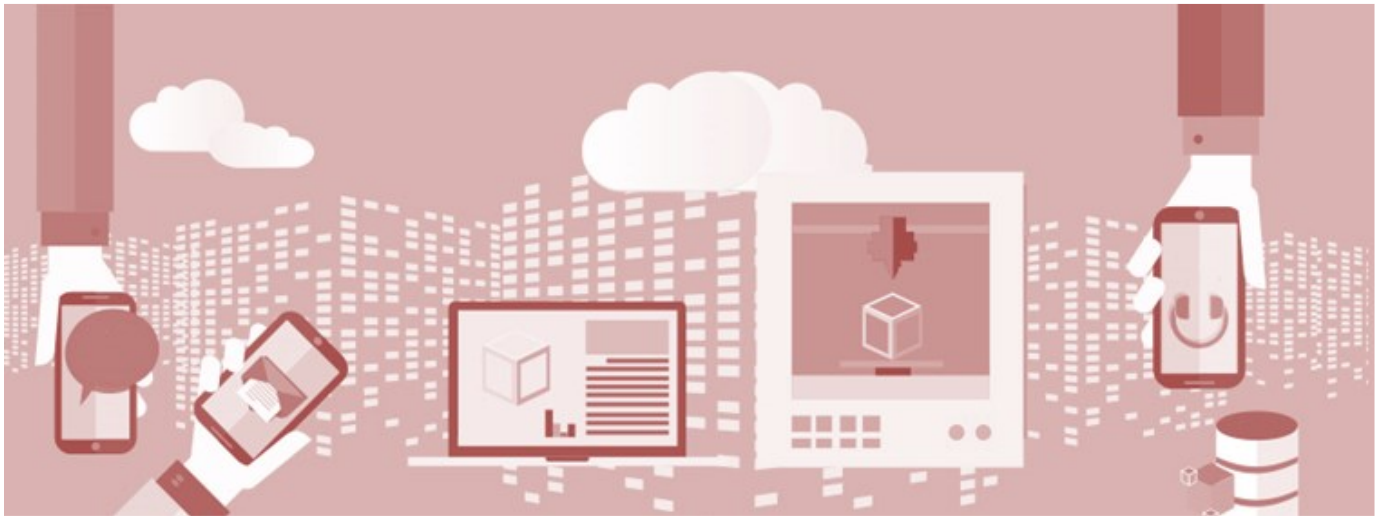


Conférence DSI 24
Sur les enjeux de cyber sécurité

LES ARCHITECTURES NUMERIQUES EN ENTREPRISE

Alexandre SEUNES
a.seunes@gmail.com
www.linkedin.com/in/alexandre-seunes

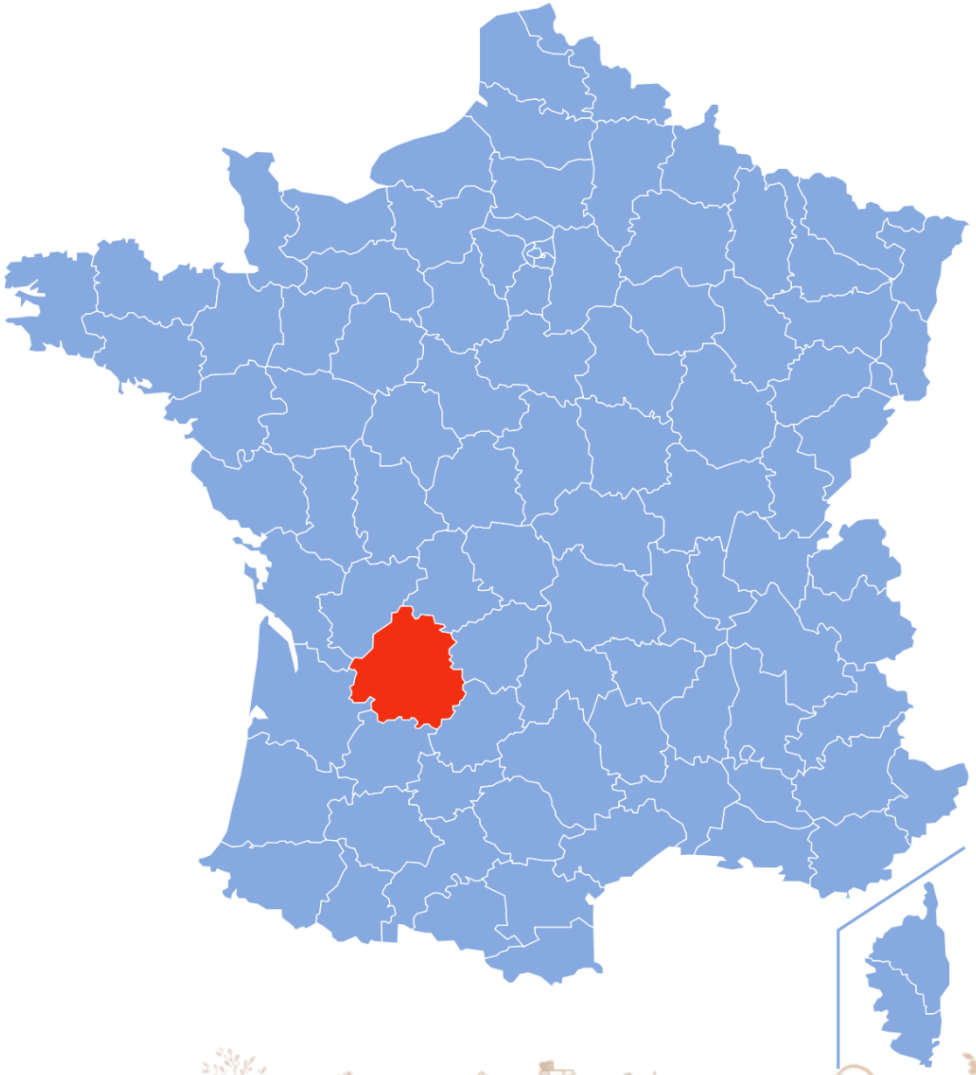
LES ARCHITECTURES NUMERIQUES EN ENTREPRISE

- Introduction : Le contexte du Département
- La transformation numérique des entreprises et des territoires

- Sujets abordés :
  - Délivrer des services numériques disponibles, sécurisés et performants
  - L'hybridation des SI : Cloud – On Premise – SAAS
  - La gestion des identités : Présentation des annuaires, des mécanismes d'authentifications
  - L'impact du RGPD : Construire, développer « Protection by design et Security by design »
  - Enjeux de la méthode « Devops »

- Exemple du schéma Directeur du Numérique des Collèges
- Exemple avec le projet stratégique Lascaux 4

Département de la Dordogne & Contexte CD24



Habitants : 415 000
Superficie : 9060 km²

Agents CD24 : 2750 agents
160 sites informatisés

38 collèges
14800 élèves
1700 enseignants

40 agents à la DSI

CD24 – Contexte

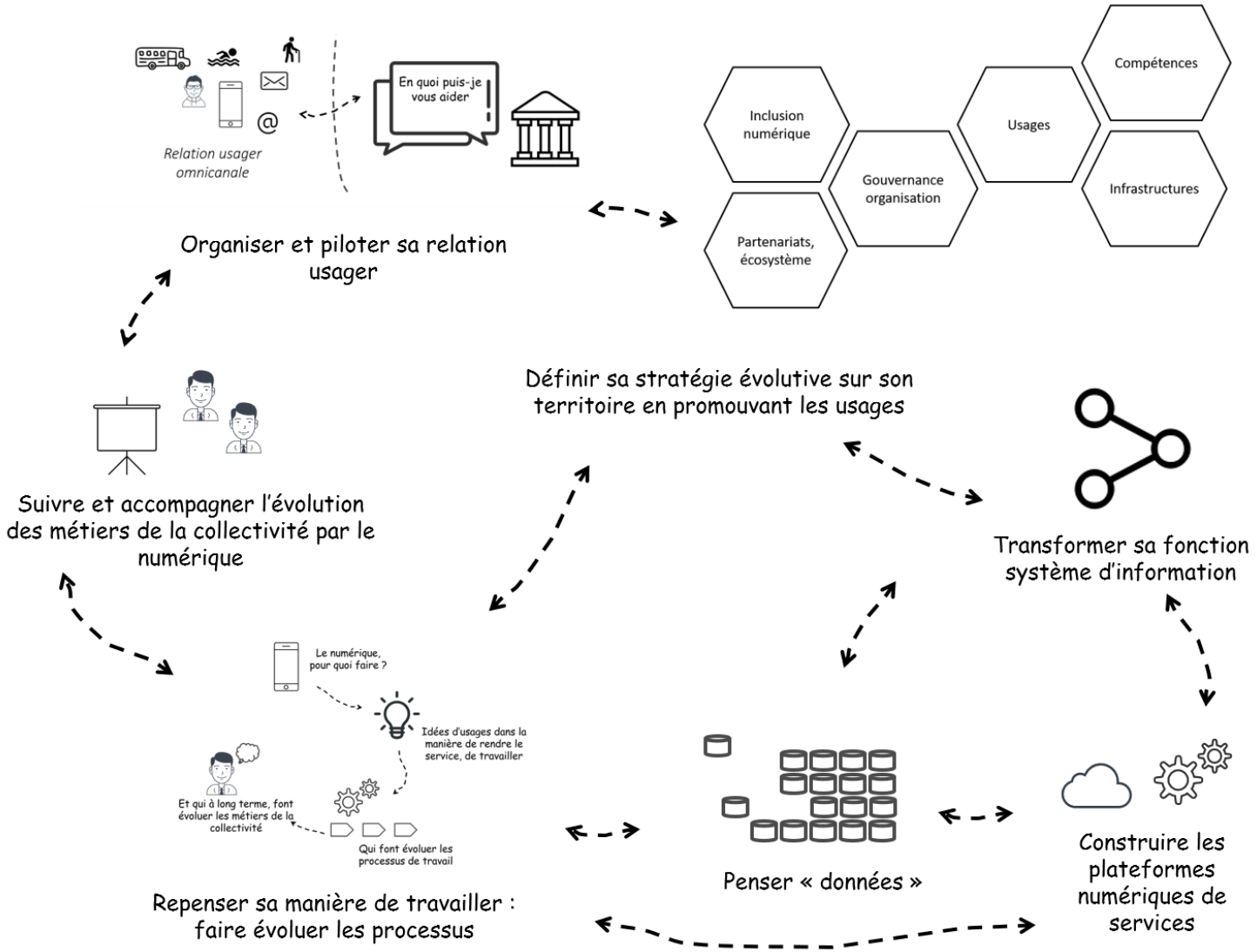
- Démarche de certification – Cours des comptes (M52 > M57)
- **Dématérialisation** de la chaîne comptable – 1 janvier 2019
- **Dématérialisation** du courrier et des dossiers
- Prise en charge compétences collèges (**assistance et maintenance informatique**) : Loi de refondation de 2013
- Mise en œuvre d'une **plateforme numérique territoriale**
- Schéma départemental **d'inclusion numérique**
- Renforcer l'attractivité du territoire

- La transformation numérique des entreprises et des territoires

- Dossier expert réalisé avec :
  - **Cédric Masera**
  - Gérard Briard
  - Armelle Gilliard
  - Alexandre SEUNES

LA TRANSFORMATION NUMÉRIQUE (TN) DE LA COLLECTIVITÉ

- Vision d'ensemble un ensemble de changement qui concernent la fonction SI



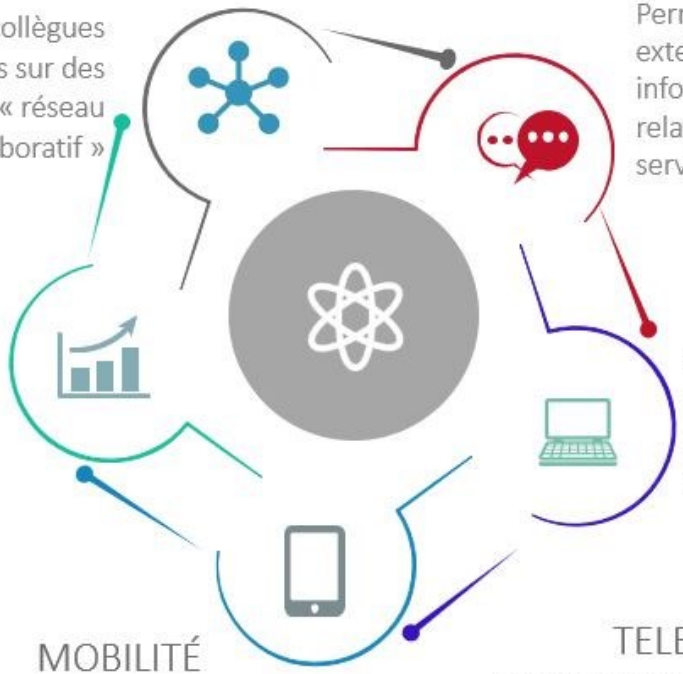
Impact de la transformation numérique

COLLABORATIF - RÉSEAU SOCIAL

Echanger et se connecter avec des collègues ou des partenaires externes sur des plateformes dédiées de type « réseau collaboratif »

GESTION DE LA RELATION USAGER

Permettre aux usagers (internes et externe) de disposer d'une information complète sur les relations d'un usager avec les services



BIG DATA ET OPEN DATA

Consolidation, ouverture et traitement d'une masse inédite de données produites par une diversité de sources, nouveaux services par la donnée (territoire/ville intelligente)

.

DÉMARCHES EN LIGNE

Permettre aux usagers externes d'accéder à des informations et des services en ligne et d'être acteurs du service public

MOBILITÉ

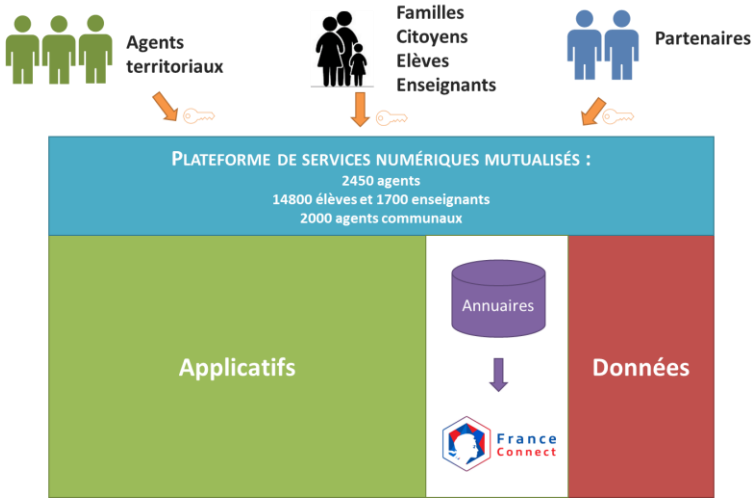
Offrir aux agents la possibilité de consulter et d'alimenter des bases métiers sur le terrain

TELETRAVAIL

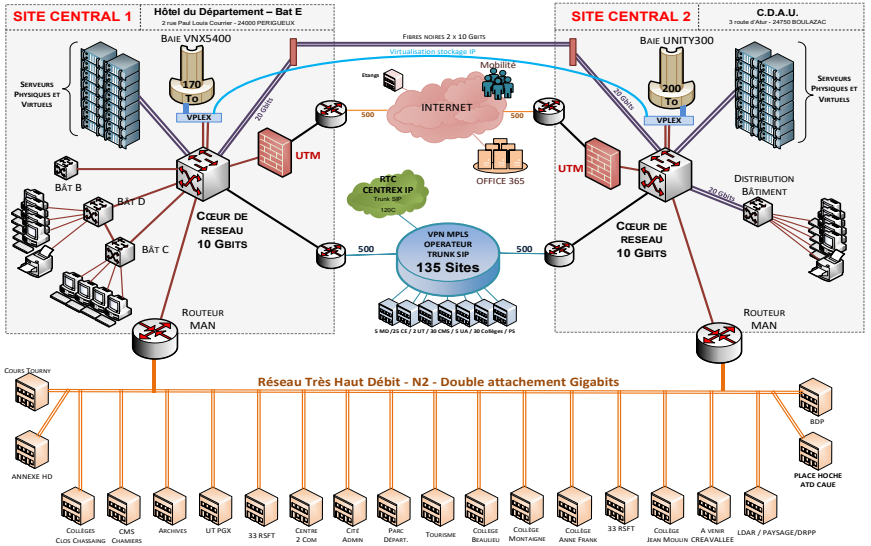
Accès au système d'information de la collectivité à distance
Maintien de l'activité en cas de crises

Offre de service numérique départementale

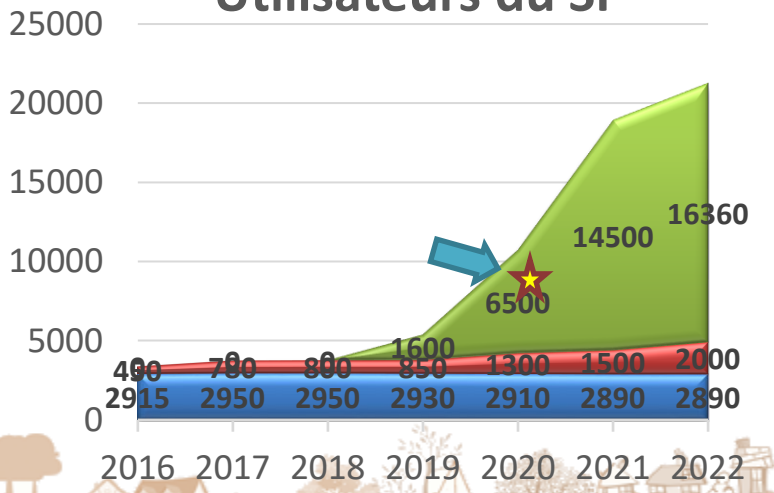
Plateformes départementales



Résiliences techniques (PRA)

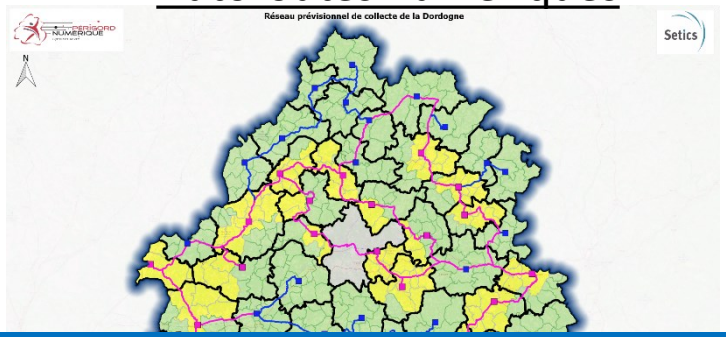


Utilisateurs du SI



Dépendance au THD

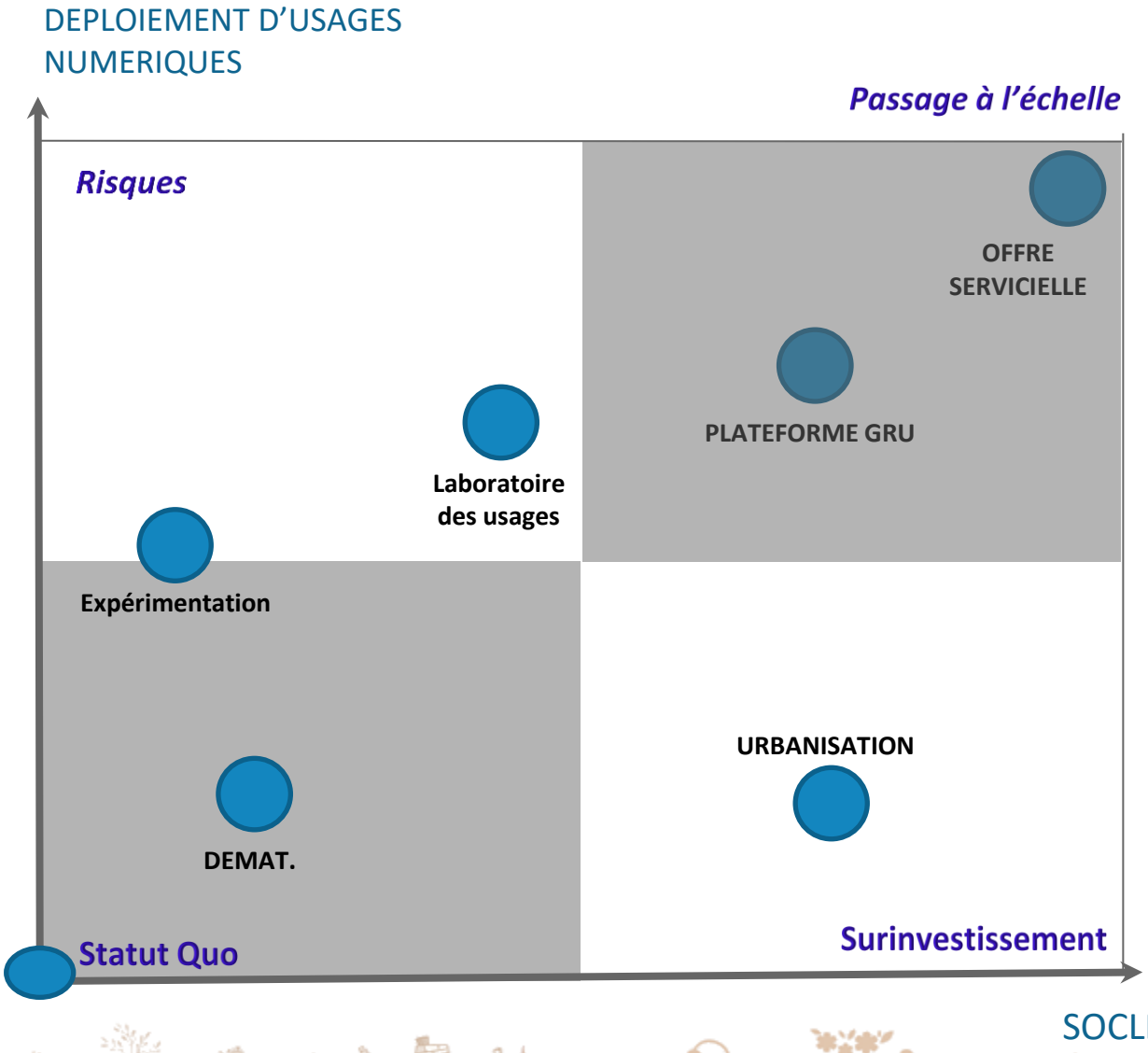
Autoroutes numériques



Autant que sur les enjeux d'hébergement des services numériques il faut anticiper et valider la **résilience des réseaux opérateurs**

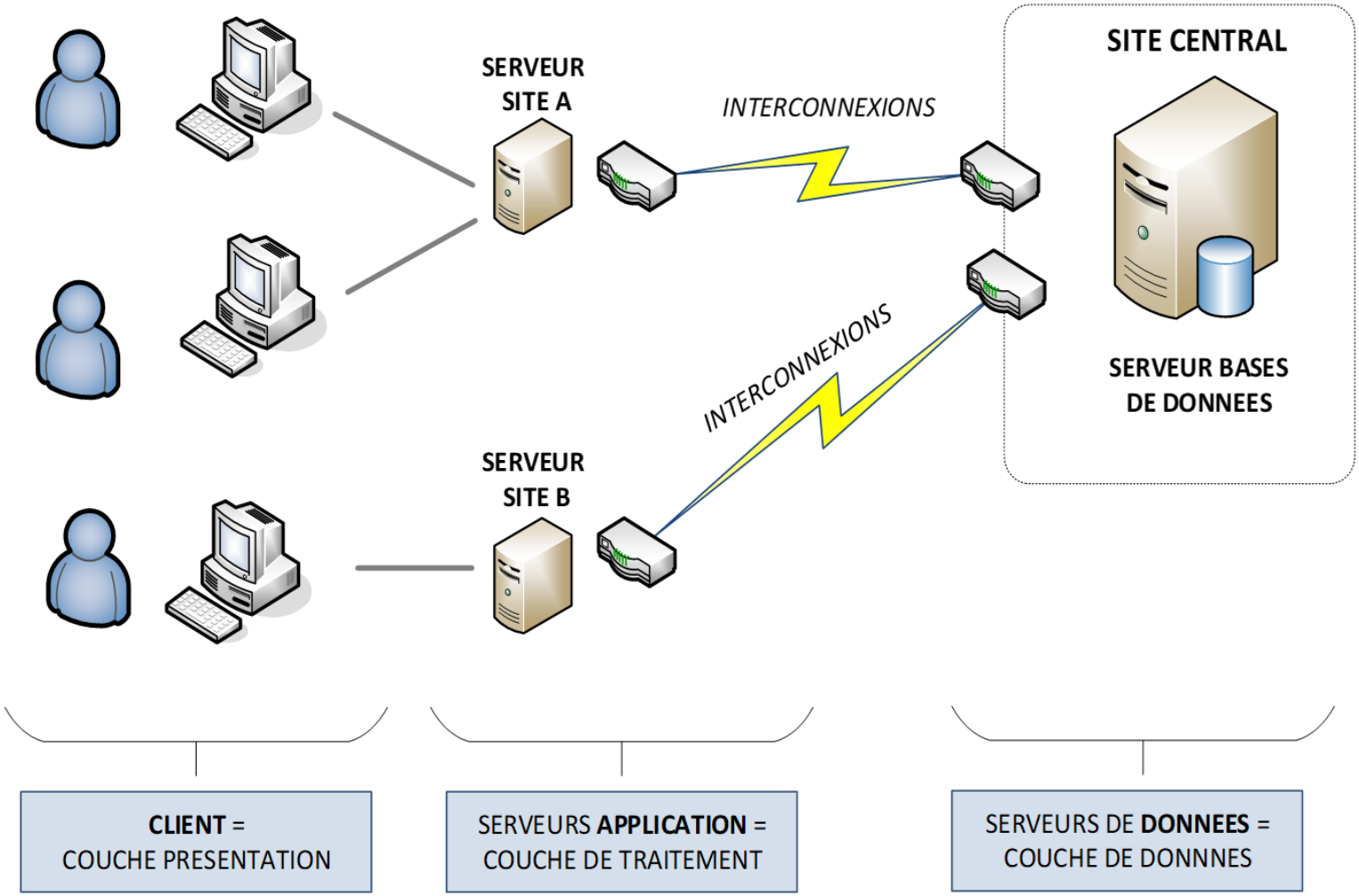
Les territoires sont souvent très dépendants des réseaux opérateurs des métropoles (dans notre cas Bordeaux Lac)

Matrice Usages / Socles



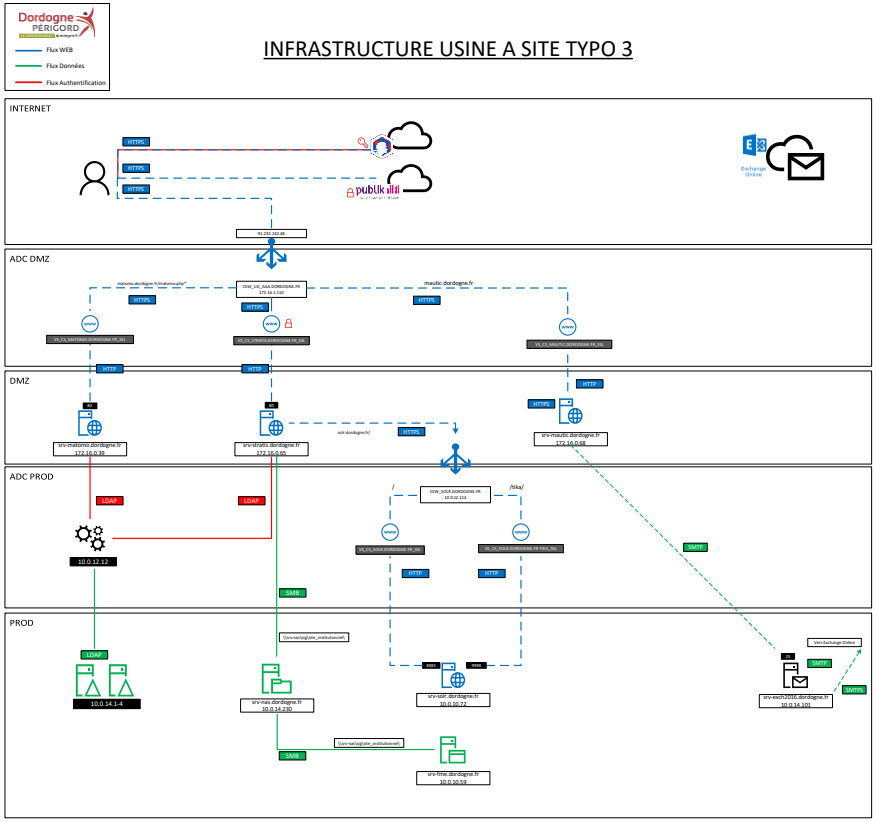
- Délivrer des services numériques disponibles, sécurisés et performants

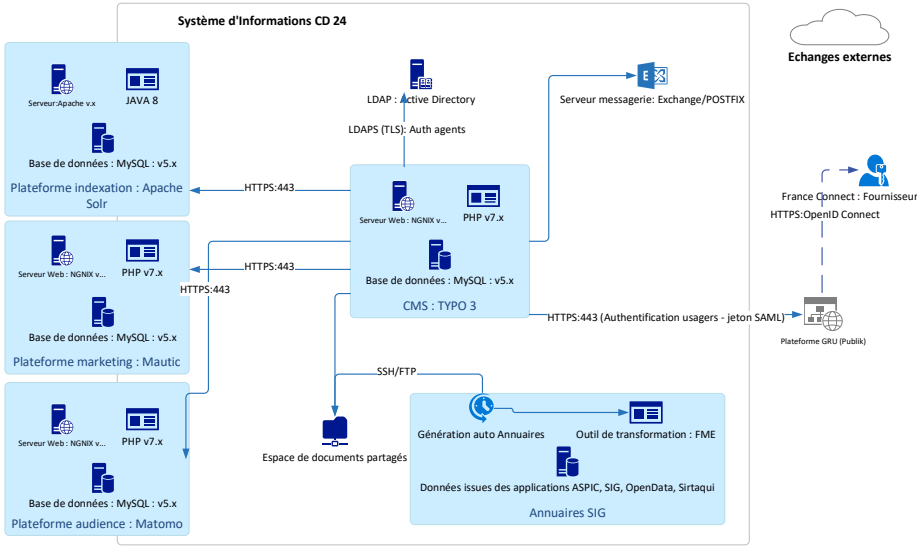
Les architecture 3 tiers n'existent plus … (ou presque plus)



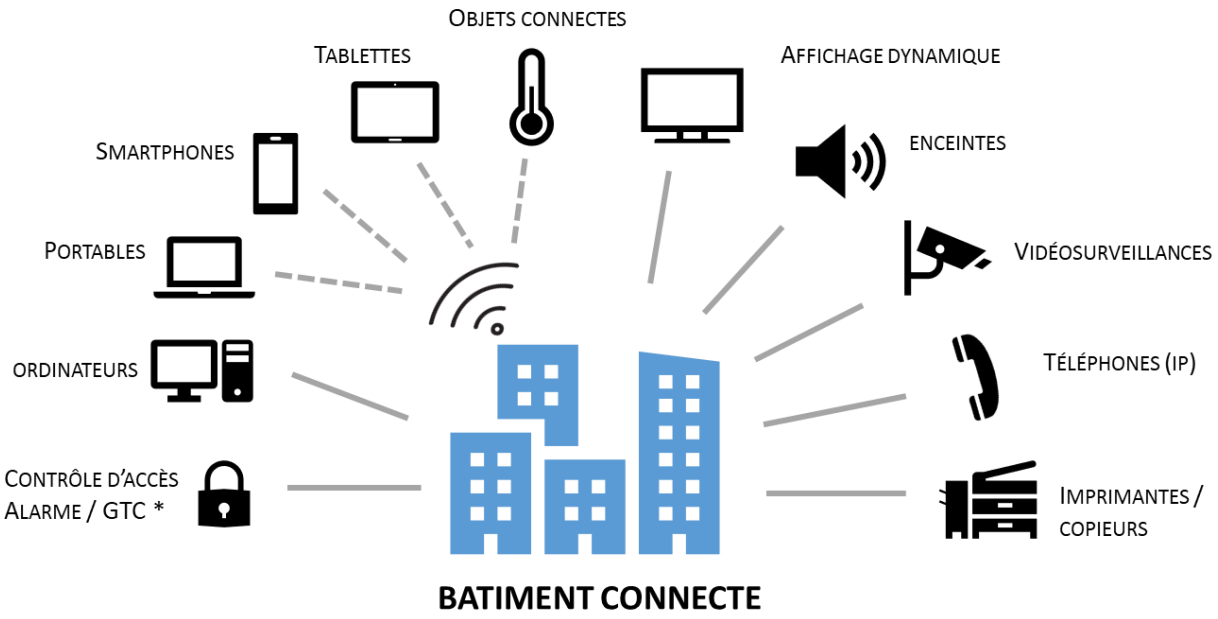
Les architectures sont désormais n-tiers, réparties

→ Complexes
→ Interopérés
→ Dépendantes

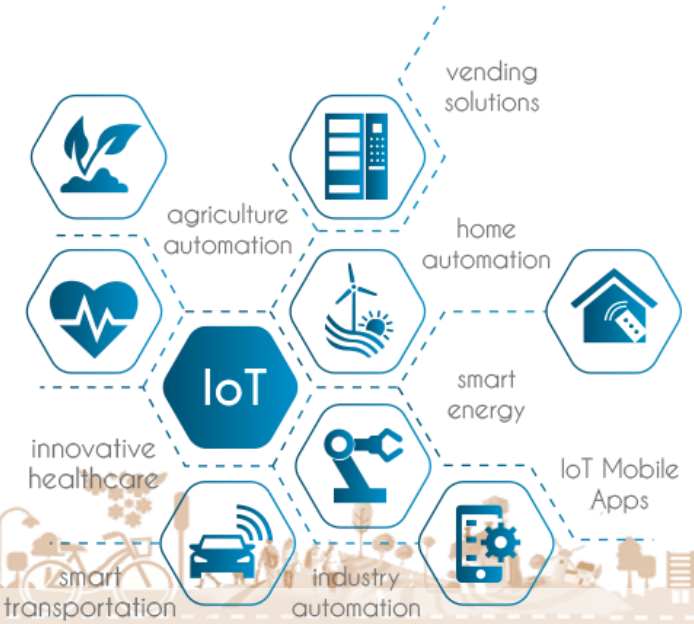




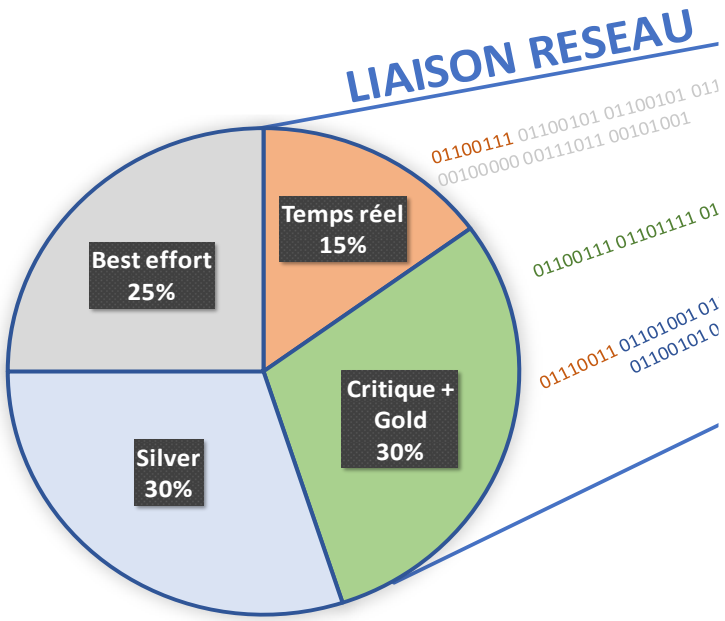
Aujourd'hui il faut penser des bâtiments connectés ….



… des objets connectés (iot)…



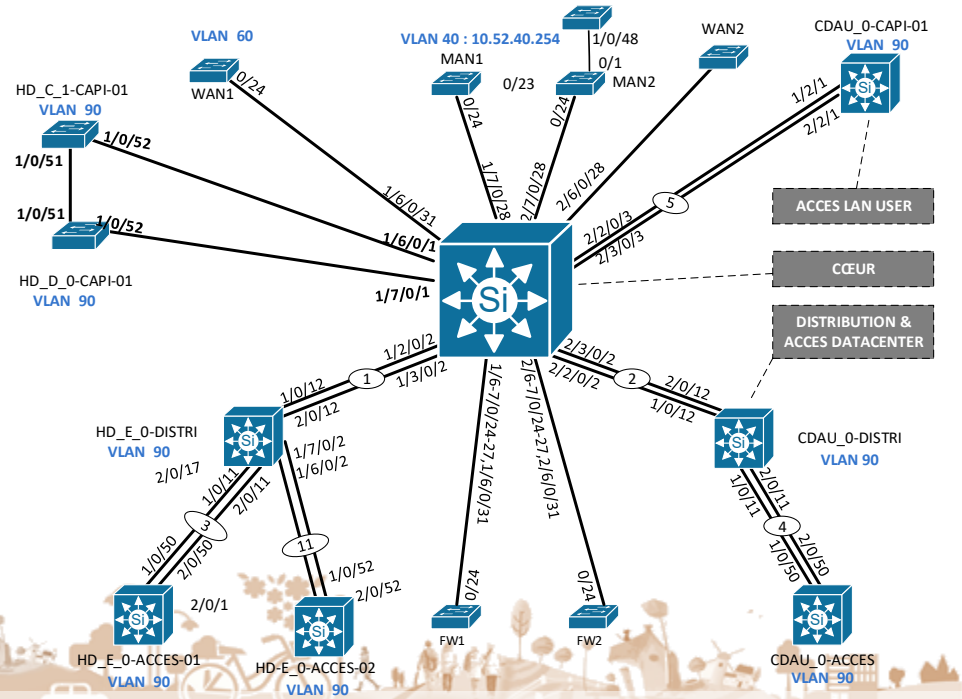
… à des multiples réseaux de plus en plus intelligents…



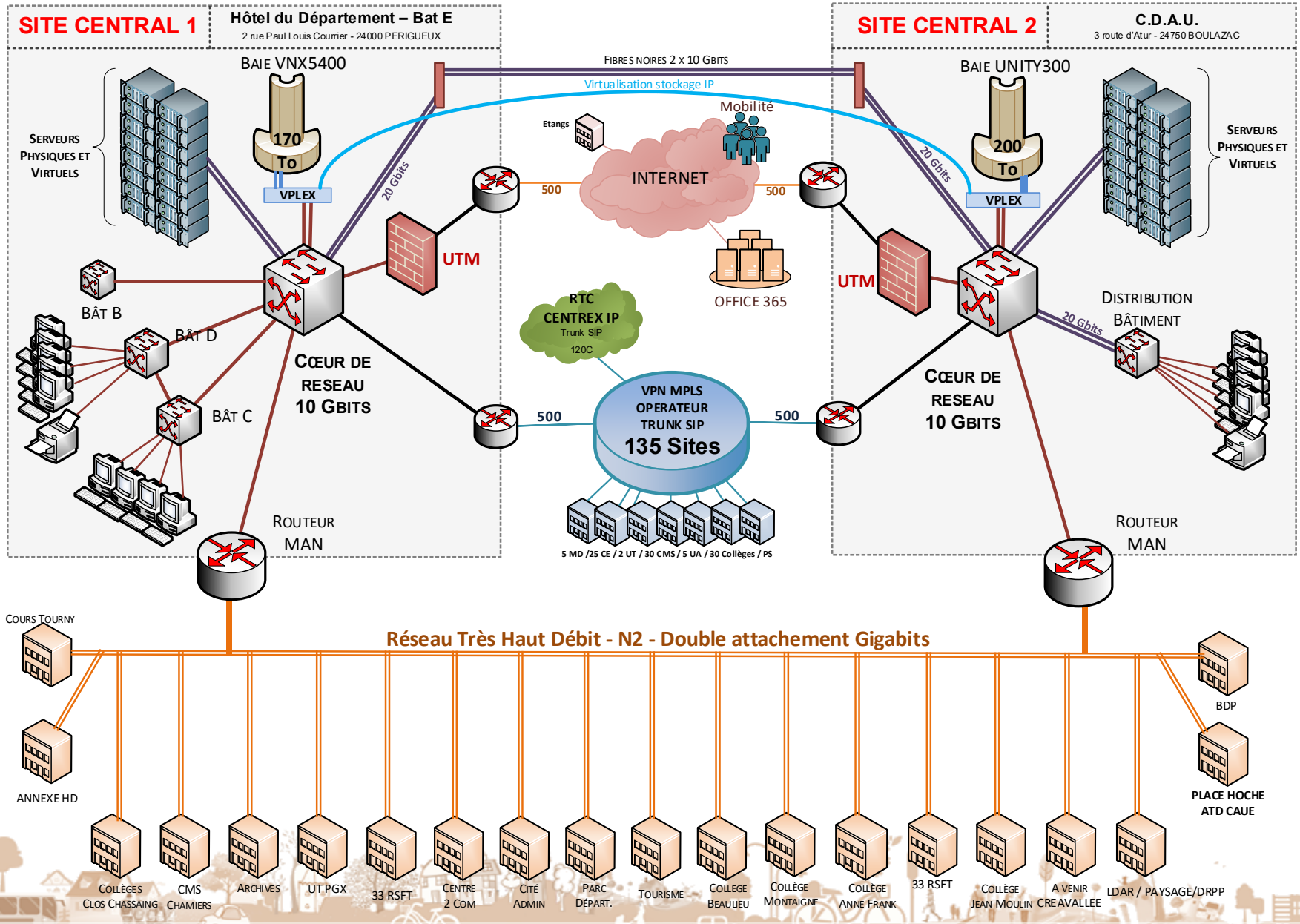
Les réseaux doivent prioriser en fonction des usages :

- Voix / video
- Streaming
- Transactionnel
- Best effort …

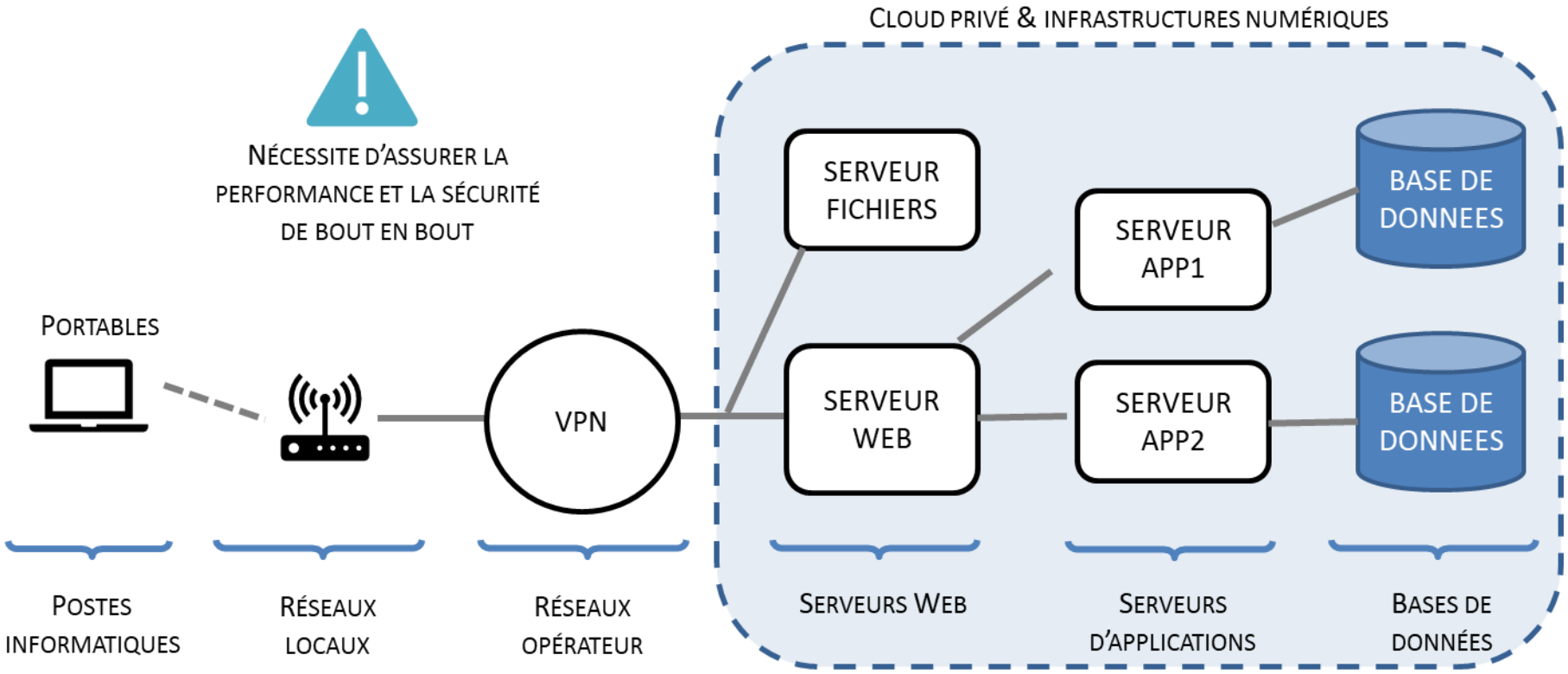
De plus en plus résilient et « intelligent »



… à des usines numériques



Maitriser un SI : Il faut une vision de bout en bout

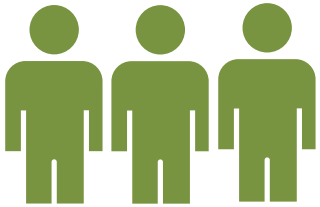


Performance

Disponibilité

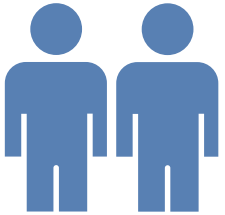
Sécurité

Construire des plateformes de services numériques



Agents territoriaux

Familles
Citoyens
Elèves
Enseignants

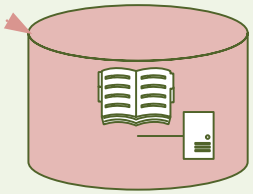


Partenaires

PLATEFORME DE SERVICES NUMÉRIQUES MUTUALISÉS :

2450 Agents
14800 élèves et 1700 enseignants
900 Agents communaux

Cloud Privé

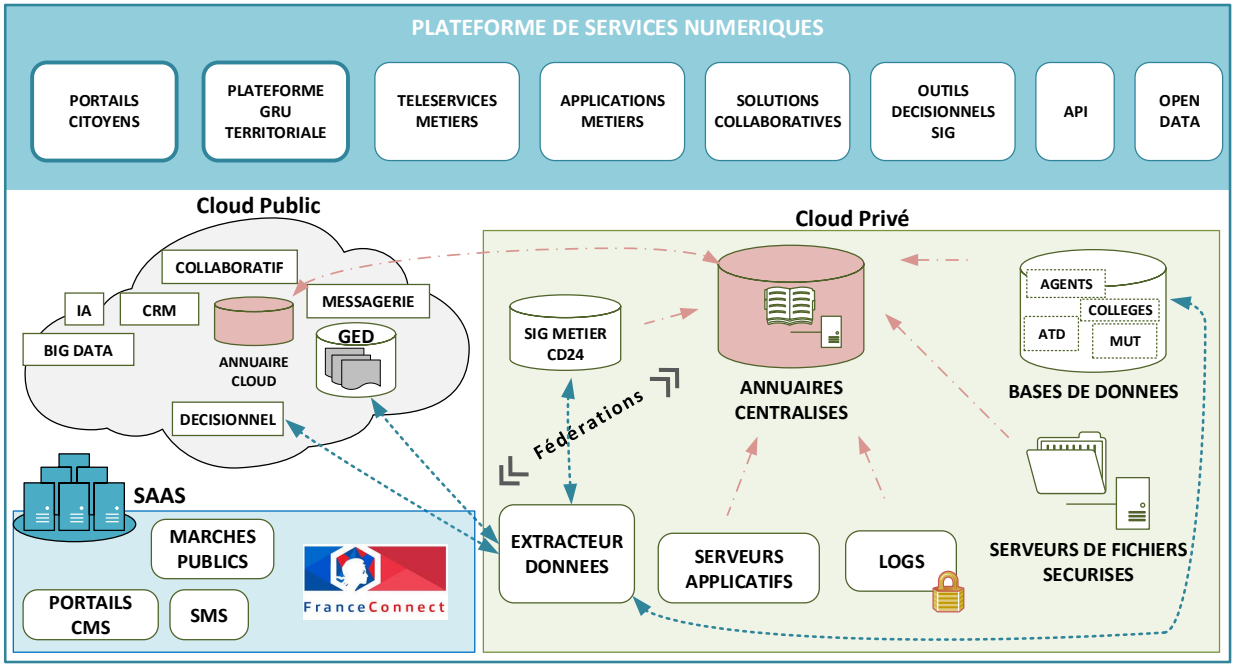


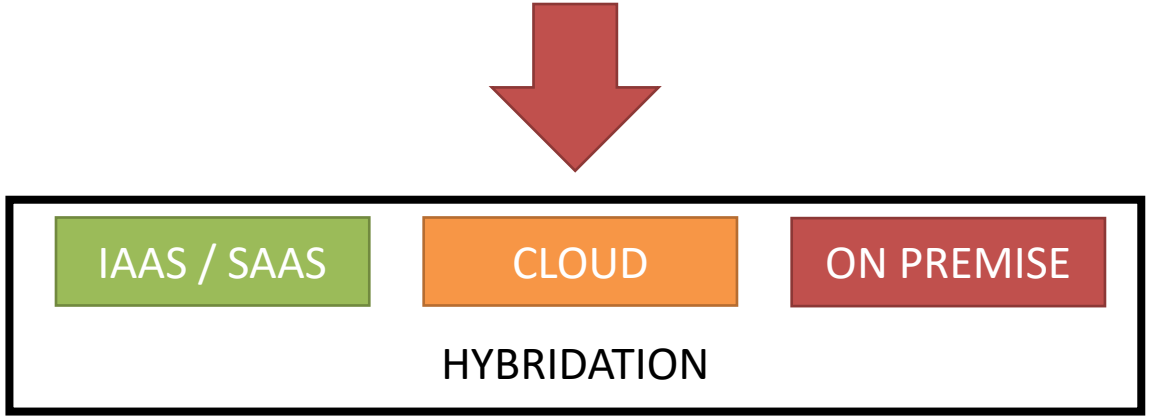
ANNUAIRES CENTRALISES

Applicatifs

Données

Ces plateformes doivent s'appuyer sur différents hébergements de services numériques

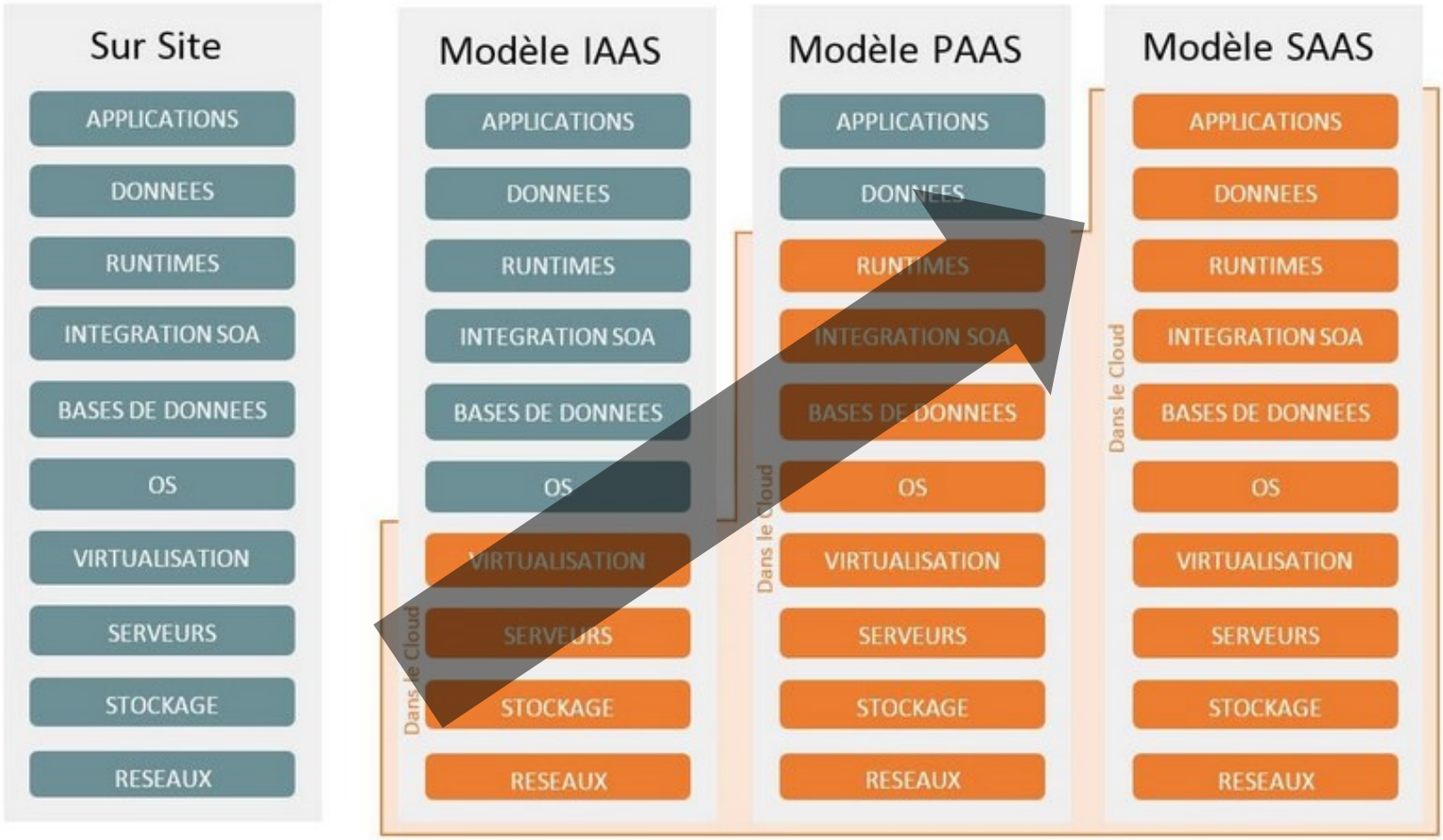




L'utilisateur ne doit pas savoir et encore moins avoir à comprendre s'il passe d'une solution d'hébergement à une autre.

Expérience utilisateur transparente

Modèle externalisation



Sur site = On Premise (en anglais)

IAAS : Infrastructure As As Service

PAAS : Plateforme As As Service

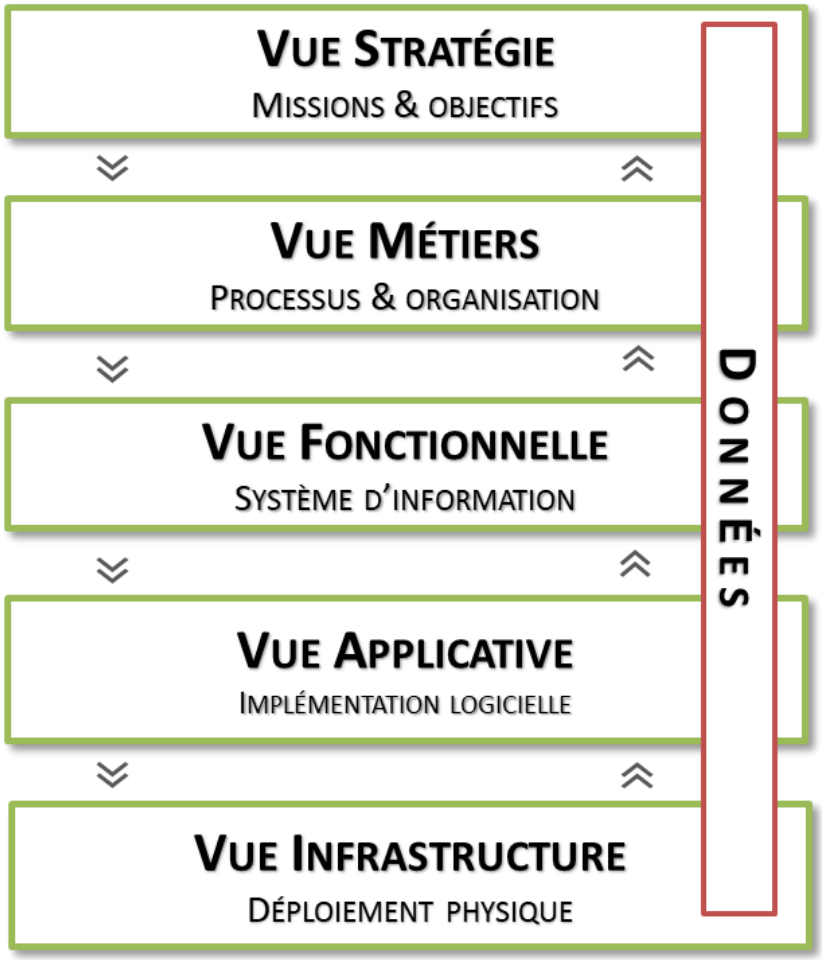
SAAS : Software As As Service

Urbaniser et industrialiser son SI

L'urbanisation du système d'information est un concept connu pour les DSI dont la représentation la plus fréquente est celle présentée ci-contre.

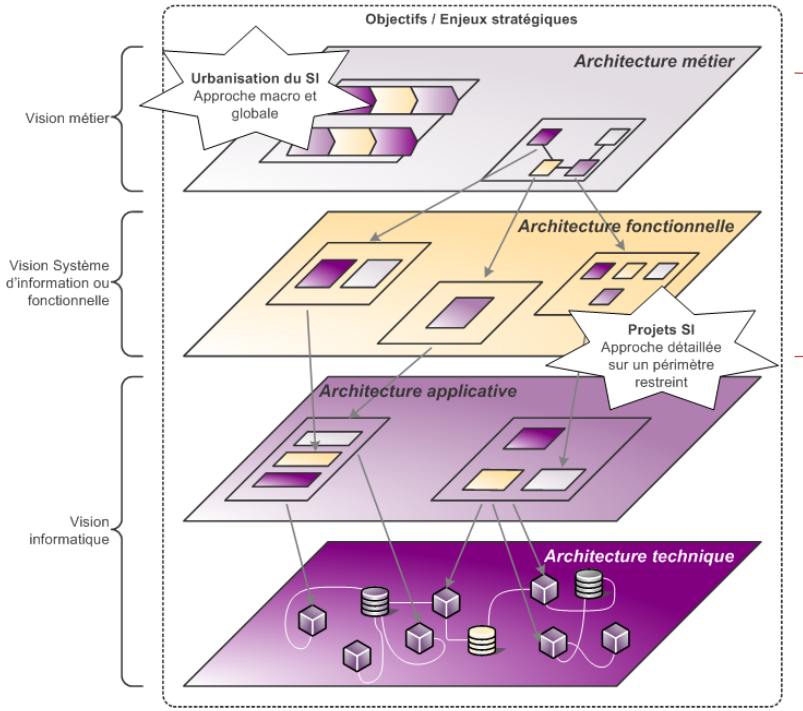
Elle consiste à faire évoluer le système d'information en fonction de la stratégie de l'entreprise et à chercher des optimisations à toutes les échelles :

- Métiers
- Fonctionnelles
- Applicatives
- Infrastructures



Urbaniser et industrialiser son SI /2

Le terme « urbanisation » est utilisé par analogie avec les travaux d'architecture et d'urbanisme dans une ville en comparant l'organisation d'une entreprise ou une collectivité avec une ville et ses différents quartiers, zones et *blocs*.



Pour urbaniser, un préalable indispensable est de créer un référentiel cartographique qui centralisera par couches :

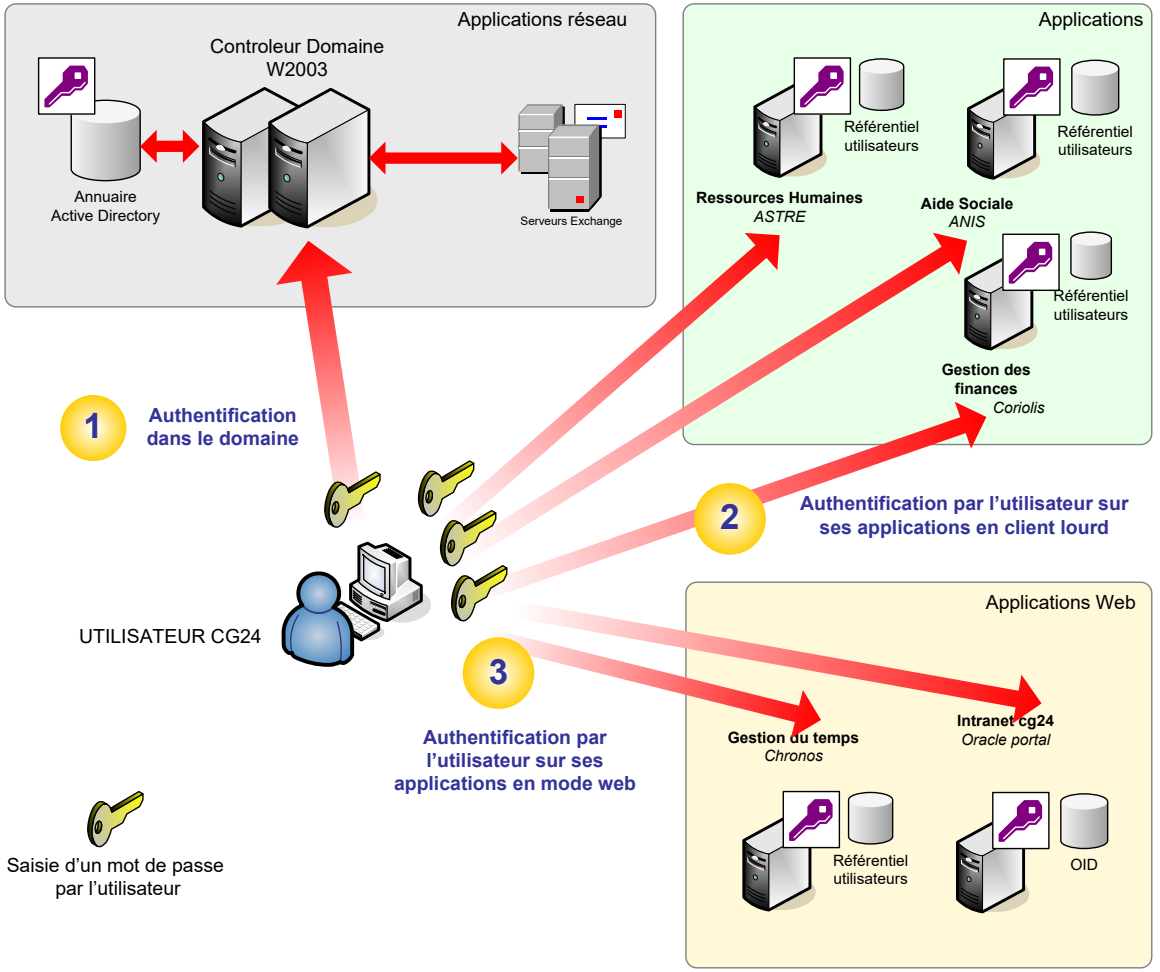
- la stratégie avec les missions et les objectifs ;
- les métiers avec la description des organisations et la rédaction des processus ;
- les enjeux fonctionnels ;
- et enfin les applications et les intégrations infrastructure.

Complexe ! Mais de plus en plus indispensable pour une entreprise avec le RGPD

Infographie reprise sur https://blog.xebia.fr/2008/04/10/urbanisation-pour-

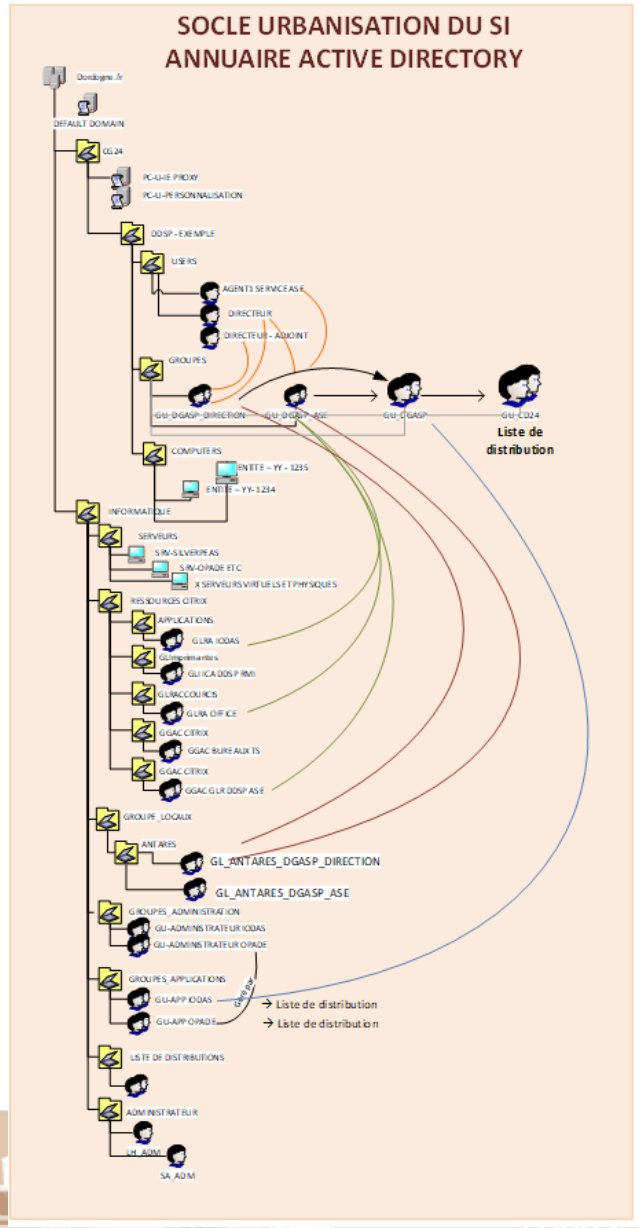
La gestion des accès au SI

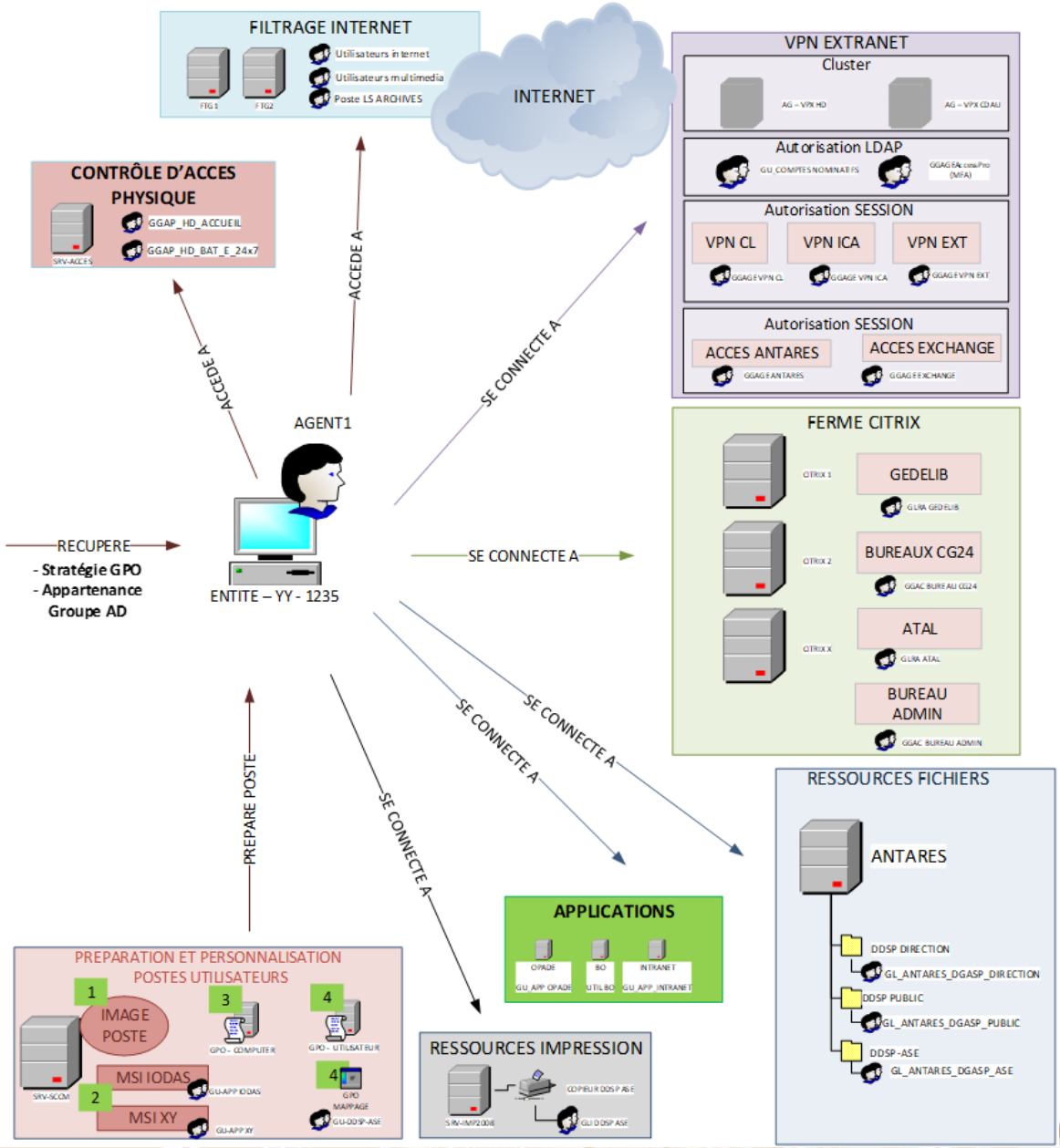
Le terme « urbanisation » est utilisé par analogie avec les travaux d'architecture et d'urbanisme dans une ville en comparant l'organisation d'une entreprise ou une collectivité avec une ville et ses différents quartiers, zones et *blocs.*



Gestion des identités
Multiplicité des accès
Risques

Annuaire d'entreprise



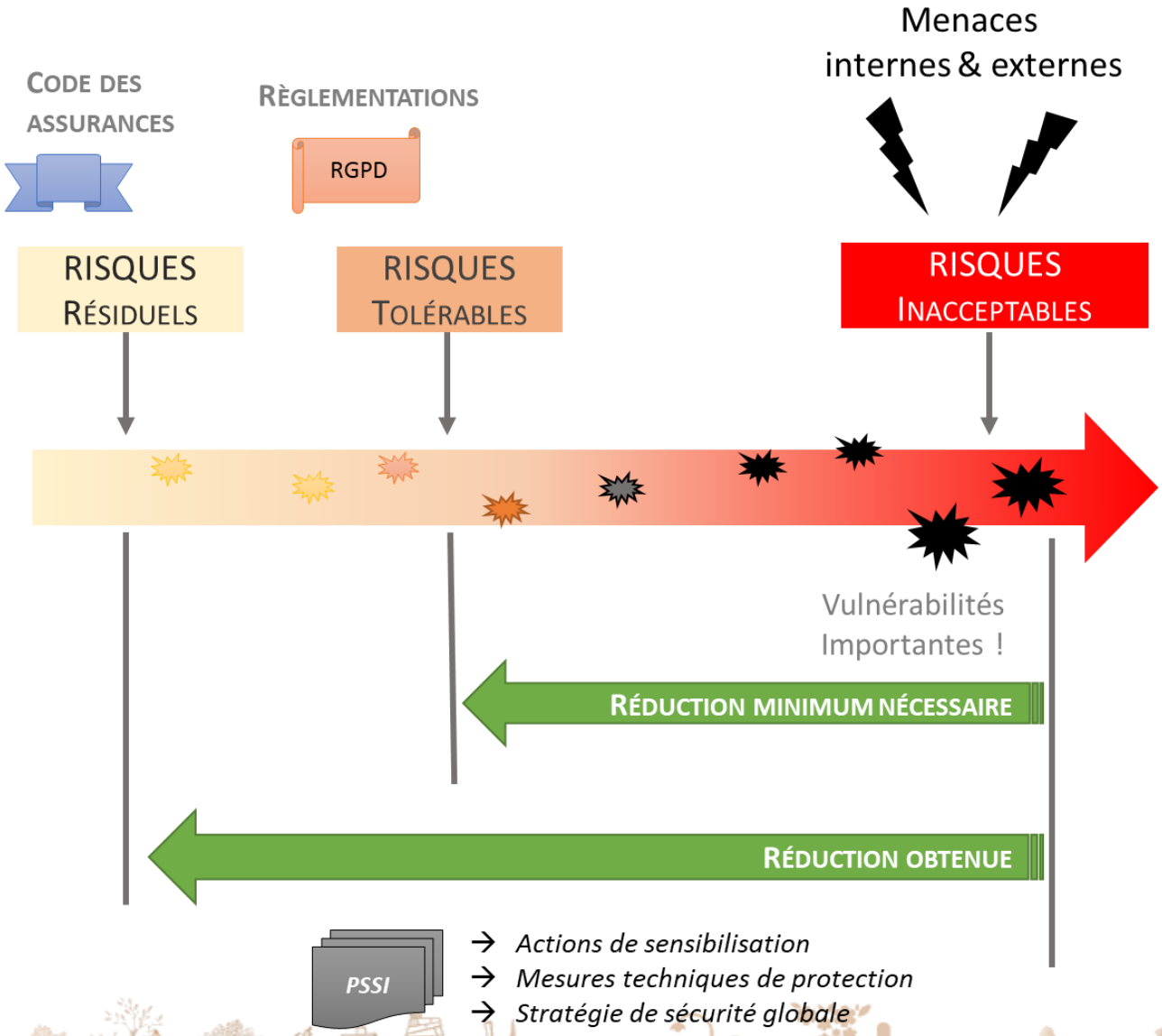


- Sécurité des Systèmes d'Information

Comment faire ?

SSI : Le périmètre du SI :

SSI – Etape 1 : Appréhender les risques



SSI - Analyse des risques – Quels dommages possibles ?

REFERENTIEL DE CONSEQUENCES / Critères de risque

CLASSE DE CONSEQUENCES ou NIVEAU DE GRAVITE	PERIMETRE DES DOMMAGES				
	DOMMAGES JURIDIQUES	DOMMAGES A L'IMAGE	DOMMAGES FINANCIERS	DOMMAGES AU FONCTIONNEMENT DES SERVICES	DOMMAGES AUX USAGERS, AUX TIERS
CRITIQUE	Incidence réglementaire engageant les responsables devant un tribunal pénal	Campagne médiatique hostile (journal de 20h,Twitter, Facebook, Radio nationale). Perte de confiance durable.	Perte au-delà de 50 K€ ou Perte au-delà de 50 jh	Désorganisation durable non-maîtrisée d'un ou plusieurs processus engageant gravement la responsabilité da collectivité	Atteinte à la santé ou à la vie de l'usager ou d'un citoyen (atteinte à la santé publique,...).
TRES IMPORTANT	Incidence réglementaire engageant les responsables devant un tribunal administratif ou civil, impliquant des frais de procédure et/ou de dédommagement.	Perte de crédibilité temporaire de la collectivité vis-à-vis des partenaires, des médias et des citoyens.	Perte de 5K€ à 50 K€ ou Perte de 6 à 50 jh	Perturbation de plusieurs processus remettant en cause le respect des échéances ou la conservation d'une accréditation ou d'un contrat	Préjudice socio-économique collectif , association, personne morale, ...(subvention non versée, atteinte à la vie privée) entrainant des plaintes formalisées.
IMPORTANT	Sanction d'une autorité administrative pour non respect de la loi.	Perte de crédibilité partielle d'une direction par rapport à des usagers internes	Perte jusqu'à 5 K€ ou Perte de 2 à 5 jh	Perturbation d'un processus ne remettant pas en cause le respect des échéances.	Préjudice socio-économique individuel entrainant une plainte formalisée d'une personne morale ou physique
FAIBLE	Mise en demeure par une autorité administrative pour non respect de la loi.	Perte de crédibilité d'un agent par rapport à des usagers internes	Perte quelques milliers d'€ ou Perte de 1jh	Mécontentement non formalisé d'un ou plusieurs utilisateurs	Mécontentement non formalisé d'un ou plusieurs usagers.

SSI - Analyse des risques – Exemples

COLLECTIVITE		Indisponible jusqu'à						Défaut Intégrité		Perte de Confidentialité		Fraîcheur des données (RPO / PMDA)
Nom de l'application	Descriptif de l'application	1h	4h	24 h	3 jours	14 jours	Présence d'un mode dégradé	Données inexactes incomplètes	Paternité contestable	Fuite Interne	Fuite externe	
IODAS	Gestion aide sociale	Fonctionnement	Fonctionnement	Fonctionnement	Fonctionnement	Juridique	Doc simple	Juridique	Juridique	Juridique	Juridique	1 heure
CORIOLIS	Gestion financière		Financier	Financier	Financier	Usagers/Tiers	Système D	Usagers/Tiers	Juridique	Juridique	Juridique	24 heures
MESSAGERIE	Mail, Calendriers ...	Fonctionnement	Fonctionnement	Fonctionnement	Fonctionnement	Fonctionnement	Doc simple	Image	Image	Juridique	Juridique	1 heure
PROGOS	Gestion subventions		Fonctionnement	Image	Image	Fonctionnement	Système D				Image	24 heures
SITE CD24	site institutionnel			Image	Image	Fonctionnement	Système D	Juridique	Juridique			24 heures
ESST	Analyse de la vache folle	Usagers/Tiers	Usagers/Tiers	Usagers/Tiers	Usagers/Tiers	Usagers/Tiers	Non	Usagers/Tiers	Usagers/Tiers		Usagers/Tiers	4 heures
AWS	Plateforme Gestion des marchés publics	Fonctionnement	Fonctionnement	Juridique	Juridique	Juridique	Non	Juridique	Juridique			

Avec ce type de démarche, on repositionne le métier au centre

Un SI > qui sont les clients ? Quels niveaux de service ?

Quels niveaux de service exigé en cas de sinistre majeur (incident électrique, incendie, inondation, etc.) ?

Ci-dessous l'exemple d'une analyse : « Etat des lieux » → « Propositions »

	ENTRETIEN	OBJECTIFS PROPOSES
Administration interne : agents [redacted] Métropole et des communes (représente 80 %)	5 jrs	24 h
Service à l'usager : état civil, service administratif, billettique (piscine : musée / zoo)	48 h ?	24 h
Informatique industrielle : service de l'eau, gestion technique bâtimentaire, bus à haut niveau de service, signalisation	8 h ?	24 h*
Sécurité & Vidéosurveillance : police municipale avec le système de Radio Téléphonie Numérique (Talkie/Walkie Hertzien - Système TETRA)	0 h	8 h *
Ecoles : annuaire / sécurité / impression / ressources réseaux	5 jrs	24 h

- Politique de Sécurité des Systèmes d'Information
- Homologation Sécurité

S'appuyer sur des référentiels et des normes

- OWASP : https://www.owasp.org
- Référentiel Général de Sécurité par l'ANSSI : https://www.ssi.gouv.fr/
- La norme ISO/CEI 27002 est une norme internationale concernant la sécurité de l'information

Sécurité des Systèmes d'Information – Ex Tableau de bord

Evolution Maturité SSI 2016-2019

ISO 27002 – CIBLE MATURITE : 3	2016	FEVRIER 2018	JUIN 2018	JANVIER 2019
Chapitre 5 - Politiques de sécurité de l'information	1,00	3,00	3,00	4,00
Chapitre 6 - Organisation de la sécurité et mobilité	1,75	2,65	2,65	2,75
Chapitre 7 - La sécurité des ressources humaines	3,94	4,06	4,06	4,17
Chapitre 8 - Gestion des actifs	1,72	2,00	2,00	2,11
Chapitre 9 - Contrôle d'accès logique	1,92	2,13	2,13	2,48
Chapitre 10 - Cryptographie	2,00	2,00	2,00	2
Chapitre 11 - Sécurité physique et environnementale	2,81	2,86	2,86	2,92
Chapitre 12 - Sécurité liée à l'exploitation	2,32	2,57	3,04	3,57
Chapitre 13 - Sécurité des Communications	2,75	2,88	2,88	3,00
Chapitre 14 - Acquisition, Développement et maintenance des SI	2,41	2,81	2,81	2,81
Chapitre 15 - Relation avec les fournisseurs	1,00	2,17	2,17	2,33
Chapitre 16 - Gestion des incidents liés à la sécurité de l'information	0,14	0,71	0,71	0,86
Chapitre 17 - Gestion de la continuité de l'activité	2,00	2,00	2,17	2,17
Chapitre 18 - Conformité	1,47	1,63	1,83	1,83
	1,94	**2,39**	**2,45**	**2,64**

Avancement PSSI REFERENTIEL ISO 27002

	JUIN 2018	JANVIER 2019
Nombre total de règles applicables	114	114
Nombre de règles prises en compte	**74**	**80**
Taux de règles prises en compte	**64,91%**	**70,18%**
Taux de règles opérationnelles	**85,07%**	**88,78%**

Avancement « Chantier de la culture sécurité »

Actions	Etat	Avancement
PSSI		**Validée - En cours de mise à jour pour 2019**
Charte des utilisateurs		**Validée - En cours de mise à jour pour 2019**
Charte des administrateurs		**Validée et signée**
Charte Prestataires		**Validée et en cours de diffusion**
Sensibilisation		**Session en cours**
Commission d'homologation		**Créée le 12 Novembre 2018**
Plan de Reprise Informatique		**Dernier test le 06 Octobre 2018**

Niveau de Sécurité RGPD

	2018	2019
Nombre total de mesures applicables	52	52
Nombre de mesures finalisées	**25**	**28**
Nombre de mesures en cours de mise en œuvre	**8**	**16**
Nombres de règles à planifier	**19**	**8**

Incidents de sécurité

	2017	2018
Nombres incidents de sécurité	6	7
Impact pour les utilisateurs	5	7
Impact pour les usagers	1	0

Dossiers de Sécurité

	2018	2019
Nombre d'applications concernées	26	36
Nombre de dossiers créés	**7**	**12**
Attestation d'homologation	**0**	**1**

Sessions de Sensibilisation

	2019
Nombre de sessions	11
Nombres de personnes	**440**

SSI – Les homologations

Le principe – Homologation technique

POUR TOUS LES DÉVELOPPEMENTS INTERNES ET NOS CAHIERS DES CHARGES

Nous devons intégrer les enjeux de sécurité par défaut

Pour la mise en production, nous devons appliquer **l'homologation technique** ci-dessous :

HOMOLOGATION TECHNIQUE MINIMUM

- J'utilise uniquement l'identité numérique centralisée et je limite au groupe fonctionnel métier
- Je chiffre entre les équipements utilisateurs et l'application
- Je bloque tous les accès directs aux serveurs et bases de données
- Je supervise et assure la traçabilité
- J'applique une stratégie de sauvegarde adaptée (si externalisation je vérifie le contrat de service)
- Je limite les amplitudes horaires
- J'active des sécurités renforcées

- Je planifie des tests d'intrusion

Le principe en synthèse

HOMOLOGATION TECHNIQUE

+

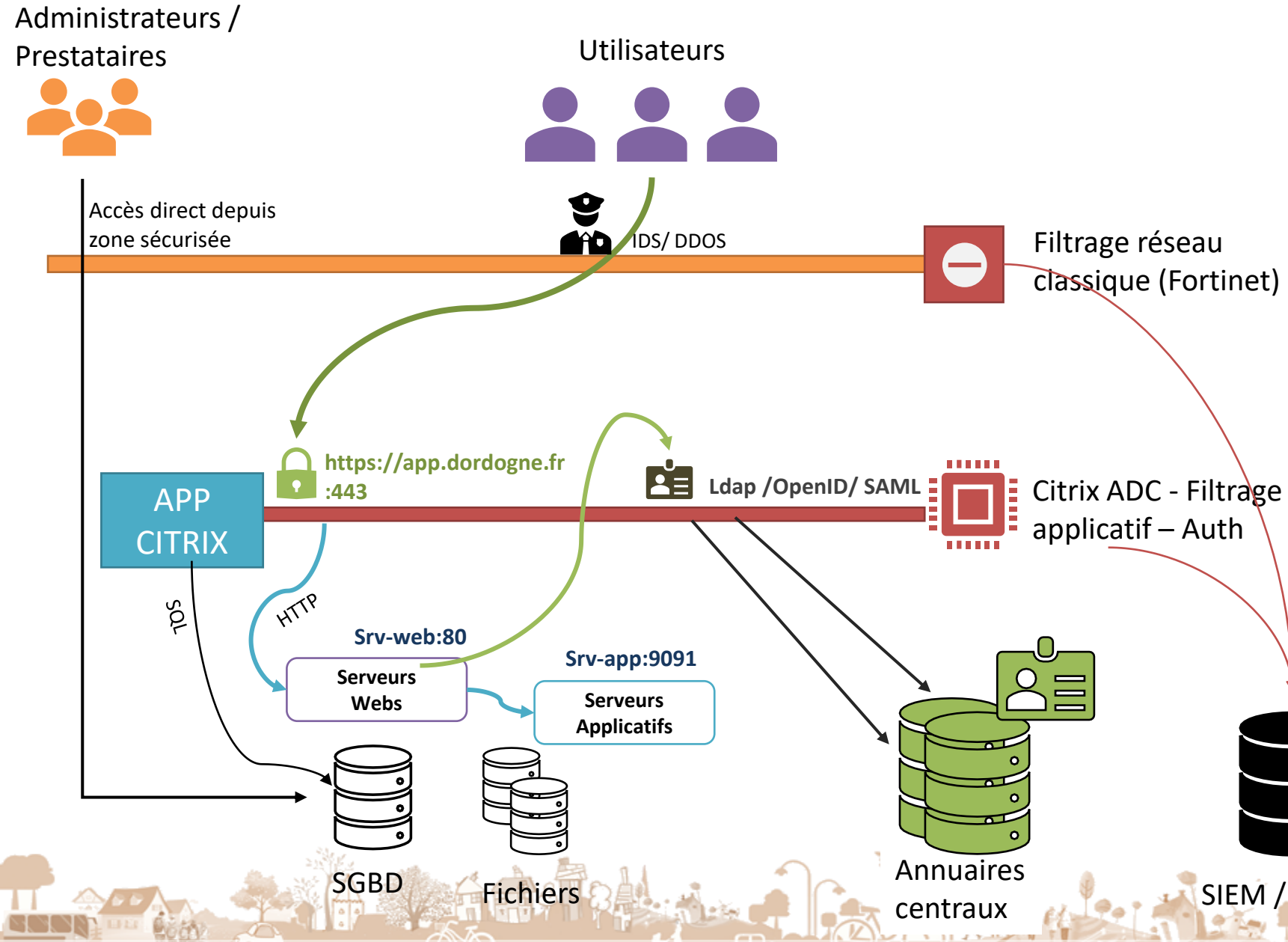
CERTIFICATION COURS DES COMPTES

- Gestion des identités et suivi des habilitations renforcées
- J'applique des contrôles automatiques aux traitements financiers

HOMOLOGATION TÉLÉSERVICES

- Je fais une analyse des risques et si données sensibles une AIPD
- J'applique des actions correctives pour arriver à risque résiduel tolérable
- Un procès verbal est dressé pour autoriser le téléservices

Principe globale d'un point de vue architecture numérique



J'utilise uniquement l'identité numérique centralisée et je limite au groupe fonctionnel métier

- L'application authentifie les utilisateurs avec les annuaires centraux
  - Authentification LDAP
    - Ldap.dordogne.fr port 389 ou préférable 686 en mode sécurisé
  - Authentification SAML / OpenID
    - L'utilisateur est renvoyé vers le portail https://aaa.dordogne.fr et est automatiquement renvoyé vers l'application avec le jeton transmis pour le fournisseur d'identité (ici c'est la solution Citrix ADC)

    → Avantages :

    → SSO pour les utilisateurs

    → Permet de gérer dynamiquement le contexte de connexion de l'utilisateur et au cas par cas activer des sécurités complémentaires (par exemple, exiger un deuxième facteur d'authentification)
  - Authentification Kerberos
    - Désormais, à éviter car moins évolutif et plus dépendant de l'environnement microsoft AD
- Pour chaque application en plus des habilitations gérées par la direction métier ou la DSIN, l'accès à l'application et l'authentification seront limités aux utilisateurs appartenant au groupe fonctionnel de l'application : exemple : GU_APP_[APPLICATIONS]

! Vigilance !

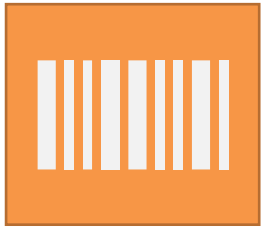
→ la connexion avec un compte utilisateur local ne doit plus être possible

Sinon :

→ La totalité des mots de passe locaux doivent être substitués par des mots de passe aléatoires de minimum X caractères avec complexité (les utilisateurs ne devant jamais les connaitre)

Seuls quelques comptes d'administration sont conservés pour les missions de la DSIN (Mot de passe sécurisé, complexe stocké sur KEEPASS)

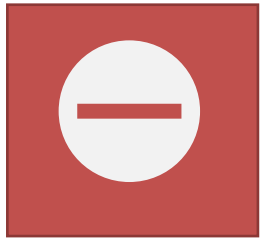
Homologation technique



Je chiffre entre les équipements utilisateurs et l'application

Quelque soit le contexte utilisateur, connecté sur le réseau local, en wifi ou en VPN, la connexion depuis son navigateur vers l'application est chiffré par Citrix ADC (SSL)

→ *Ainsi les données transitant sur les réseaux ne seront plus affichées en claires*



Je bloque tous les accès directs aux serveurs et bases de données

- Le pare-feu autorise la communication aux seules adresses ip et port sécurisé publié par Citrix ADC

- Les utilisateurs conservant des accès client lourd de type access, passeront désormais par une application (ex Access) publiée sur un serveur Citrix

J'active des sécurités renforcées : En externe systématiquement, et en interne autant que possible

- Détection d'intrusion (IDS) et Déni de services
- Antivirus
- Blocage des URL d'administration
- Apprentissage avancée URL

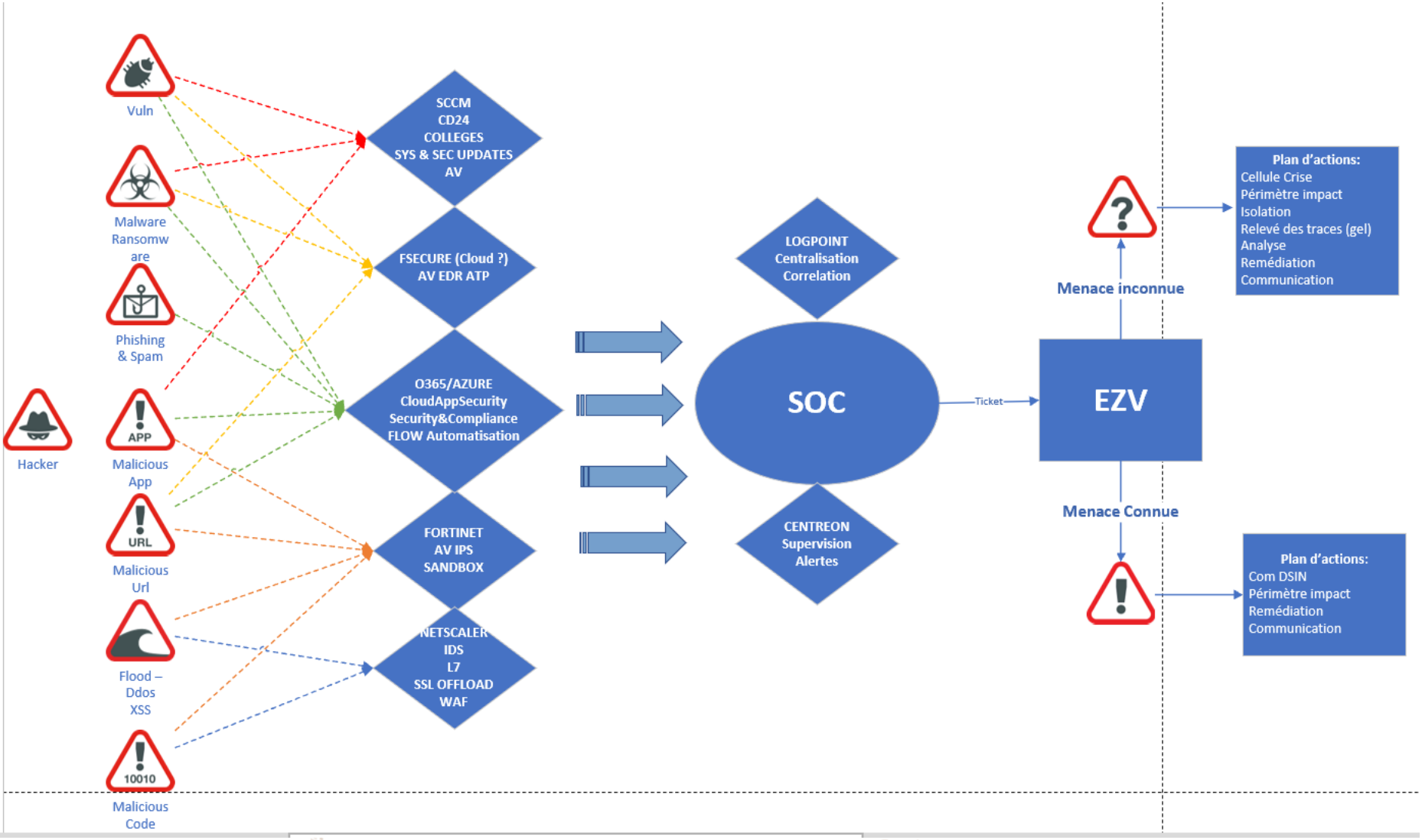
Je supervise

- La totalité des services et processus critiques au fonctionnement d'un processus métier et assure la traçabilité pour :

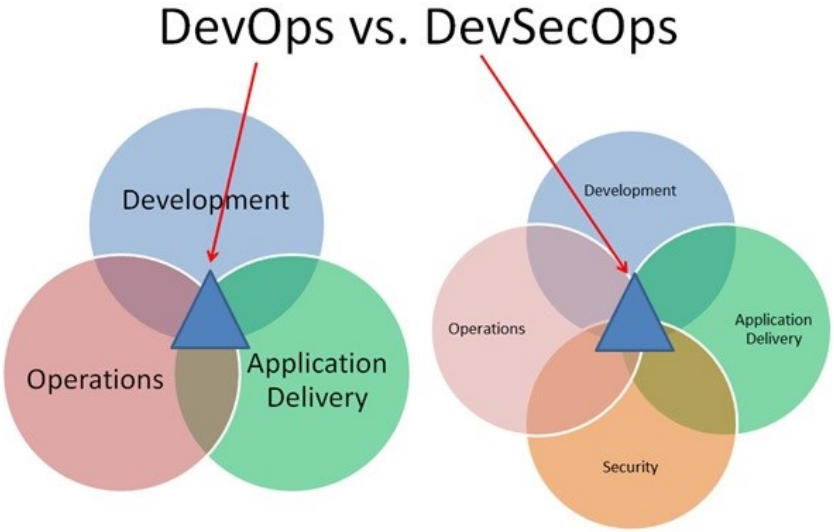
« Savoir qui se connecte à quoi, depuis où, avec quel équipement et quand »

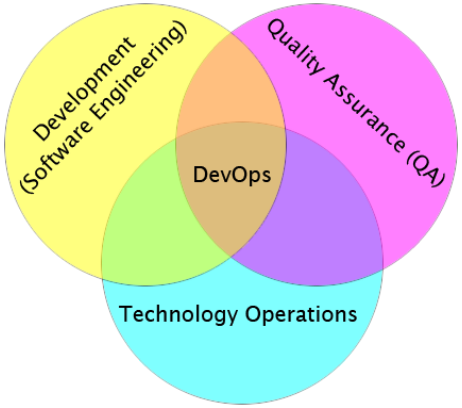
- Récupération des évènements / logs sur la règle firewall vers l'application
- Récupération des évènements / logs sur citrix netscaler
- Je sauvegarde

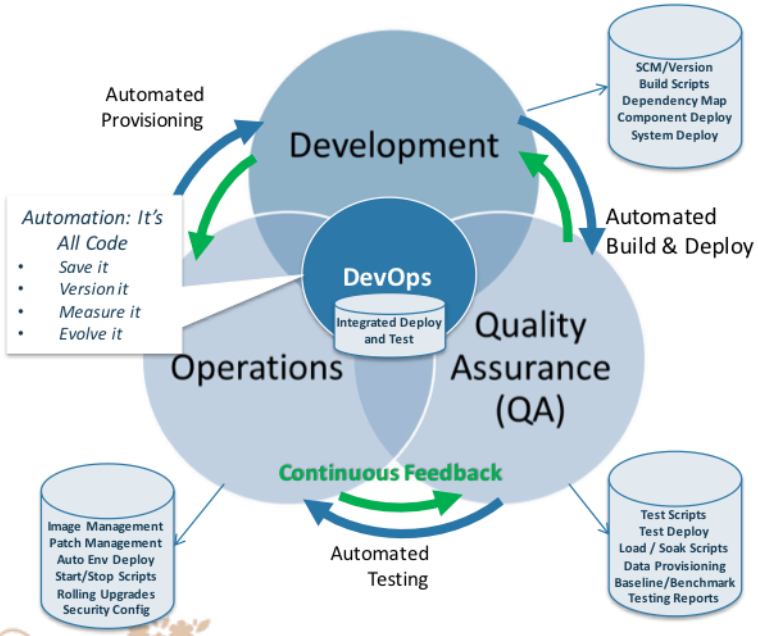
Un mot sur les concepts de Centre Opérationnel de Sécurité



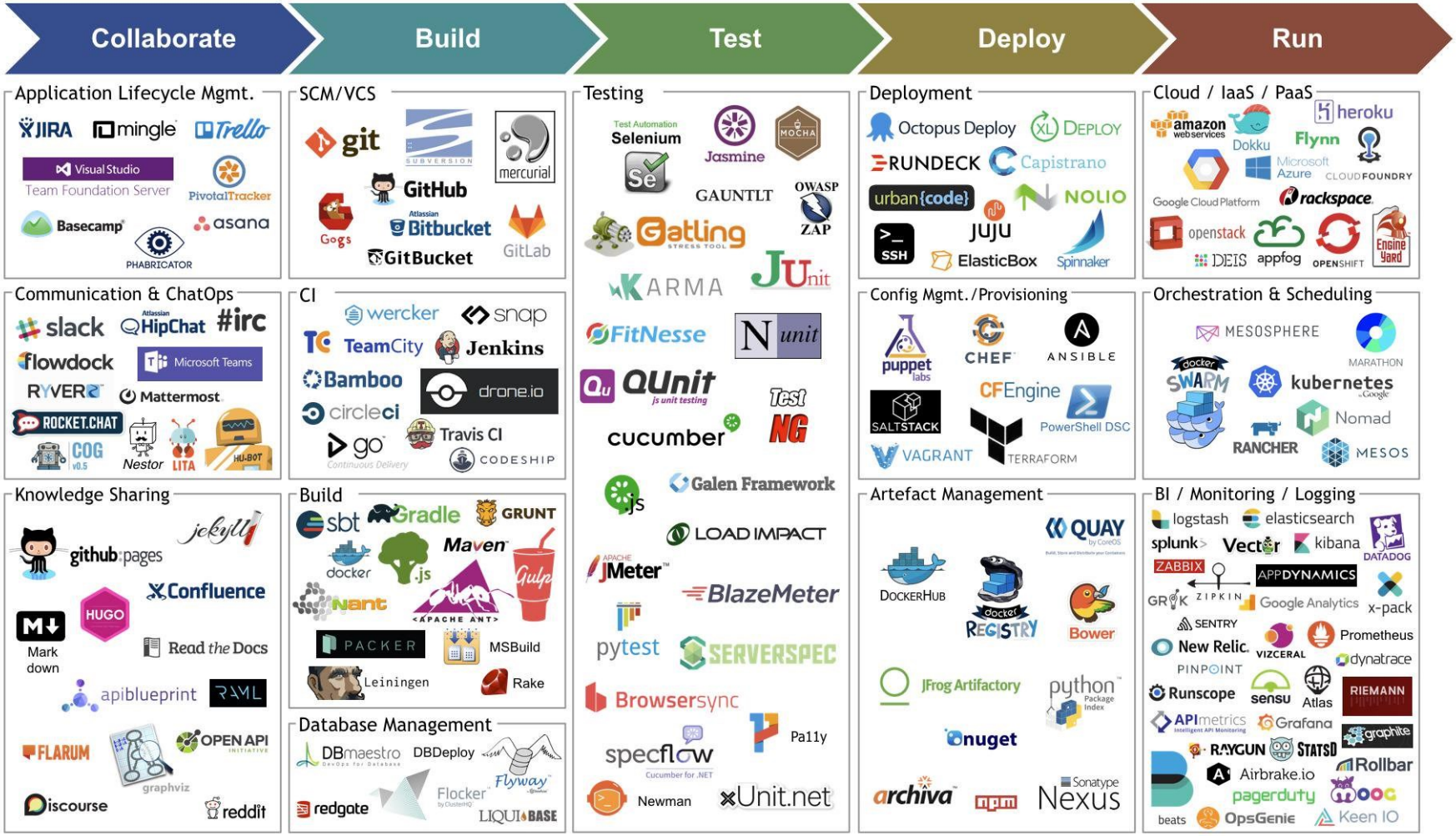
DevOps , un peu comme ITIL … ce n'est pas une norme !







Améliorer une chaine de livraison



https://twitter.com/oxalide