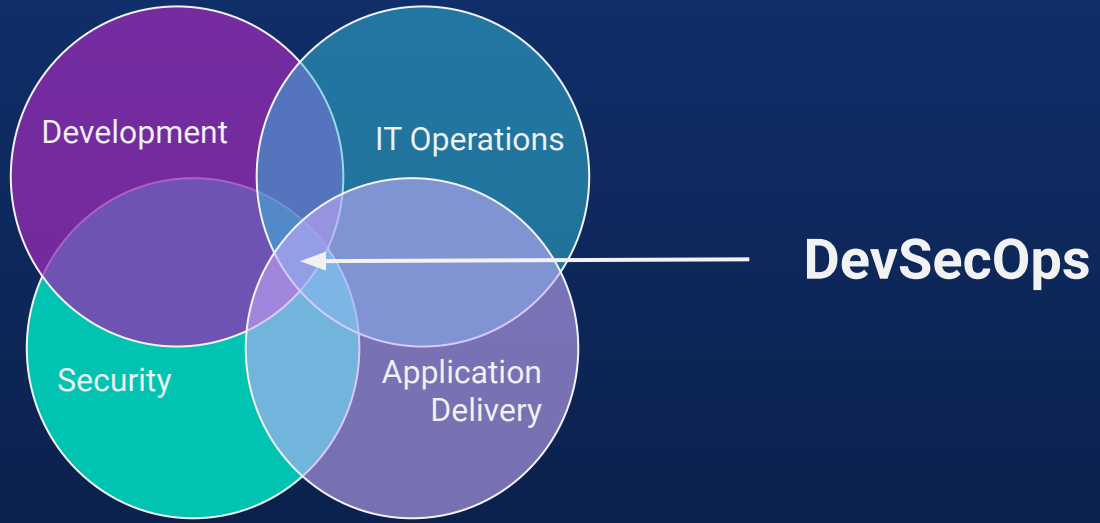
03

DevSecOps



DevSecOps

Approche DevOps dans laquelle la sécurité est prise en compte tout au long du projet



En plus de sécuriser les applications, cette méthode permet de maîtriser le coût des projets

04

Différents outils

Il existe énormément d'outils

Catégorie	Mesure	Outils (au choix)	Existant	P1 - Initialement prévu	P2 - via secureCodeBox	P3
Infrastructure	Utilisation de repository	• Nexus Repository Manager Jfrog Arifactory Docker Trusted Registry		✓		
	Utilisation de l'APIM	• AxWay	✓			
	Utilisation de l'AM	• AxWay Gravitee AM Keyloak	✓			
Build et Run	Scan de code statique	• Kiuwan (sécurité du code) SonarQube (qualité du code)	✓			
	Scan de conformité (durcissement)	• Ansible Salt				✓
	Scan de durcissement	• Lynis				
	Scan API	• Tinfoil API (compatible OpenAPI)				
	Scan applicatif	• ZAP ZAP API Arachni			✓	
	Scan de vulnérabilité	• Google Security Scanner				
	Scan d'image	• Google Security Scanner • Tenable.io Container Security • Clair • Docker Dive • Docker Trusted Registry		✓		
	Scan réseau	• Nmap			✓	
	Scan SSL	• SSLyze			✓	
	Tests de performances	• Artillery Gatling	✓			
Tests externes	Test d'intrusion	• NA				
	Bug Bounty	• NA				
Exploitation	Supervision API	• Prometheus & Grafana		✓		
	Analyse sécurité des journaux	• ELK				

Secure Coding

- SAST : Audit de code source automatisé (Static Application Security Testing)
- DAST : Audit dynamique automatisé (Dynamic Application Security Testing)
- Test d'intrusion réalisé par un hacker "éthique"

05

Démonstration

CodeQL : Analyse de code sémantique créé par Github

Merci pour votre écoute !