Cloud π Native

au profit de la doctrine Cloud au centre de l'État et des migrations d'applications

Sensibilisation aux enjeux de l'offre

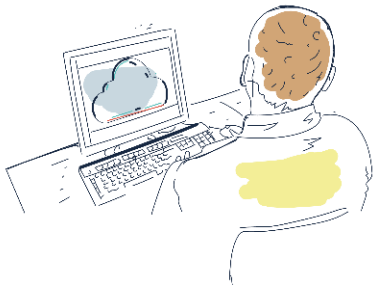
Cloud π Native

CONSTRUISONS ENSEMBLE LES APPLICATIONS DE DEMAIN

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

De quoi parle t-on ? Histoire, protagonistes

La chaine, de personnes et d'outils, utilisée par l'administration pour **produire et mettre en service** des produits numériques pour **répondre aux besoins des agents et des usagers**



Développeurs (Dev)
Production du code

Outils de production

Usine logicielle, forge, …

Pilotage/chefferie de projet

Gestion de projet, utilisation des ressources

Gouvernance/ décisionnaires

Organisations et moyens

UX designers

Challenge besoins, tests utilisateurs

Architectures, exigences

Conception, structuration

Opérateurs (Ops)

Gestion du produit

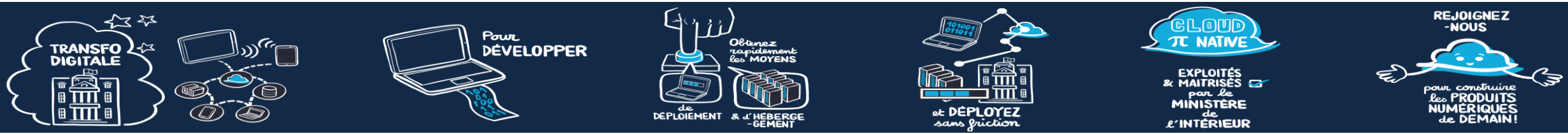
Sécurité SI (Sec)

Homologation, autorisation

Infrastructures (infra)

Faire « tourner » le code

Utilisateurs
Agents ou usagers



MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Dans quel monde s'inscrit-on ? pourquoi transformer la production du numérique public?

Quelles opportunités ? le cloud et la doctrine « cloud au centre »

Quel est l'état de l'art visé ? L'approche "Cloud native"

Quelle est la proposition du MIOM? La solution "Cloud π Native" du Ministère de l'Intérieur

Conclusion

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Transformation numérique et administration publique

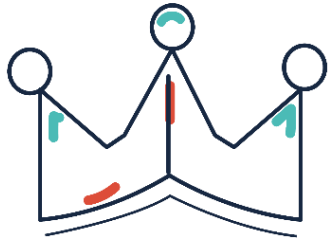
L'enjeu vital : proposer aux agents et usagers des produits numériques « aussi bons » que ceux qu'ils utilisent en tant que consommateurs

Un « nouveau monde » logiciel a émergé

- **Contexte** « VUCA », GAFA, disruptions numériques
- **Nouveaux standards « de fait »:** qualité, sécurité, technologies, culture
- **Domaines régaliens exposés**

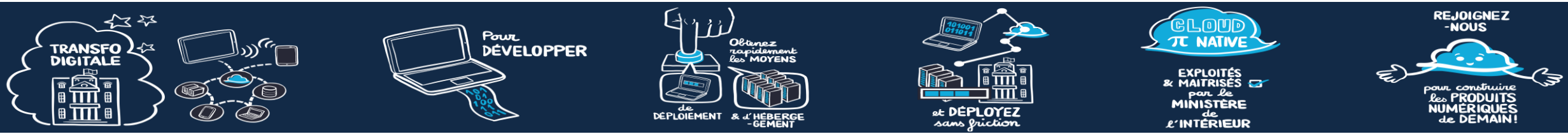
« Comment ont-ils fait? »

- **Qualité:** évolution continue (mode produit), production industrialisée
- **Infrastructures Cloud:** sécurité, automatisation, croissance à cout marginal
- **Culture:** autonomie dev/UX, open source, innovation



Autonomie stratégique de l'administration publique

- **Cadre législatif:** régulation
- **Maitrise technique:** standards (SSI, RGPD, …)



MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

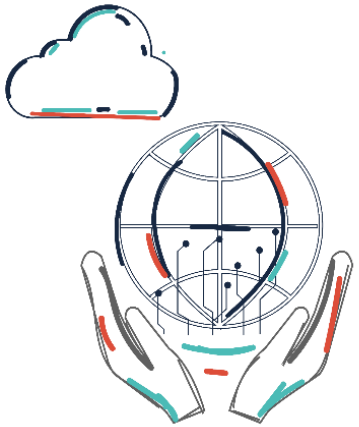
Maîtrise du patrimoine- pourquoi le cloud?

Le patrimoine numérique de l'administration est à la fois **1) l'interface** avec les usagers & agents **2) l'incarnation de de son organisation** (loi de Conway). Le maitriser est un **enjeu vital.**

Maitrise du périmètre: choix produits (logiciels et matériels)

- Achetés ou consommés (« **buy** »)
- Développés en interne (« **make** »)
- Sous-traités à l'extérieur (« **faire faire** »)

Périmètre clair vs. « shadow IT »



Maitrise du cycle de vie des produits:

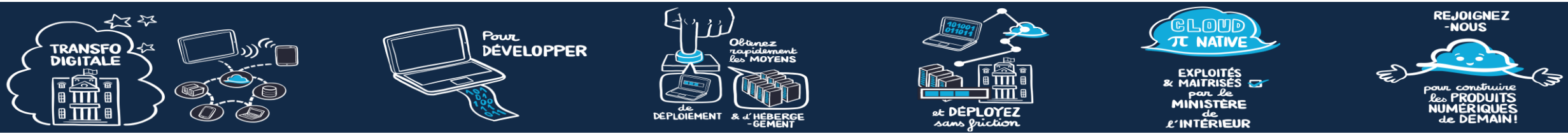
- **Dev:** écriture, assemblage, gestion de version, partage…
- **Ops:** déploiement, hébergement, MCO…
- **Sec, Gouv:** lancement, homologation, évol., arrêt…

Responsabilités claires vs. diluées

« Le cloud »: cadre pour le patrimoine numérique

« Où? » il est hébergé

« Comment? » il est produit, géré



MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

La doctrine « Cloud au centre »

2021, doctrine gouvernementale « Cloud au centre »: « *faire du cloud le mode d'hébergement et de production par défaut des services numériques de l'État pour tout nouveau produit numérique, tout produit connaissant une évolution substantielle.* »

Au centre des stratégies ministérielles d'hébergement… et de transformation

- **Production:** principes de conception (architecture), socles techno., approches et cultures (DevOps)
- **Focalisation sur l'usage**: sur le client/usager (mode produit) ET les développeurs
- **Passage à l'échelle:** nouveaux produits, innovation (IA, big data, ..), coût marginal faible
- **Standards:** impact environnemental, dépendances (Open source), protection (RGPD)

Pour…

Souveraineté

Sécurité: disponibilité, intégrité, confidentialité (droit extra-UE!)

Accès aux technologies les plus récentes

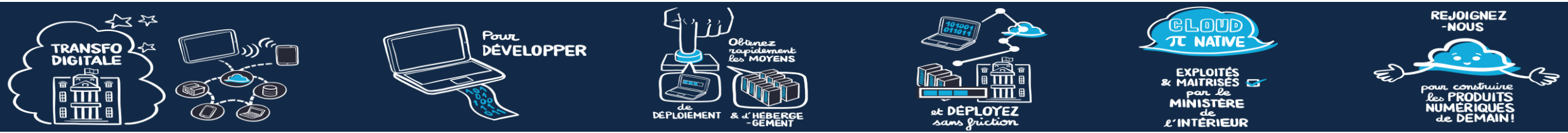
Choix : réversibilité et interopérabilité

Accélération

Soutien: industriels du cloud FR et UE

Structuration: filières FR et UE

Autonomie stratégique: standards FR et UE

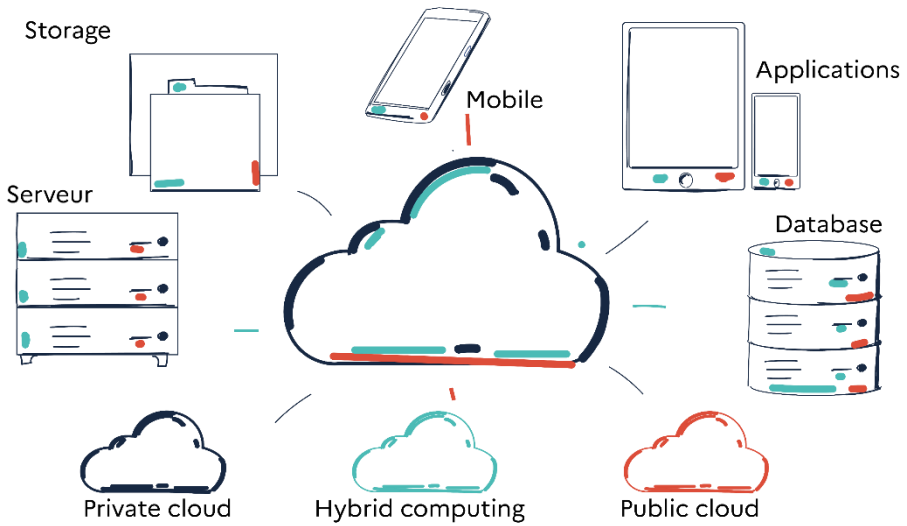


MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

DNUM

Le "cloud", qu'est ce que c'est ? (1/3)

Une nécessité pour la transformation numérique : sans la puissance du cloud, l'adoption massive d'outils numérique pendant la crise covid n'aurait pas été possible



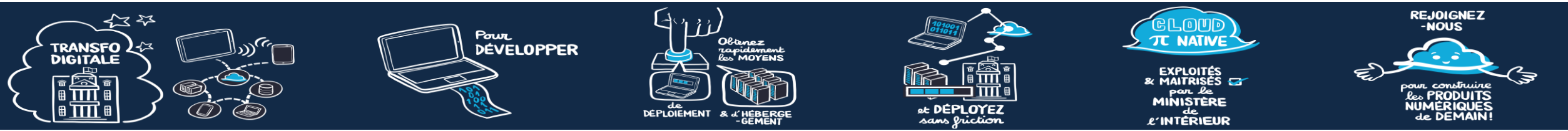
"Juste" des datacenters/serveurs…?

- Des resources (serveurs, stockage, calcul performant…)

+ Allocation dynamique/fluide des ressources

5 fonctionnalités *(*NIST)*

- **Mutualisation** de ressources géographiquement distribuées
- **Disponibilité** via un réseau performant
- **Accès facile** à la demande (UX, identification, sécurité…)
- **Facturation à l'usage,** cout marginal faible
- **Elasticité,** redimensionnement rapide (scalabilité)



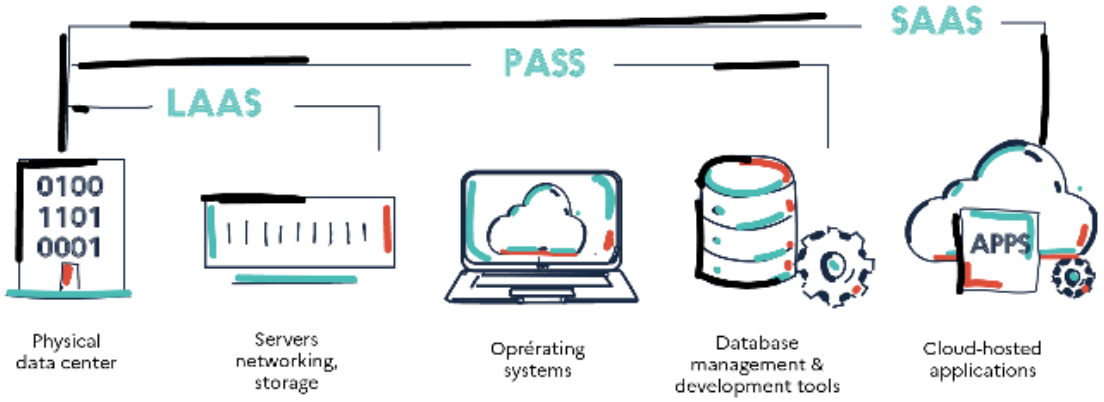
MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Le "cloud": quelles offres pour quelles garanties? (2/3)

Que garantie l'offre d'un fournisseur de service cloud ? Est-ce plus ou moins sûr que des infrastructures « *on-premise* » implantées et opérées au sein de l'organisation?

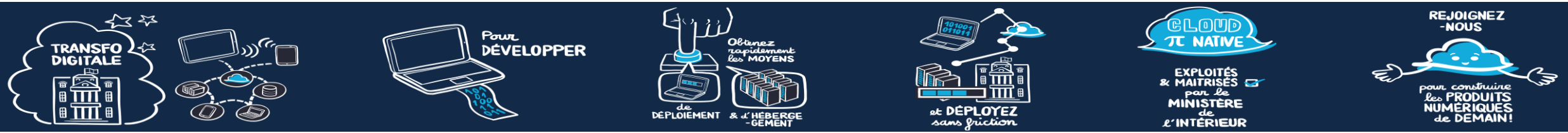
Garanties opérationnelles et juridiques

- Développement, opération, MCO des technologies sous-jacentes
- Equipes dédiées, automatisation étendue
- Contractualisation du partage des responsabilités



Sécurité

- **Haute disponibilité**, scalabilité rapide
- **Intégrité,** tolérance aux pannes
- **Confidentialité:** protection données, immunité au droit extraterritorial…



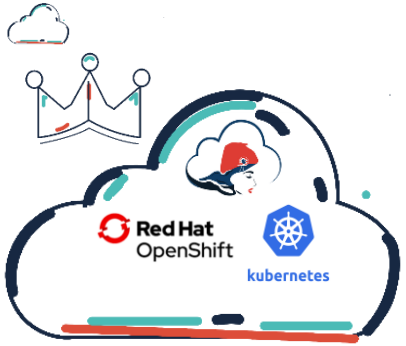
MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Le "cloud", à qui faire confiance? (3/3)

Par qui sont fournies les technologies et les services cloud? Qu'est ce qui distingue les différents types de fournisseurs, avec des avantages/risques de natures différentes

Alibaba Cloud

OVHcloud



- **Fournisseur interne** : organisation pour elle-même **(cloud privé)**
- **Fournisseur commercial:** organisation pour des clients **(cloud public)**

Des fournisseurs particuliers

- **Oligopoles:** hyperscalers US (AWS, Azure, Google) … et chinois
  - Risques de nature géopolitique vs. perrformance
- **"Cloud de confiance":** OVH (bac à sable Cloud Pi Native)
  - Loc. UE+ référentiel SecNumCloud (ANSSI) vs. résilience inf. (+ petits)

Cloud souverain "internes", mutualisé pour l'administration publique

- **Nubo (DGFiP):** souverain, adapté données sensibles
- **Cloud π (MIOM):** souverain, jusqu'au niveau DR (diffusion restreinte)
- Confidentialité élevée vs. cout investissement initial

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Vous avez dit "Cloud Native" ?

Le « cloud native » est un **modèle, approche de production** pour « *des applications scalables au sein d'environnements modernes et dynamiques publics, privés ou hybrides* » **(promesses du Cloud)**

Leviers techniques

Infrastructures cloud

Patrons de conception (architectures techniques)

Outils de production (usines logicielles)

Levier culturels

Usager au centre, évolution continue…

Open Source

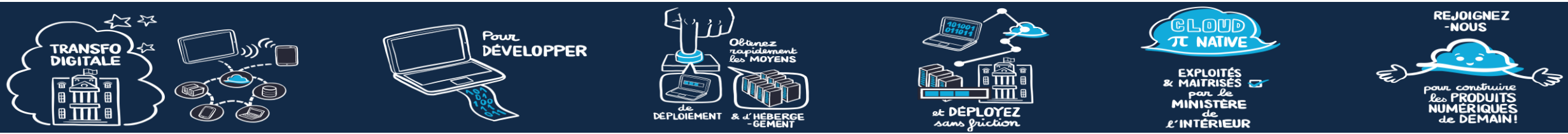
Conduite du changement

Leviers organisationnels

Organisation en « mode produit »

Agilité à l'échelle

Responsabilités Dev, Sec, Ops, partagées au sein du processus de production (« DSO »)



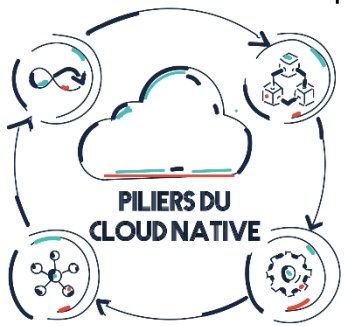
MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

L'état de l'art "Cloud Native"

Ensemble de projets open source soutenus par la cloud native computing foundation et répertoriés dans le **CNCF « landscape »** pour promouvoir les standards technologiques et bonnes pratiques du modèle « Cloud Native »

Outils DevOps
Automatisation, standardisation, collaboration, autonomie

Conteneurs
Consommation de ressources automatisée, fine, résiliente



API
Interopérabilité et interconnexion applications et données

Microservices
Applications modulaires et reconfigurables

DOCKER
Technologie de conteneurisation

KUBERNETES
Gestionnaire de conteneurs

Clusters kubernetes

Plateforme de conteneurs & microservices qui assurent le **pilotage** de la consommation des ressources d'infrastructures

Clusters vs. machines virtuelles (VM)

- **Indépendance:** portabilité & interopérabilité fournisseurs infra/OS
- **Automatisation:** pilotage d'un état cible, orchestration
- **Résilience:** décentralisé, fiable, extensible

amazon
1 déploiement en production toutes les 10 secondes

GitHub
30 secondes pour un retour arrière en production

NETFLIX
16 min pour déployer en production multi-régions

facebook
2 déploiements/jour pannes rarissimes

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Le "Cloud Native", cible de la trajectoire DTNUM

Le passage à l'état de l'art « Cloud native » s'inscrit dans la **trajectoire d'accélération numérique** que soutient et promeut la DTNUM pour socle de production à l'état de l'art

Offre « Isocele »: infrastructures physiques + virtualisées

- **Infrastructures infogérées**
- **Dépendances**: équipes/infra

Offre « Cloud π »: infrastructure à la demande (Iaas)

- **VM :** autonomie dans les tenants
- **Forge en option:** possibilité de standardisation

Offre « Cloud Native »

- **Clusters** : gestion automatisée d'infrastructure (Cloud π gen 2)
- **Production standardisée :** collaboration étendue, ouverture de flux, homologation en continu, … (usine DSO)

- **Migration Cloud Pi gen1 → gen2**
- **Usine logicielle**

- **Transformation d'applications**
- **Création de nouveaux services numériques**

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

DNUM

L'offre "Cloud Native" du MIOM : Cloud π Native

L'offre "Cloud π Native" est un « package » permettant de transformer des applications existantes ou de produire de nouveaux services numériques à l'état de l'art en capitalisant sur un cloud automatisé et souverain (kubernetes sur les infra MIOM)

Cloud π

Ressources cloud souverain, automatisé et indépendant (clusters)

Usine logicielle DevSecOps (« DSO »)

Outils de production & collaboration (Dev, Sec, Ops, ...) automatisant, standardisant et traçant les opérations au long du cycle de vie

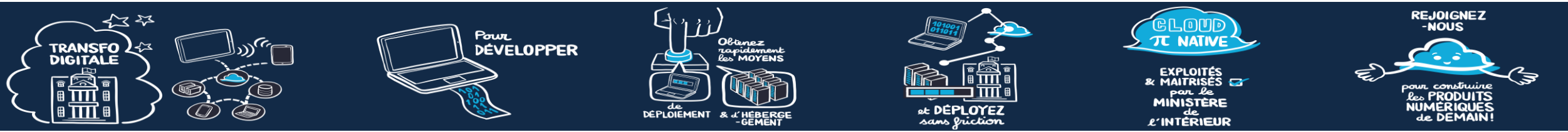
Cadre de cohérence technique (CCT cloud native)

Un cadre d'exigences qui se base sur les principes du cloud native qui s'impose à tous. Guider des utilisateurs tout au long du cycle de vie

Accompagnement

pour la montée en compétences des équipes clientes afin d'atteindre l'autonomie (les outils et les paroles ne suffisent pas)

Cloud π Native
CONSTRUISONS ENSEMBLE LES APPLICATIONS DE DEMAIN



MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

"Usine logicielle DSO" : qu'est ce que c'est ?

L'usine permet la **continuité du processus de production entre les environnements** (matériels, logiciels, système d'exploitation, qui exécutent les programmes) des différents acteurs, jusqu'au déploiement

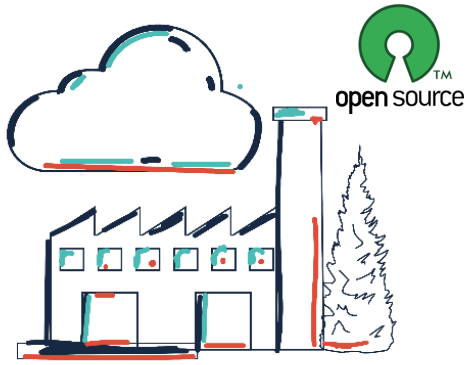
Environnement développeurs
Hors périmètre MIOM (RIE, internet)

Environnement DevSecOps « DSO »
Périmètre maitrisé MIOM

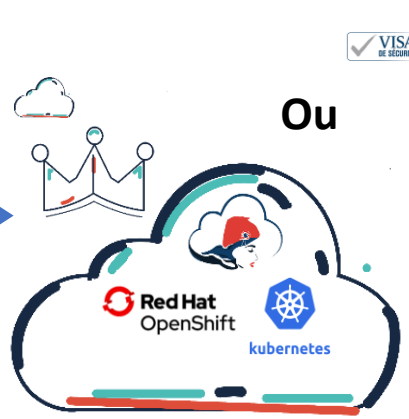
Environnement de production
Périmètre régalien ou « de confiance »

Exigences

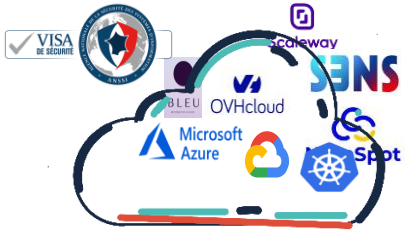
Synchro.



Déploiement



Ou



« Chaine primaire »

- Dépôt développeurs (y compris prod. externalisés)
- Gestion flux de travail
- Vérification (qualité, fonctionnalités)

« Chaine secondaire »

- Dépôt MIOM: point de vérité unique, architectures-type (helm), automatisation
- Interfaces de coopération, traçabilité
- Sécurisation & vérification, homologation en continue

Clusters managés

- **Cloud π :** sécurité jusqu'au niveau DR
- Hyperscalers: labellisés « SecnumCloud », bac à sable

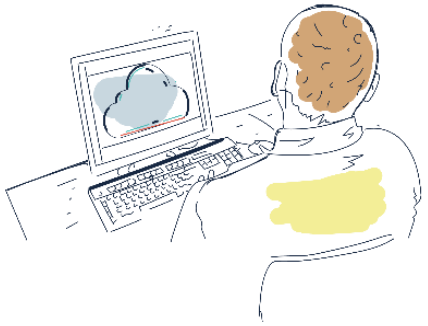
MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Cloud π Native : qu'est ce que ça change?

L'automatisation et la collaboration offerts par l'usine modifient la façon de travailler et permettent une autonomie accrue qui conduit à un **nouveau modèle de responsabilités « *you built it, you run it* »**

SSI (sécurité des SI)

Pilotage/gouvernance
Projet et organisation



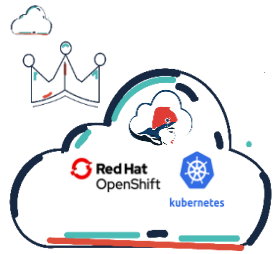
Equipe responsable de l'application
« de la production du code, à la mise en service, à la MCO »

Accompagnement

Exploitation de clusters
mutualisés ou dédiés

Socle DSO et services communs
« cloud native »

Exploitation infrastructures,
réseaux



MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Les bénéfices pour les utilisateurs (+/-) directs

Ces changements d'outils, d'organisation et de culture produisent un **rapprochement dev/utilisateurs, cercle vertueux** qui bénéficie à l'ensemble des utilisateurs de l'offre (*métriques retex et démo)

Gouvernance projet/organisation

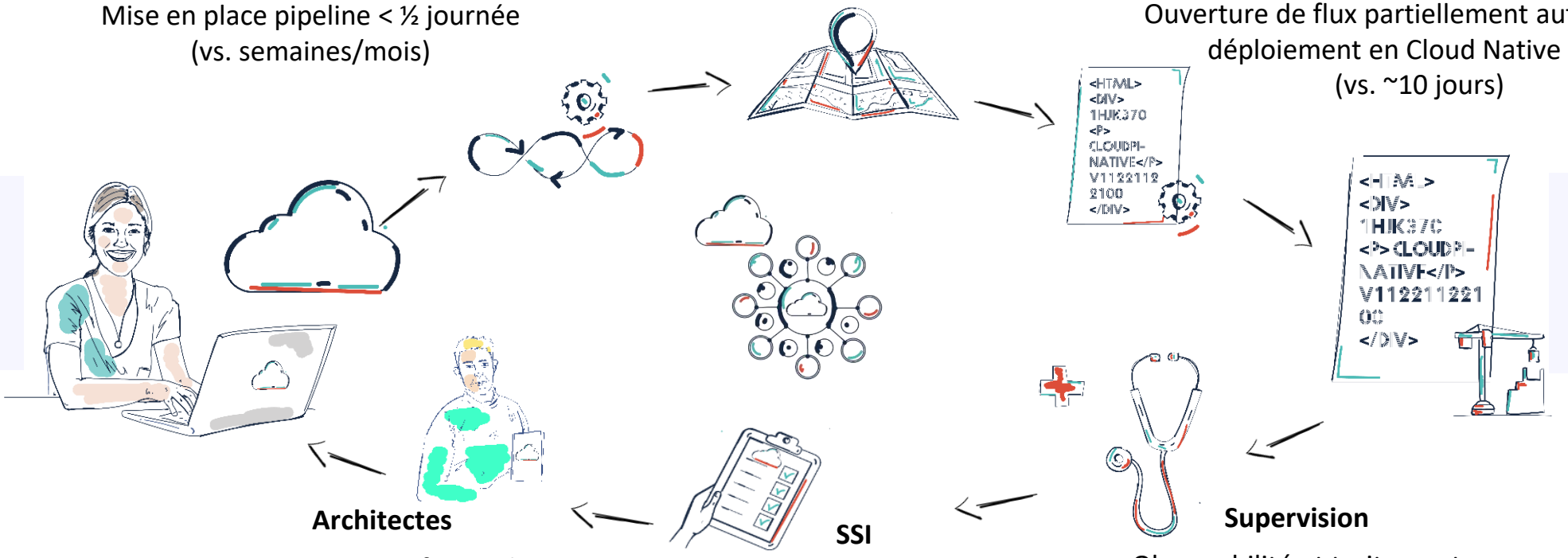
Cartographie (CANEL), état du patrimoine
(vs. consolidation de listes)

Production

Mise en place pipeline < ½ journée
(vs. semaines/mois)

Déploiement, mise en service

Ouverture de flux partiellement automatisée, déploiement en Cloud Native < ½ h
(vs. ~10 jours)



Développeurs

Délais de souscription à la console 1 à 2 semaines

Utilisateur

1er incrément de produit en moins de 6 mois

Architectes

Exigences sous forme de règles (CCT), architecture type

SSI

Homologation facilitée en 3 mois
(vs. 5-18 mois)

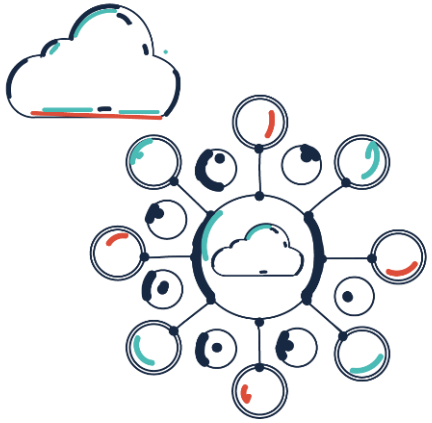
Supervision

Observabilité et traitement des vulnérabilités

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

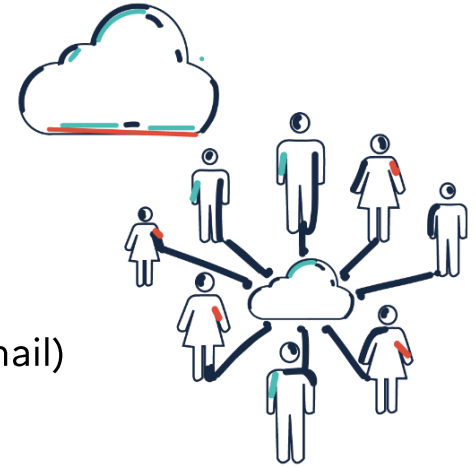
Les bénéfices pour la transformation de l'organisation

D'un point de vue plus large, l'approche « cloud native » est porteuse de conséquences à long terme au niveau organisationnel qui **rejoignent les objectifs transformation numérique de chacun**



- **Prédictibilité , confiance de mise en service**: industrialisation, homologation
- **Cadre ouvert à l'innovation:** règles claires vs. liste fermée de solutions autorisées
- **Enrichissement continu:** intégration API, hub données, IA/LLM, big data, GPU…

- **Attractivité profils « tech »:** techno. à l'état de l'art, open source
- **Réduction distance utilisateur**: coévolution produit/usages, UX design
- **Autonomie des applications:** self-service DevOps pour nouveaux services



- **Ouverture vs. sécurité :** sécurité de bout en bout, en continu (homologation)
- **Coopération vs. autonomie:** traçabilité opérations, pilotage via interfaces (vs. mail)
- **Besoins vs. moyens:** équation make vs. buy, inno/MCO/dé-commissionnement

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

L'offre Cloud π Native : parcours "client" cible

Disponible via un **parcours intégré supporté par des outils** en amélioration continue pour **réduire les « frictions » organisationnelles, la charge cognitive et de travail** des utilisateurs

Cloud Pi Native
Plateforme DevSecOps du gouvernement français

Portail PI (RIE)

demarches-simplifiees.fr

"La console cloud π native"

Gestionnaire de clusters

Je découvre
l'offre Cloud π Native et prend contact avec le programme pour cadrer ma conception

Je souscris à l'offre
Je précise les quotas dont j'ai besoin

J'initialise
l'environnement de mon projet

Je déploie en continue
les évolutions et supervise mon produit numérique

< 5 jours : accès à un cluster, pipeline

< 2H

Sans impact client
Homologation en continue

Auto-formation
Service teams (devops)
mutualisée/ dédiée

< 6 mois : premier incrément viable de l'application (MVP)

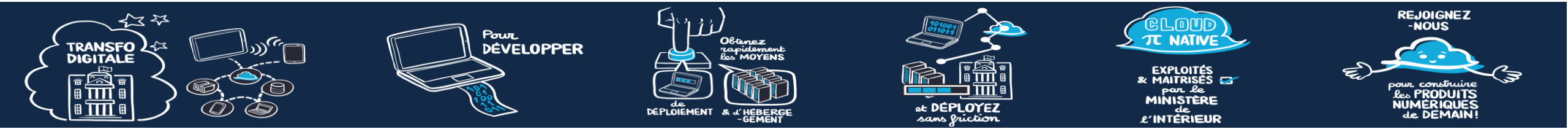
MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

L'offre Cloud π Native – à qui s'adresser?

Derrière l'offre, ces outils, l'organisation, les catalogues… **les équipes sont prêtes à vous répondre** et mettent régulièrement à jour la documentation pour vous permettre de mieux la comprendre

- **Mission :** développement de l'offre en agilité
  - **Clients accompagnés ou expérimentateurs:** 20 en cours (MIOM, MEAE, MinArm, MJ,….)
  - **Développement de l'offre:** nouvelles fonctionnalités, refontes, consolidation
- **Document, CCT, embarquement/formation**: ouverts en open source
- **Contact**: cloudpinative-relations@interieur.gouv.fr, salon Tchap

  - **Equipes: 30 personnes** (dont Cloud π et centre d'hébergement)
    - **Direction programme:** Éric Tiquet (DSO), Fréderic Massieu (Cloud π)
    - **Socle:** fonctionnalités et performances de l'usine logicielle
    - **Service team et adoption**: accompagnement des projets clients
    - **Exploitation**: mise en place et maintien des clusters
    - **Octant:** automatisation de la chaine de service (réseau, flux, cloud, …) avec le BACI
    - **Canel:** cartographie applicative



MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Conclusion

1. **« Cloud π Native » : réponse au besoin de transformation numérique**
2. **S'appuie sur la stratégie « cloud au centre »**
3. **Capitalise sur l'état de l'art « cloud native »**
4. **S'intègre à la trajectoire du MIOM**
    - Proposer un socle de production attractif, à l'état de l'art
    - Assurer la sécurité et la souveraineté
    - Permettre l'ouverture et l'innovation (notamment IA)
    - Renforcer la transversalité (coopération, autonomie)
    - Adéquation des fins (besoins) et des moyens (ressources)