CLOUD TEMPLE
Innovative by design

LA SÉCURITÉ AU CŒUR DE LA CULTURE DEVOPS

17/09/2020

M. DAVY ADAM

M. GIULANO IPPOLITI

INTERVENANTS

Davy ADAM

Architecte Cloud Public
Et Hybride

Giulianio IPPOLITI

Directeur Grand Ouest, RSSI et DPO chez
Cloud Temple

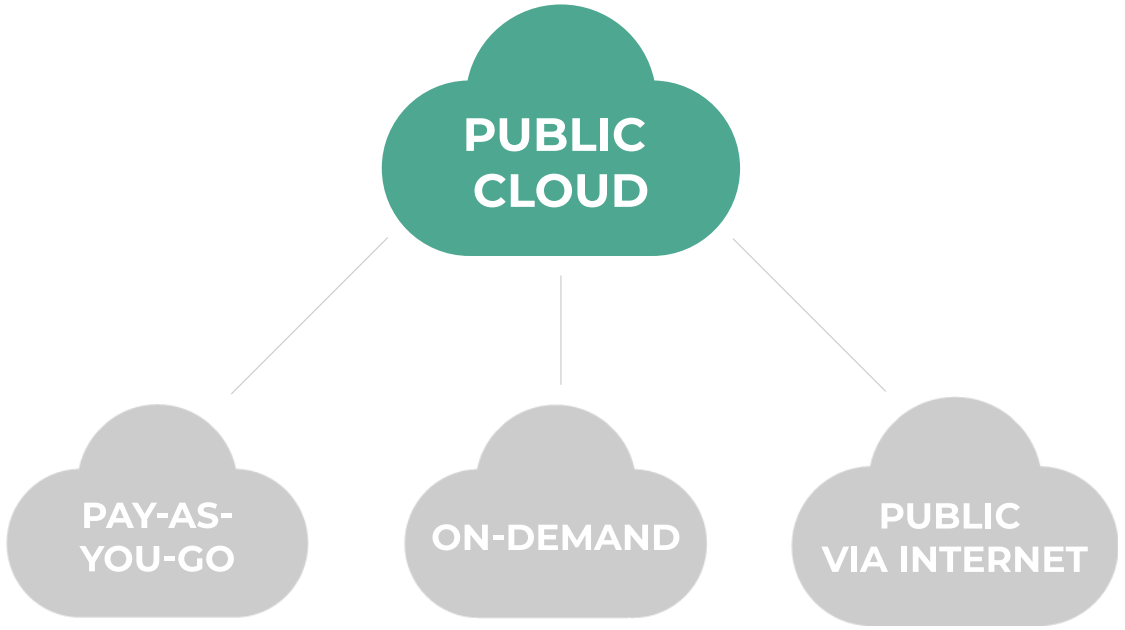
CLOUD TEMPLE
Innovative by design

INTRODUCTION À DEVSECOPS

M. DAVY ADAM

LE CLOUD

Qu’est-ce que c’est ?



LE MIRAGE CLOUD

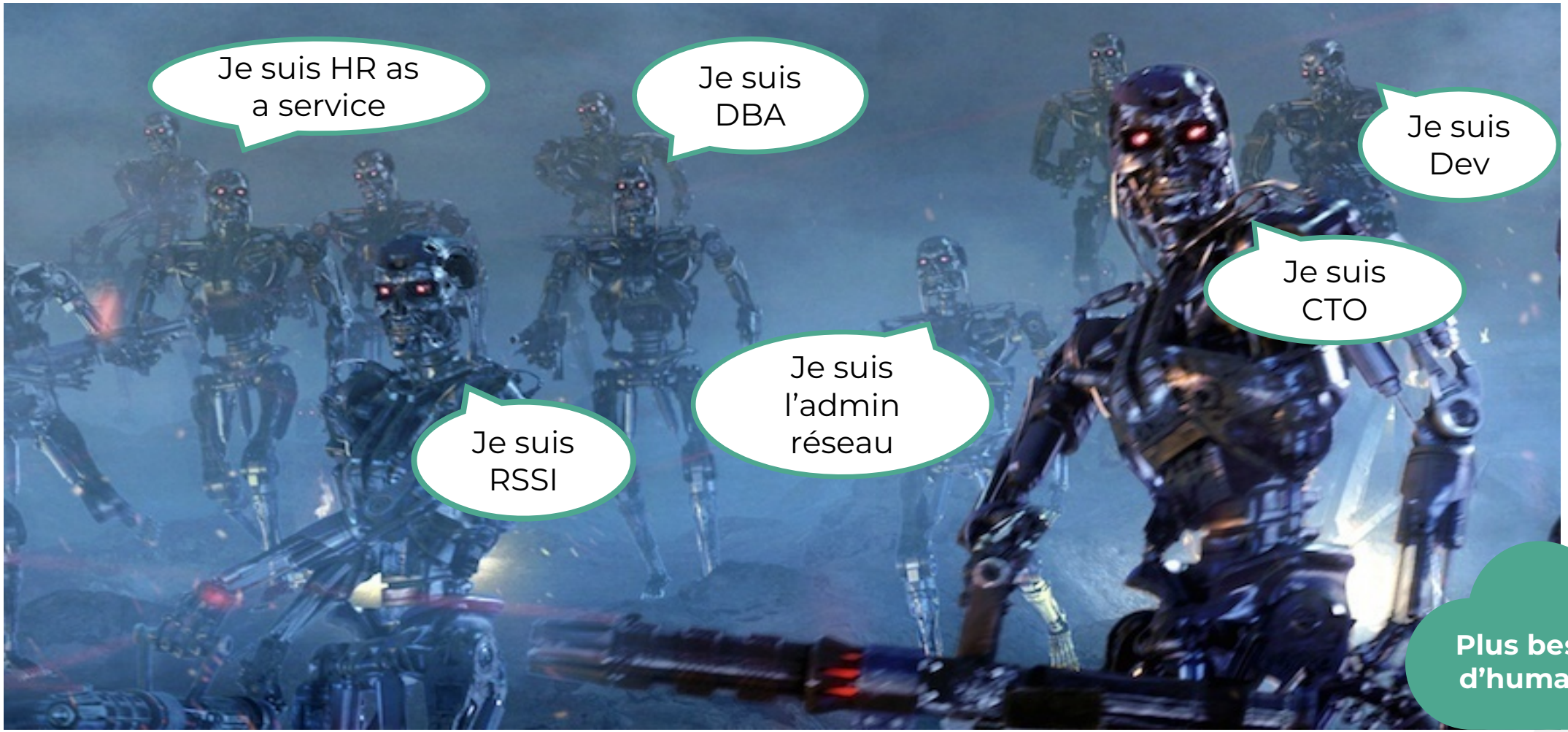
In cloud we trust !

Le cloud public est :

- Hautement disponible
- Scalable (élastique)
- Redondant
- Automatisé
- Monitoré
- « Serverless »
- Chiffré
- Sauvegardé

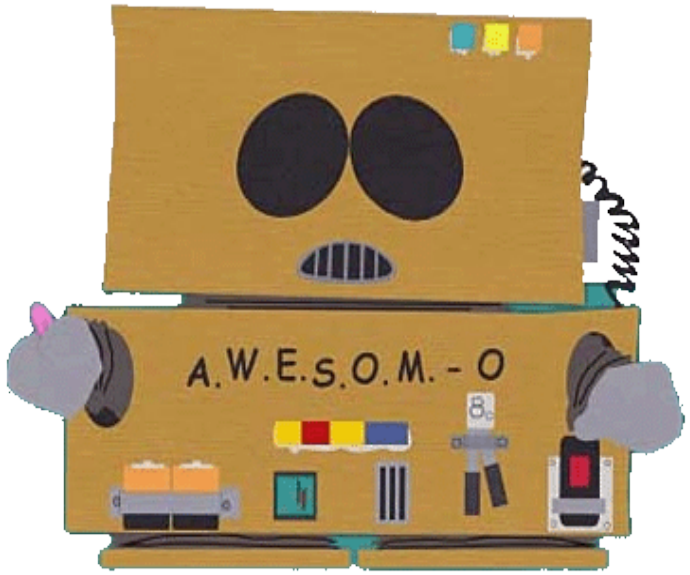
- La raison pour laquelle je n'ai plus de travail
- Conscient
- Sarah Connor ?
- …

LES PEURS DU CLOUD



LA RÉALITÉ

Je suis...



Juste humain...

PILOTER LE CLOUD

Le cloud public fournis différents services et options :

- Le niveau de haute disponibilité
- Le niveau d'adaptation et de mise à l'échelle
- La redondance des infrastructures et parfois des services
- L'automatisation
- Des collections de métrique et des services de supervision pour aider à controler mes applications et leurs infrastructures
- Des services **« serverless »**
- Le chiffrement des données en mouvement et au repos pour pouvoir instaurer le niveau de sécurité que l'on souhaite
- Sauvegarder mes données
- La raison pour laquelle j'ai un nouveau travail !

LES 6 BÉNÉFICES DU CLOUD

Passer du modèle CAPEX/OPEX en un tout OPEX

Plus de coût d'investissement initial en matériel. Uniquement une gestion de coût d'exploitation.

Arrêter de dépenser pour des datacenters

Economie de coût sur les investissements matériels.

Augmenter l'agilité et la rapidité

Profiter du modèle à la demande pour permettre d'atteindre l'agilité voulue en utilisant des ressources seulement quand on en a besoin.

Ne pas deviner les capacités

Ne pas avoir à investir sur une prévision non confirmée. Automatiser l'ajustement en ressource en fonction des besoins mesurés.

Profiter des économies de masse

Très grande quantité de ressource accessible sans investissement en amont, disponible à la demande sans engagement.

Go global dans la minute

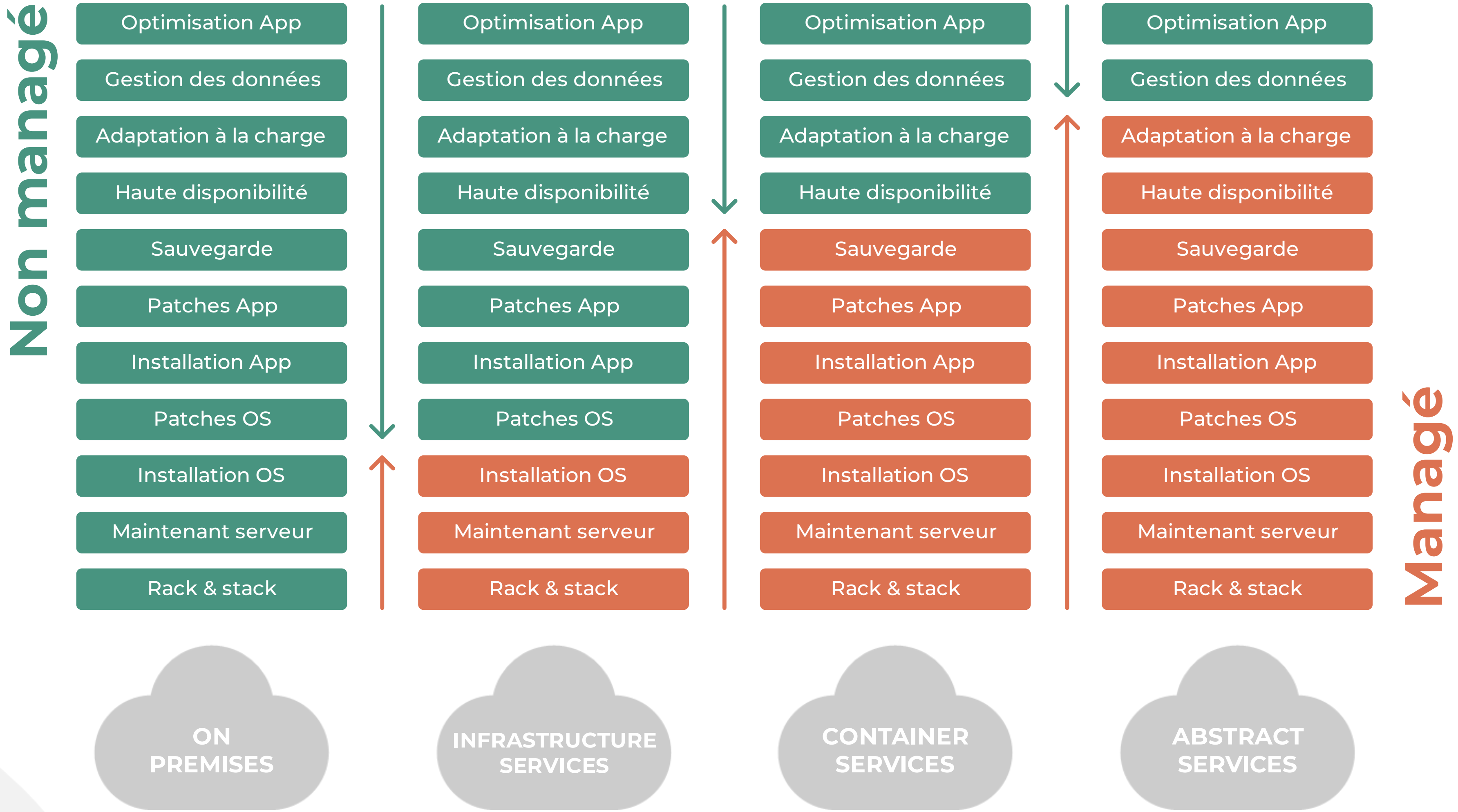
Profiter des datacenters disponibles mondialement fournis par le partenaire Cloud à la demande.

AGILE

4 valeurs

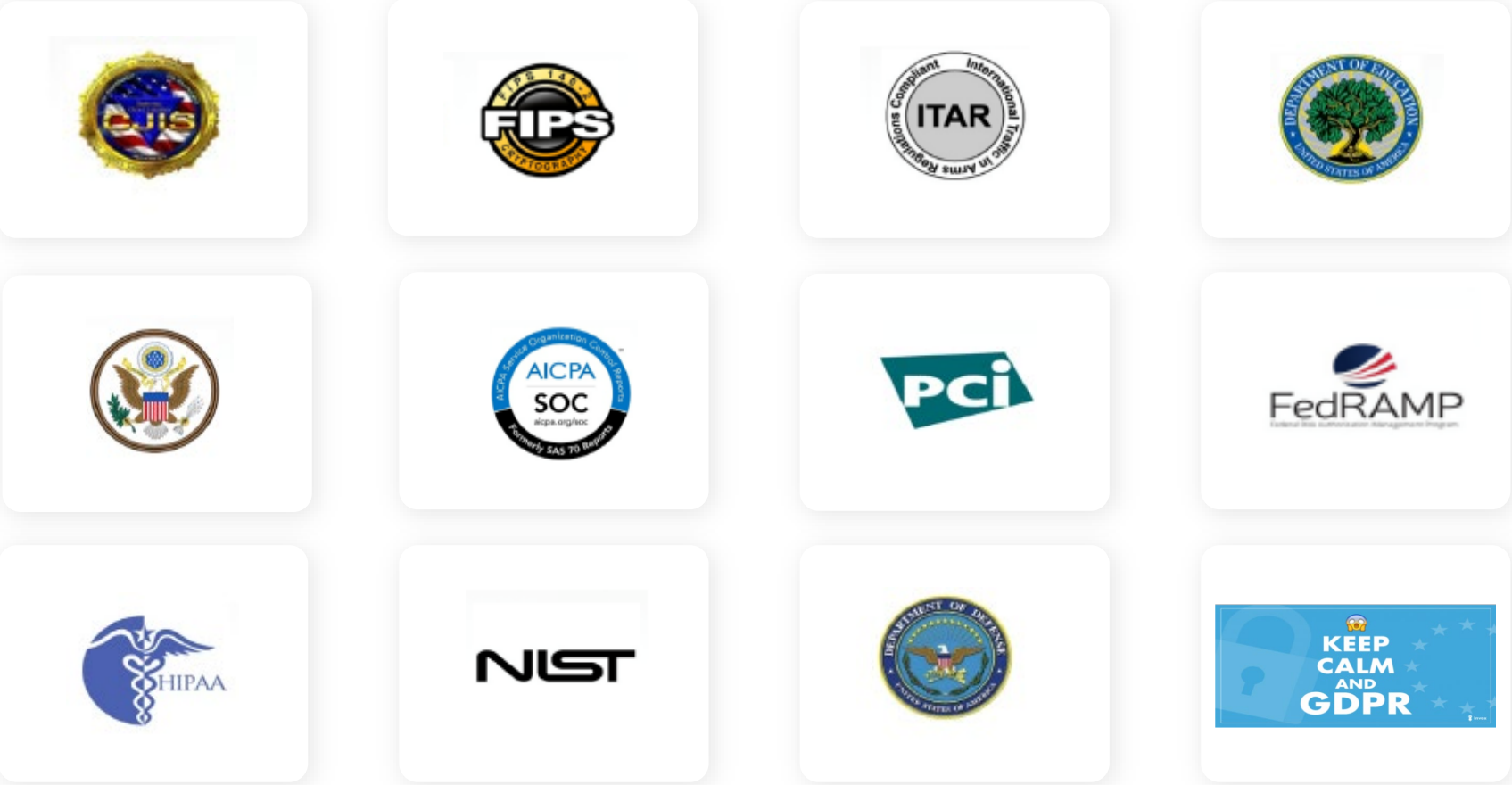
- Changement est une culture – itérations nombreuses, petite taille
- Les gens avant les process avant les outils
- Collaboration – Travailler ensemble pour se comprendre
- Un produit qui fait sens et qui se suffit

RESPONSABILITÉS PARTAGÉES



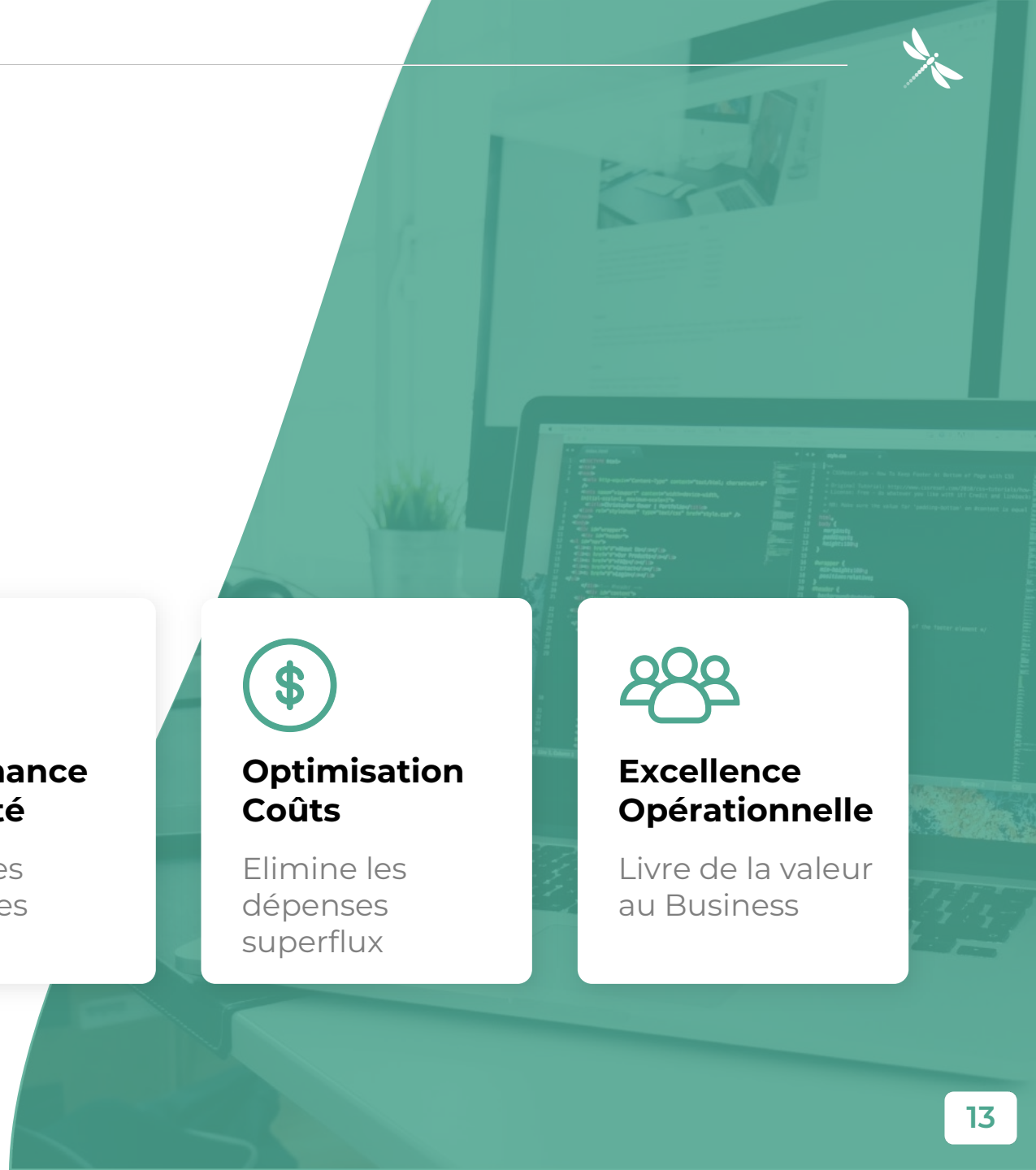
CLOUD ET CONFORMITÉ

Dois-je faire confiance ?



5 PILIERS DU CLOUD AWS

AWS : Well-Architected framework a été développé pour aider l'adoption de la culture cloud pour faciliter les architectes à mettre au point des infrastructures plus sécurisées, fiables, résilientes, performantes et économiques pour l'hébergement de leurs applications.



Sécurité

Protéger et surveiller les systèmes

Fiabilité

Reprise après indicent et mitigation de l'impact

Performance Efficacité

Usage des ressources

Optimisation Coûts

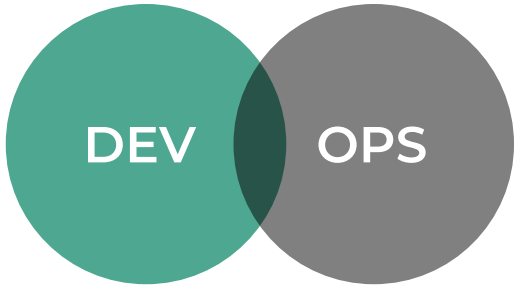
Elimine les dépenses superflux

Excellence Opérationnelle

Livre de la valeur au Business

DEVOPS

- DevOps fournis aux équipes la culture et la compréhension pour atteindre les objectifs d'agilité souhaitées
- Réunir ensemble les forces de chaque équipes
- Documenter toutes les actions
- Réduire les surfaces de projet
- Automatiser l'ensemble des étapes
- DevOps nécessite une véritable bascule de culture



DEVOPS

La loi de CONWAY

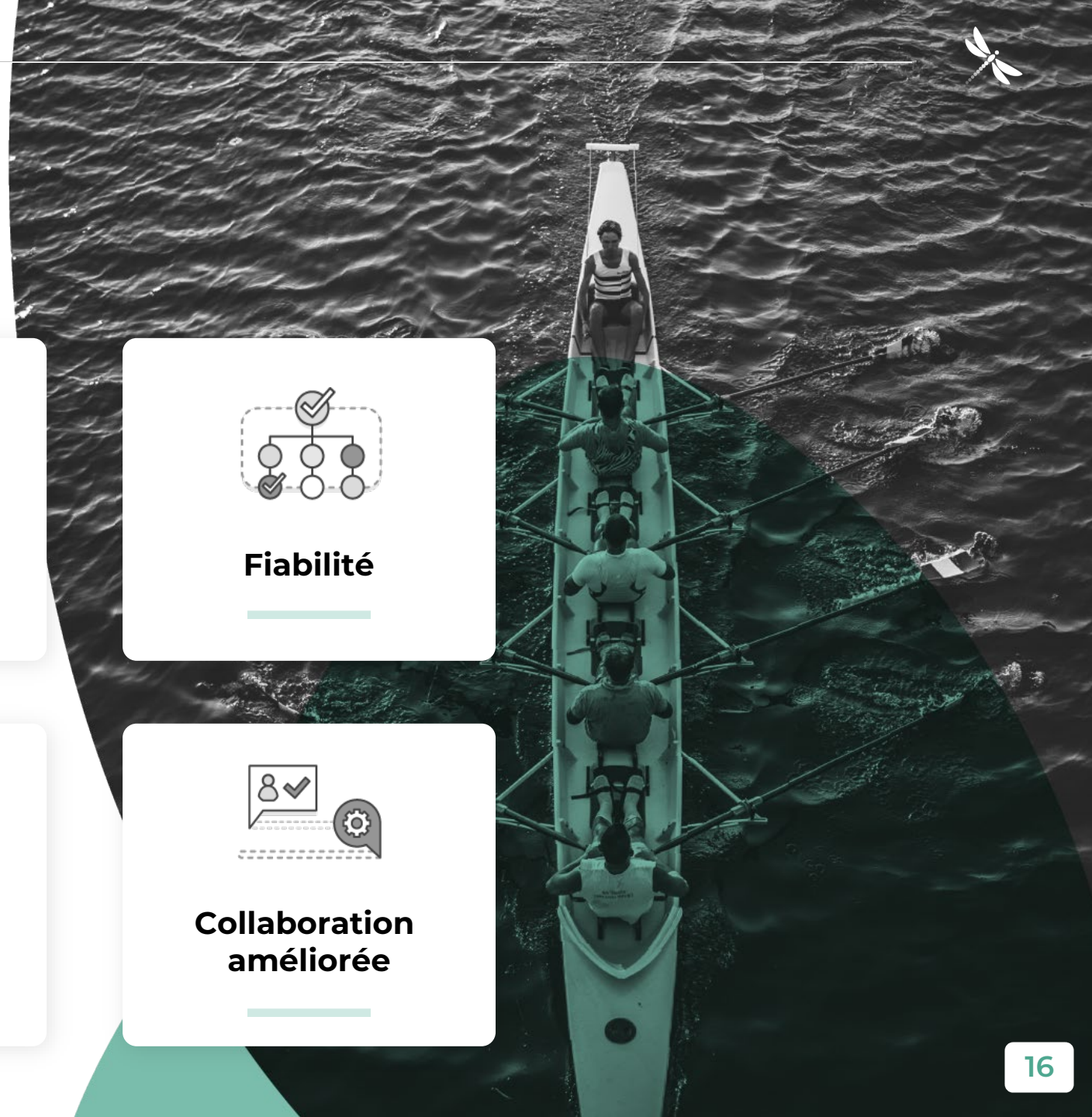
LES HUMAINS

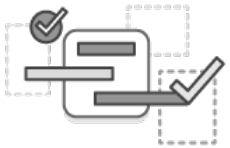
LES PROCESS

LES OUTILS

DEVOPS

Bénéfices





Vitesse

Livraison rapide

Fiabilité

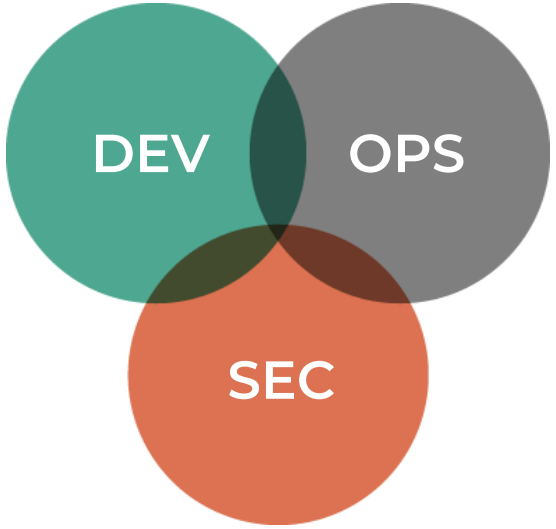
Adaptation à la charge

Sécurité

Collaboration améliorée

DEVSECOPS

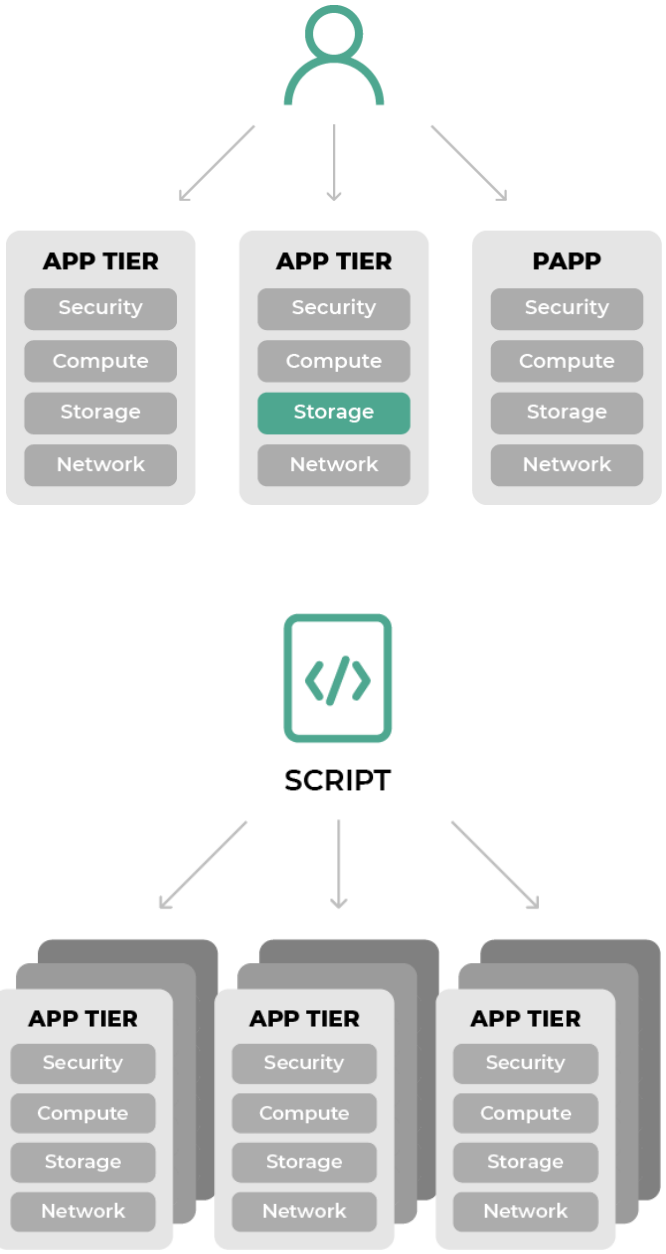
- Apporter les bénéfices de l'agilité et de l'automatisation aux domaines de la sécurité, à grande échelle
- La sécurité, les normes et standards font partie de la définition du produit



AUTOMATISATION

Infrastructure as code

- L'humain fait des erreurs
- L'humain a trop de **valeur** pour lui faire faire
- des tâches répétitives
- Un script, un template = documentation
- **Fiable**
- **Sécurisé**
- Environnement variable
- Adaptation à la charge
- **Résilient**
- Versionné



INFRASTRUCTURE AS CODE

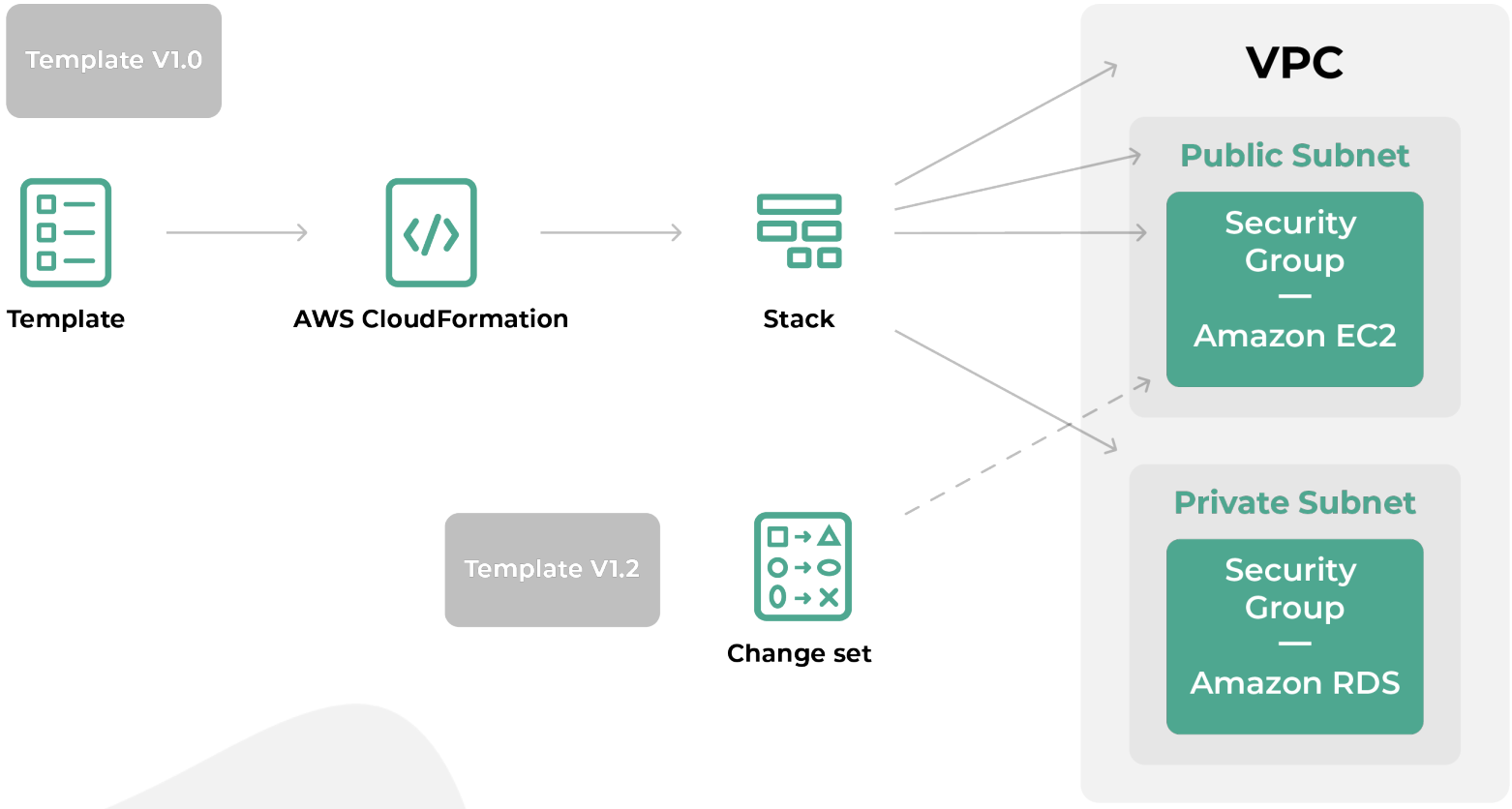
On parle d'infrastructure **as code** quand les environnements sont le fruit d'appel **d'API** et que tous les composants peuvent être invoquer par itération programmatique.

- Un script suffit pour déployer tout un environnement :
  - Documentation
  - Répétable
  - Fiable
  - Auditable

```
"subnet11c4a766": {
    "Type":
"AWS::EC2::Subnet",
    "Properties": {
     "CidrBlock": "10.1.10.0/24",
       "AvailabilityZone" : {
    "Fn::Select" : ["0", {
     "Fn::GetAZs" : {
       "Ref" : "AWS::Region"
     }
    }]
  },
```

INFRASTRUCTURE AS CODE

AWS CloudFormation est un service de gestion des déploiements et mises à jour d'infrastructure.



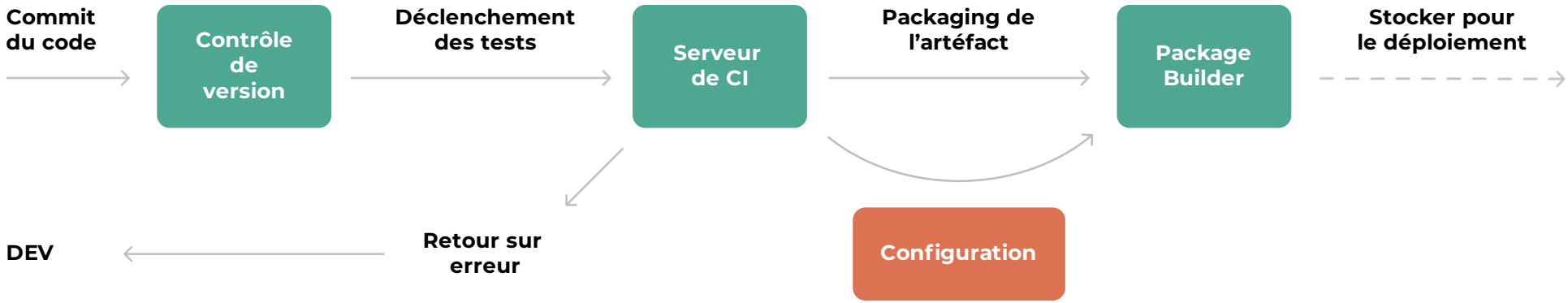
EN CONTINUE

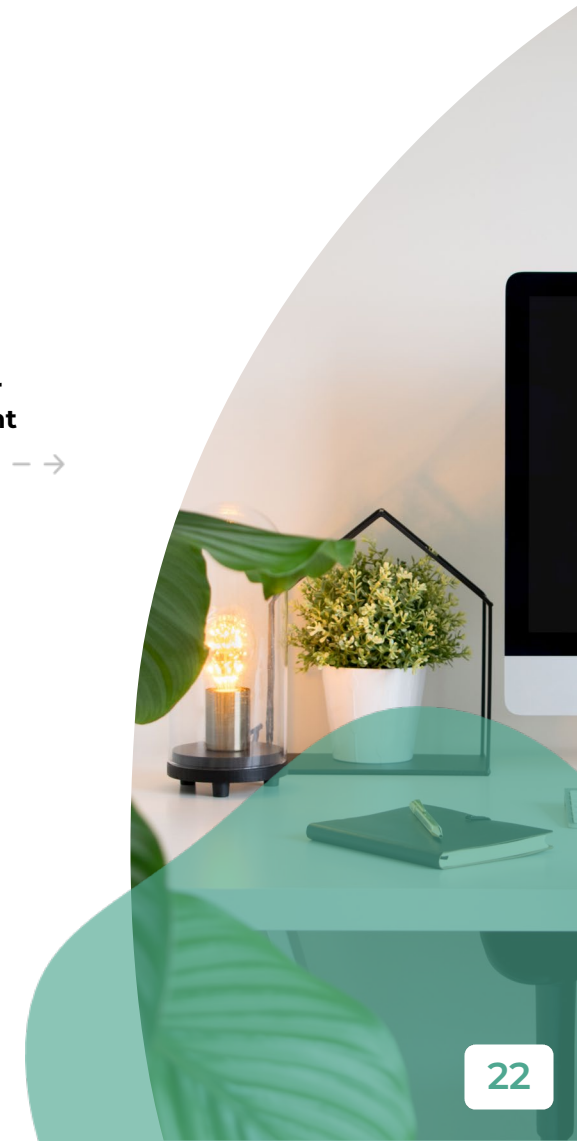
- Intégration
- Déploiement
- Supervision
- Retour
- Apprentissage
- Changement

CONTINUOUS INTEGRATION

Intégration continue

Soumettre une nouvelle version de code à un traitement automatiser de validation avant sa finalisation.



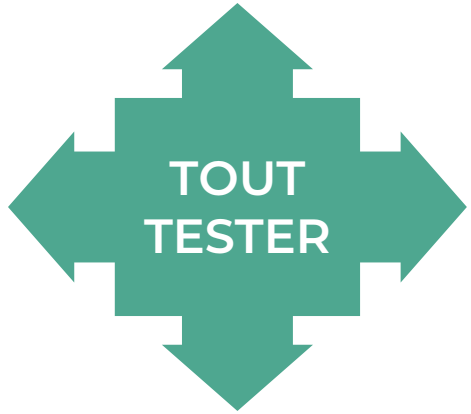


CONTINUOUS INTEGRATION

Intégration continue

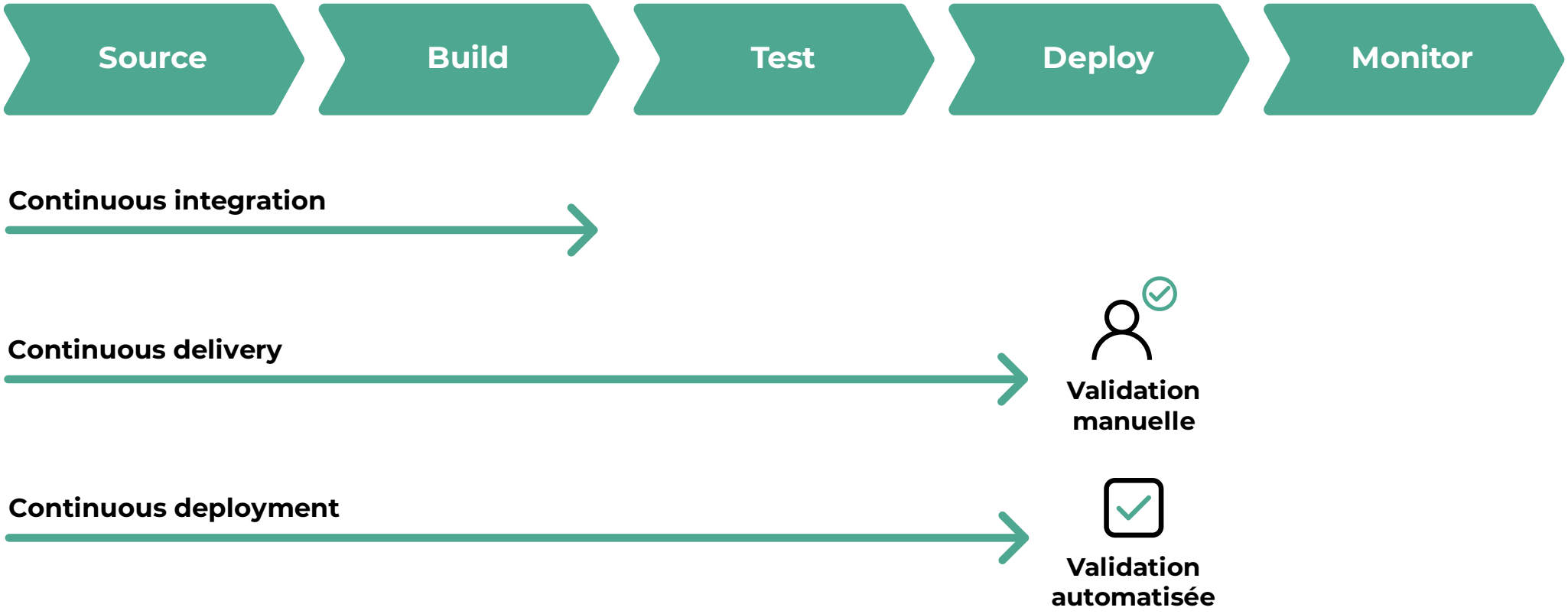
- Structurer la livraison des outils jusqu'au preneur de décisions de façon automatisée
- Fournir un produit finalisé, validé, testé conforme pour la mise en production

- Apporter de la valeur par l'automatisation des tests (éviter les étapes manuelles)
  - Tests unitaires
  - Tests d'intégration
  - Smoke test
  - Tests de charge
  - Test utilisateurs



CONTINUOUS INTEGRATION

Intégration continue



CONTINUOUS MONITORING

Supervision continue

- Superviser les infrastructures de l'application mais aussi l'usage du cloud
- Le cloud propose une intégration systématique aux services de supervision tel que **AWS CloudWatch, AWS CloudTrail** et fourni la possibilité de compléter cette vue par l'intégration rapide avec d'autres services
- Déclencheur d'automatisation

AWS CloudWatch

AWS CloudWatch Logs

AWS CloudTrail

AWS AWS Config

AWS XRay

CONTINUOUS FEEDBACK

Retour continue

Valorisation du retour d'expérience des clients, utilisateurs, consommateurs

Permet de :

- Valider les choix faits
- Valider l'ergonomie
- Un point de vue réaliste de l'usage sur le terrain
- Orienter les prochains projets, décisions, évolutions

CONTINUOUS LEARNING

Apprentissage continue

Une valeur DevOps par excellence, apprendre et transmettre l'acquis pour :

- Pérenniser les expériences
- Eviter de répéter les erreurs
- Créer une culture commune
- Favoriser l'adoption des décisions, des changements et des standards

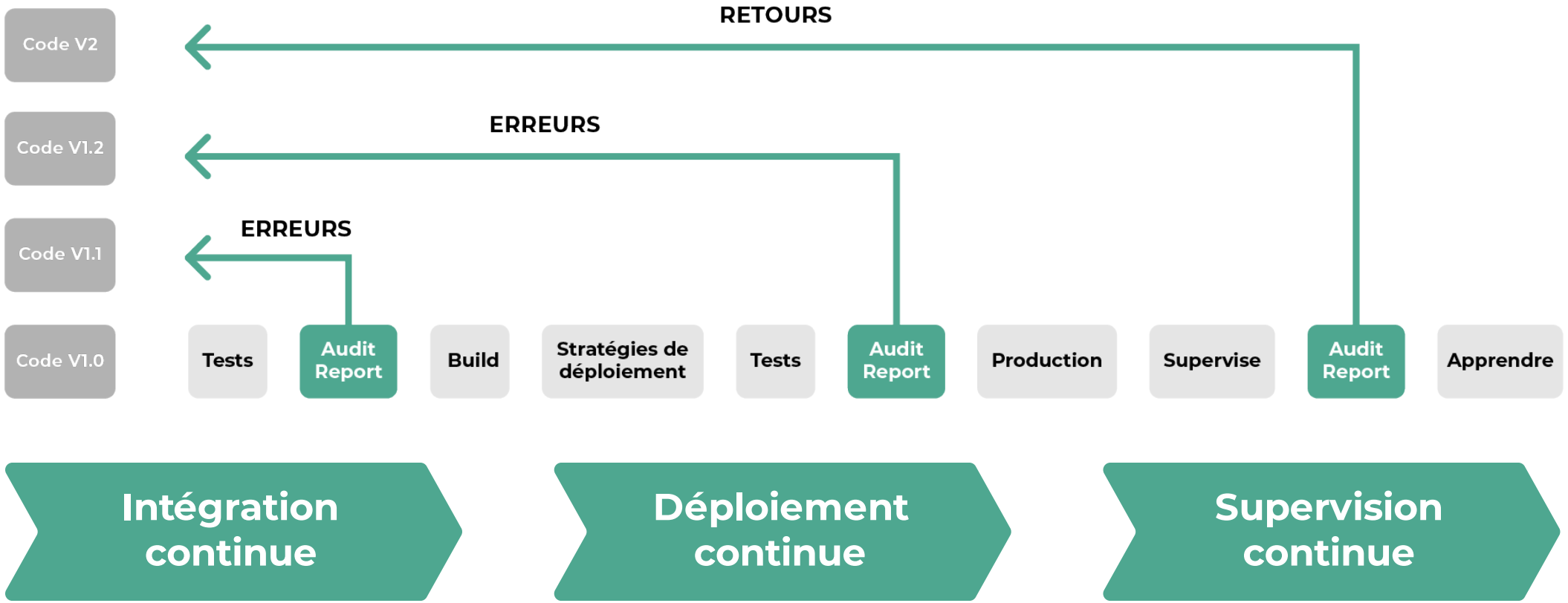
CONTINUOUS CHANGING

Changement continue

Faire du changement une culture de l'entreprise pour accroitre l'agilité et mettre les individus dans un contexte d'innovation sans crainte et sans résistance.

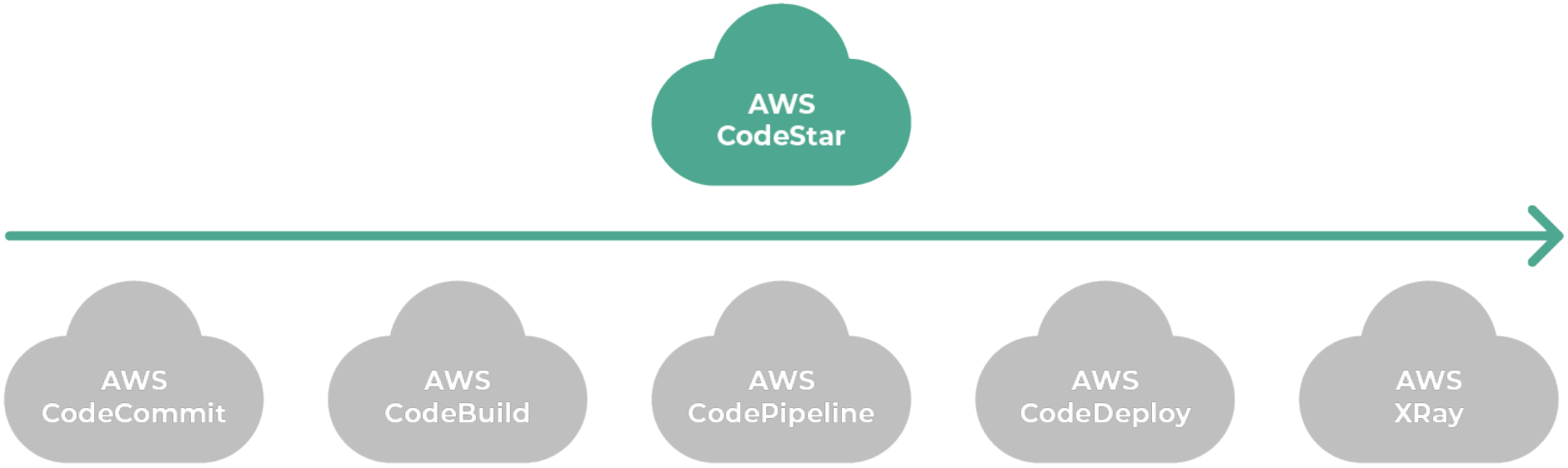
PIPELINE D'AUTOMATISATION

1/2



PIPELINE D'AUTOMATISATION

2/2



Intégration continue

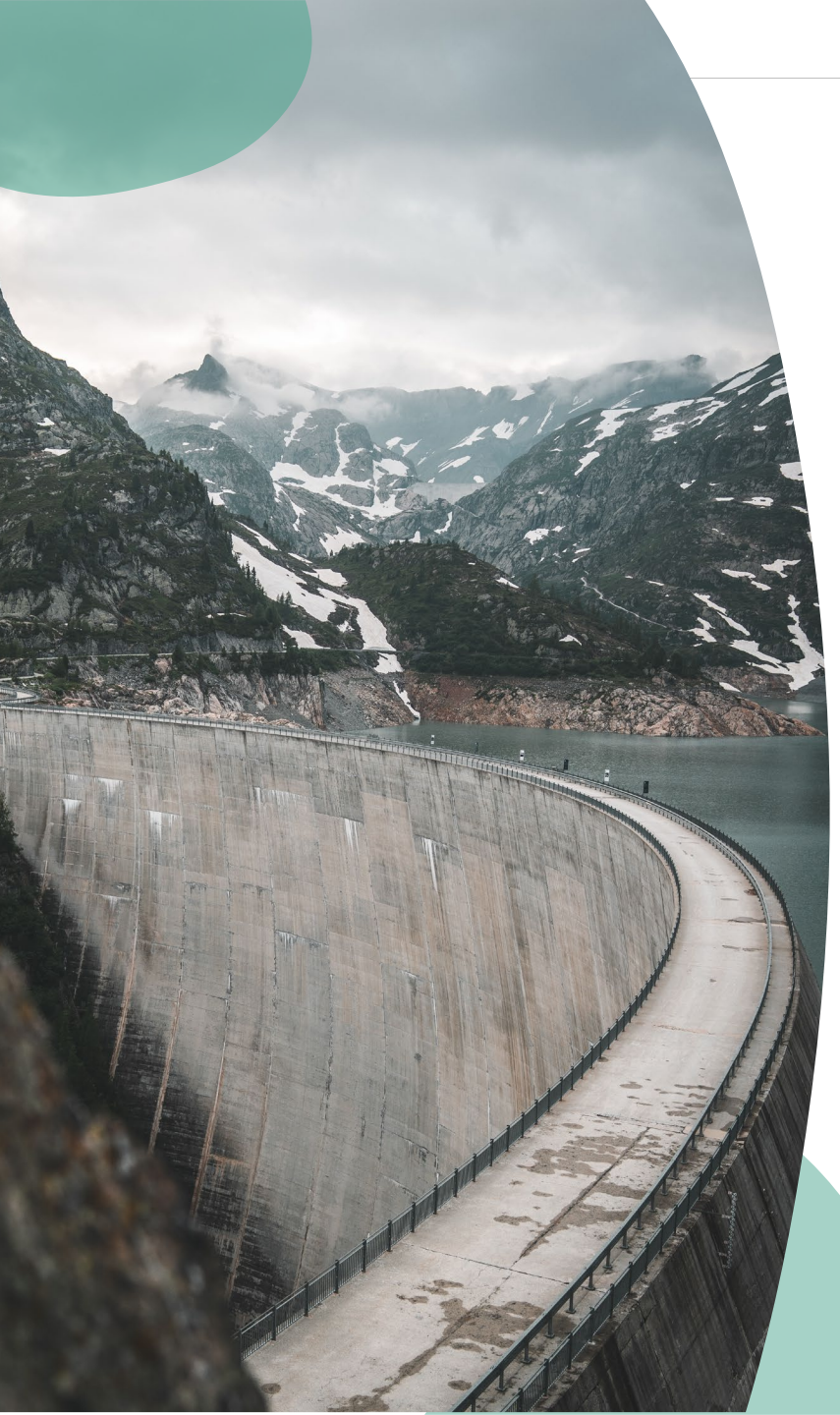
Déploiement continue

Supervision continue

CLOUD TEMPLE
Innovative by design

DEVSECOPS OU COMMENT INTÉGRER LA SÉCURITÉ DANS LES PRATIQUES DEVOPS

M. GIULIANO IPPOLITI



COMMENT LIVRER À HAUTE FRÉQUENCE DU SOFWARE SÉCURISÉ ?

Le contexte

- Besoins clients qui changent continuellement
- Time-to-market réduit (concurrents, règlementations)
- Emergence des pratiques agiles et de la culture DevOps

Limites de l'approche de sécurisation traditionnelle

- Séparation des rôles
- Droit de veto de l'équipe Sécurité
- Sécurisation sur besoins figés, spécifications formalisées
- Stopper pour auditer

COLLABORATION

L’équipe sécurité travaille « AVEC » les développeurs

- Dès le début des projets (shift security to the left)
- Rédaction de user stories orientées sécurité
- Rencontres récurrentes
- Partage d’expérience

Nomination de champions sécurité

- Scalabilité
- Diffusion naturelle des bonnes pratiques
- Enrôlement volontaire

Binômage

COLLABORATION

Formation au développement sécurisé

- OWASP Top 10, CWE Top 25
- Certifications : GWEB, CSSLP, CASE

Sensibilisation

- **Par l'équipe Sécurité**
  - Démonstrations de piratage
  - Outils : DVWA, Metasploitable
- **E-Learning**
  - Prime pour suivre MOOC ANSSI, CNIL

OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

AUTOMATISATION

Le pipeline de CI/CD doit inclure les tests de sécurité

- Anti-fragilité : amélioration par le stress !

Freins pour l'adoption

- Faux positifs
- Findings non activables
- Lenteur des outils SAST et DAST
- CVE sans solution, ça peut stopper un déploiement

OUTILLAGE POUR LES TESTS DE SÉCURITÉ

Lint

- Vérification des bonnes pratiques de codage
- Contrôles basiques de sécurité
  - Appels système (injection de commandes)
  - Expressions régulières (ReDoS, safe-regex)

SCA – Software Composition Analysis

- Identification des dépendances open-source vulnérables
- Possibilité de configurer des politiques (CVSS)

OUTILLAGE POUR LES TESTS DE SÉCURITÉ

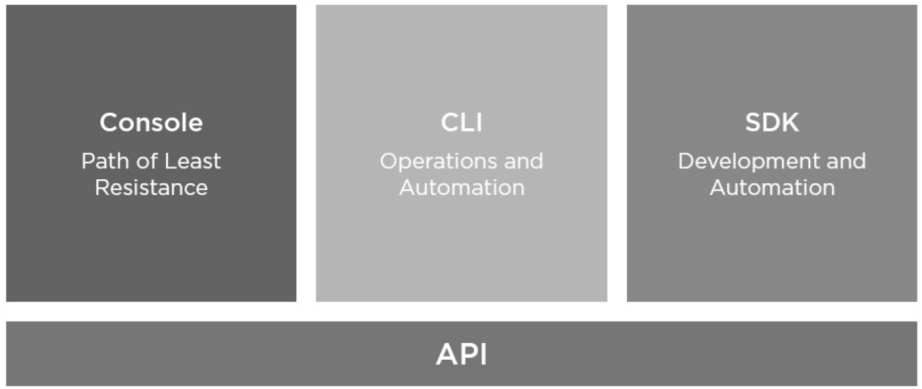
SAST – Static Application Security Testing / White Box

- Recherche de vulnérabilités dans le code source :
  - Buffer owerflows, injections SQL, XSS
- Bonne scalabilité… mais beaucoup de faux positifs
- Parfois intégré dans les EDI

DAST – Dynamic Application Security Testing / Black Box (street test)

- Analyse des vulnérabilités sur l'application qui tourne
- Surface d'attaque élargie à OS et Middleware

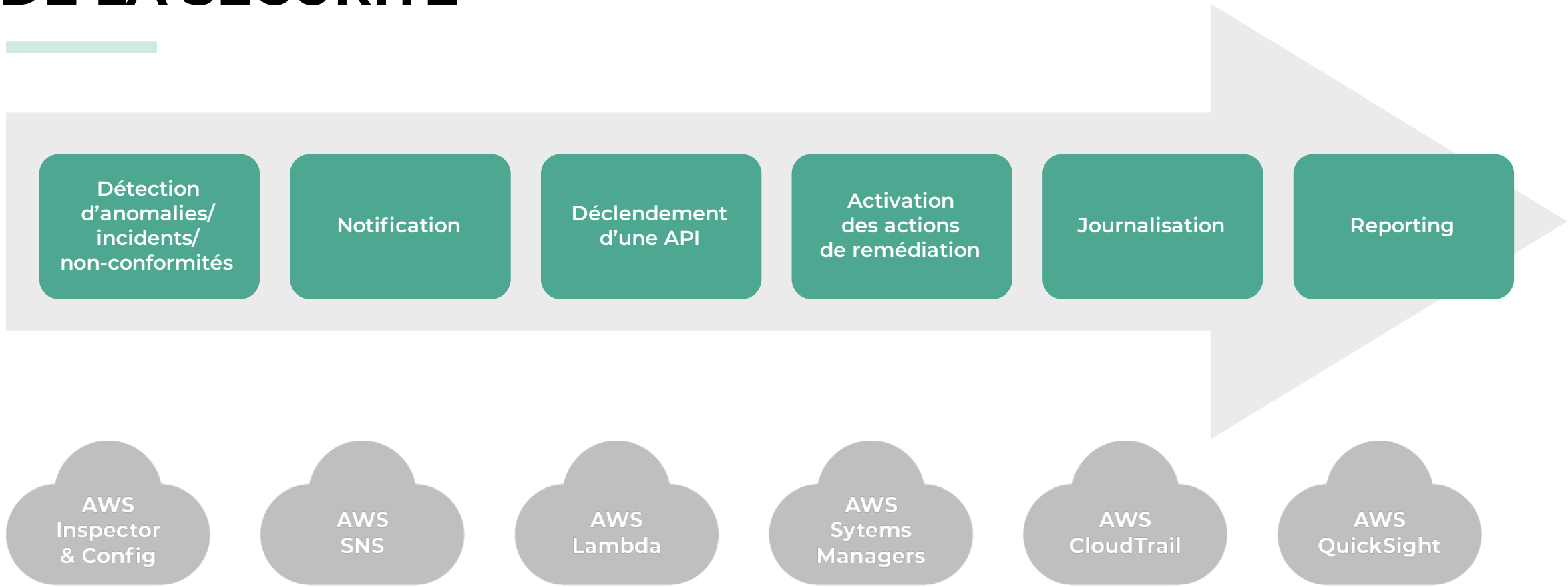
CLOUD PUBLIC – SÉCURISATION DES POINTS D'ENTRÉE



RÈGLES D'OR

- Activer la MFA
- Rotation régulière des clés d'accès
- Révoquer ou supprimer les clés inutilisées
- Ne jamais écrire des clés directement dans le code source plutôt les rôles. (cf fuites via github !) - utiliser
- Approche type « deny all » par défaut
- Respecter le principe du moindre privilège
- Si possible, utiliser la fédération d'identité plutôt que multiplier les comptes IAM

CLOUD PUBLIC – AUTOMATISATION DE LA SÉCURITÉ



CLOUD PUBLIC – VMS ET CONTENEURS

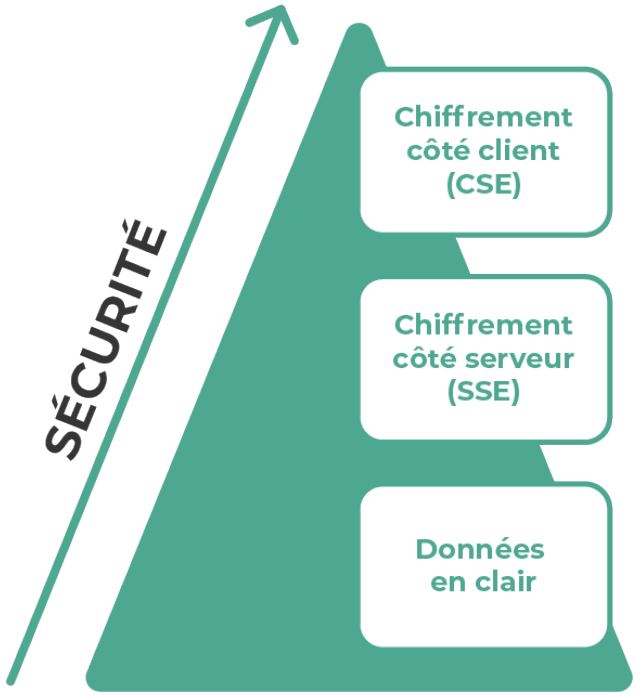
Focus sur le durcissement

- Désactiver les services et protocoles non sécurisés
- Désactiver les services réseau inutiles au démarrage : réduction de la surface d'attaque
- Supprimer toutes les credentials (mots de passe, clés SSH, ...)
- Nettoyer les logs
- Durcir les configurations (cf CIS Benchmark,...)
- Utiliser Docker Content Trust (DCT)

Les classiques

- Automatiser la gestion des vulnérabilités
- Utiliser le principe du moindre privilège pour les accès
- Eviter les SPOFs (cf Chaos Monkey de Netflix)

CLOUD PUBLIC – CHIFFREMENT



Gestion des clés

- Où sont stockées les clés ?
  - KMS, HSM, …
- Qui gère les clés ?
  - Politique d'accès

QUESTIONS /RÉPONSES

CONTACTEZ-NOUS

cloud-temple.com

contact
@cloud-temple.com

RETROUVEZ-NOUS ÉGALEMENT SUR