UNIVERSITÉ DE RENNES 1

Enjeux futurs de sécurité

date de la formation :

05/12/2017

lieu de la formation : Rennes

Sommaire

partie 1 : Big Data

partie 2 : Cloud

partie 3 : SDN

partie 4 : IoT

partie 5 : DevOps

partie 1 : Big Data

partie 2 : Cloud

partie 3 : SDN

partie 4 : Iot

partie 5 : DevOps

Big Data, kesako ?

Big Data, kesako ?

- L'explosion quantitative des données numériques a obligé les chercheurs et ingénieurs à créer de nouvelles méthodes pour aborder et analyser ces informations.

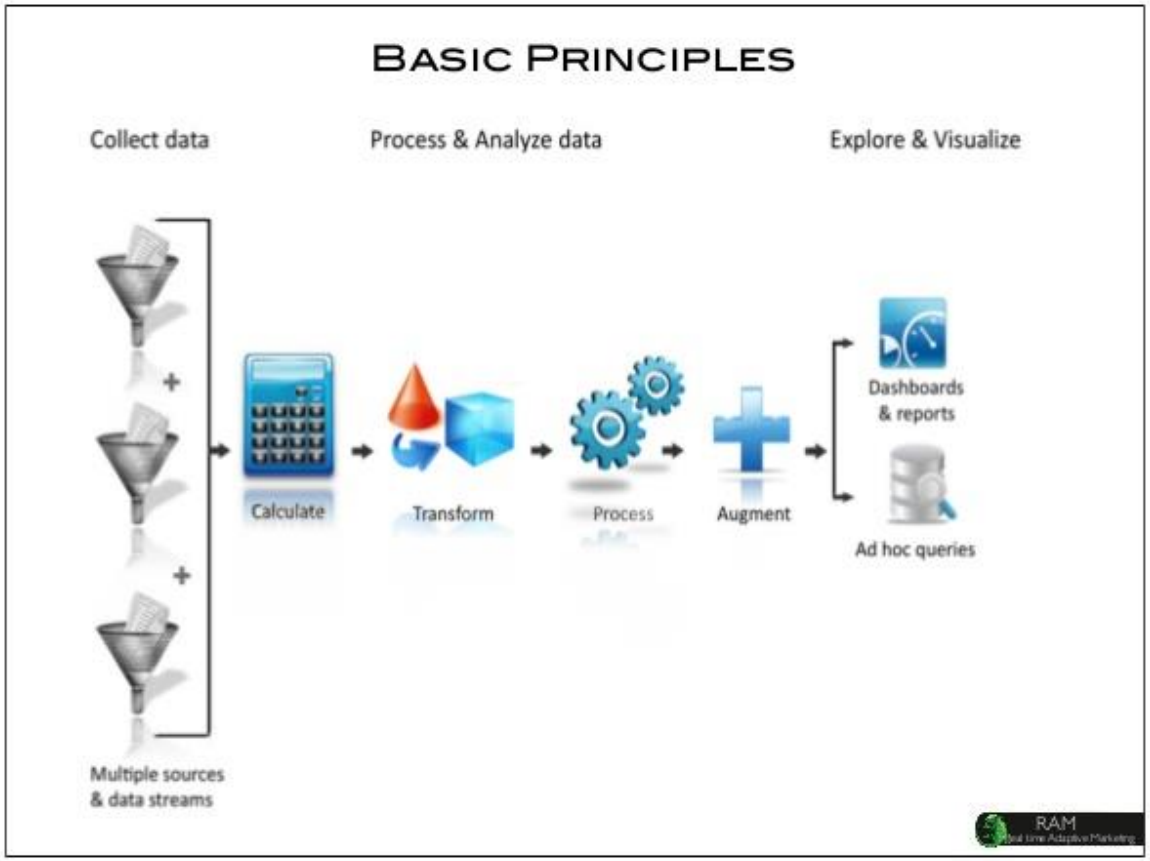
- L'objectif était de trouver des moyens pour les :
  - Capturer
  - Stocker
  - Rechercher
  - Partager
  - Analyser
  - Présenter

- Le Big Data est un concept permettant de stocker et analyser un volume énorme de données

Big Data, kesako ?

- Aujourd'hui, ce sont plus de 2,5 * 10^{30} octets qui sont créés par jour.
- L'hyper-connectivité des individus, la multiplication des terminaux (ordinateurs, téléphones, tablettes), et des objets connectés, ont fait se multiplier les données transitant sur le réseau
- On estime que le nombre de données produites par les internautes doublerait tous les 18 à 24 mois.
- Demain, nous posséderons en moyenne 8 objets connectés à titre personnel.

Big Data, kesako ?



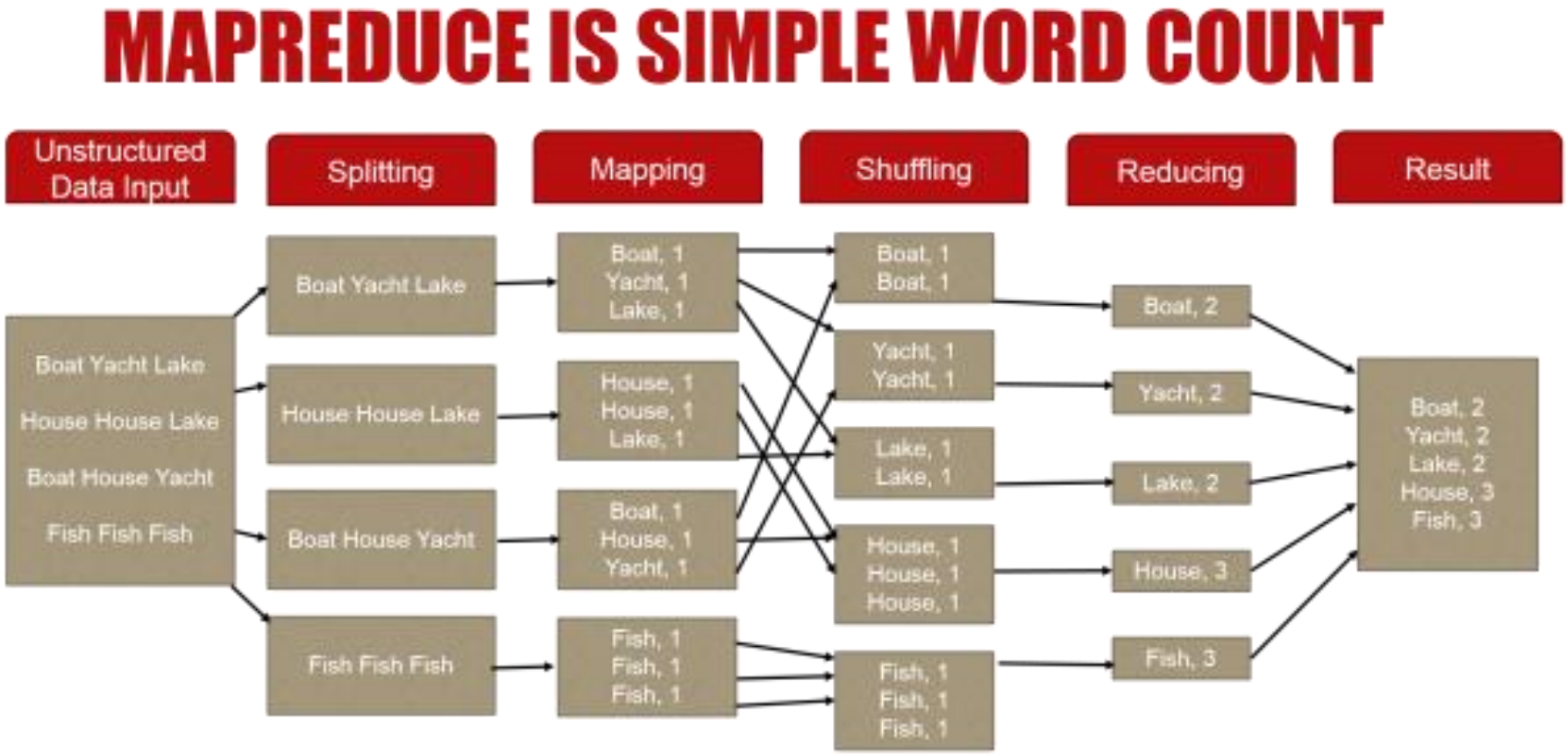
Big Data, comment ça marche ?

- MapReduce est un design pattern dans lequel sont effectués des calculs parallèles, et souvent distribués, de données potentiellement très volumineuses, typiquement supérieures en taille à 1 téraoctet

- MapReduce permet de manipuler de grandes quantités de données en les distribuant dans un cluster de machines pour être traitées.

- De nombreux frameworks ont vu le jour afin d'implémenter le MapReduce. Le plus connu est Hadoop qui a été développé par Apache Software Foundation.

Big Data, comment ça marche ?



Big Data, quels sont les enjeux de sécurité ?

- Comment identifier et sécuriser les données importantes ?
- Les mécanismes de sécurité traditionnels sont conçus pour protéger des données statiques sur un périmètre restreint, comment peut-on les adapter pour protéger des flux de données ?
- Comment le Big Data peut être un outil pour analyser et prévoir les menaces ?

protection de la vie privée et qualité de la donnée

- Pour les entreprises, ces données sont d'inestimables informations pour développer de nouveaux services et créer de la valeur ajoutée.

- Néanmoins, les entreprises doivent "sécuriser les données personnelles contre tout traitement non autorisé ou illégal, mais aussi contre la perte accidentelle, la destruction ou l'altération des données personnelles en mettant en œuvre les mesures de sécurité physique, technique et organisationnelle appropriées".

- Les procédés d'anonymisation irréversible se développent de plus en plus.

Des cyberattaques en constante augmentation

- Le vol de données aurait augmenté de 78% en 2014 comparé à l'année précédente. Plus d'un milliard de données a été dérobé.

- La mise en place, dès la conception d'un projet, des grandes briques de sécurisation permet de réduire fortement ces risques.

- Big Data ou pas, les mécanismes d'authentification, de contrôle d'accès, d'audit et de chiffrement, sont des éléments incontournables de la sécurité de tout système.

De nouveaux risques apparaissent avec le Big Data

- Avec le Big Data, trois nouveaux types de risques apparaissent. Ils peuvent être liés :
  - à l'acquisition de données,
  - à la réglementation,
  - à la vie de la donnée.

- C'est une nouvelle technologie pour la plupart des organisations , les nouvelles technologies sont souvent mal comprises et présentent donc des vulnérabilités (back-doors non-connues and et des identifiants par défaut).

- La surface d'attaque des nœuds d'un système ne sont pas forcément revus entrainant des serveurs durcis inégalement.

De nouveaux risques apparaissent avec le Big Data

- L'authentification des utilisateurs et l'accès aux données depuis différents points ne peuvent pas avoir été suffisamment contrôlés.

- Les obligations légales ne peuvent pas être entièrement couvertes, avec la problématique de l'accès aux journaux et aux audits.

- Il reste une opportunité pour l'insertion de données malveillantes ou d'une vérification inadéquate.

Dépasser les niveaux de sécurité classiques

- La sécurité informatique repose aujourd'hui sur deux étapes principales :
  - l'entreprise se protège contre les menaces connues ;
  - elle s'efforce d'identifier et de se protéger en temps réel contre des menaces inconnues, notamment via les technologies de "bac à sable" (sandboxing).

- Le recours au Big Data va permettre de mesurer l'impact que la menace détectée a eu ou aurait eu sur l'infrastructure.
- Le Big Data a la capacité d'analyser des volumes massifs et épars de données.
- Les solutions Big Data peuvent donc venir en complément des solutions de gestion des logs et du SIEM (Security Incident Monitoring).

L’analyse prédictive des menaces grâce au Big Data

- Les pratiques analytiques liées au Big Data peuvent renforcer les systèmes de sécurité des entreprises et anticiper tout signal faible de menace.

- Les fournisseurs disposent en effet d’incroyables bases de données incidents, traces, malwares et exécutables. En mutualisant les historiques et les référentiels de menaces, ils créent plus d’intelligence.

L’analyse prédictive des menaces grâce au Big Data

- Les pratiques analytiques intègrent des modèles de représentation des menaces et des attaques. Les données sont nécessaires pour la formation et la déduction de modèles à partir de ces analyses.

- La vitesse de traitement et de calcul des technologies du Big Data, additionnée à cette connaissance plus fine, permet une automatisation plus efficace des réponses.

Le facteur humain au cœur des préoccupations liées à la sécurité

- 84% des incidents sont liés au facteur humain.
- Les affaires Snowden et Manning rappellent à quel point le contrôle des accès et de l'utilisation des données sont des points critiques.
- Des signaux d'alerte automatiques peuvent être programmés lorsque, par exemple, un utilisateur accède à des données inhabituelles à une heure inhabituelle.
- Le Big Data permet ainsi aux entreprises d'inscrire la gestion de leur sécurité dans une dynamique proactive, pour anticiper et répondre aux menaces les plus avancées.

Sommaire

partie 1 : Big Data

partie 2 : Cloud

partie 3 : SDN

partie 4 : IoT

partie 5 : DevOps

Le Cloud, kesako ?

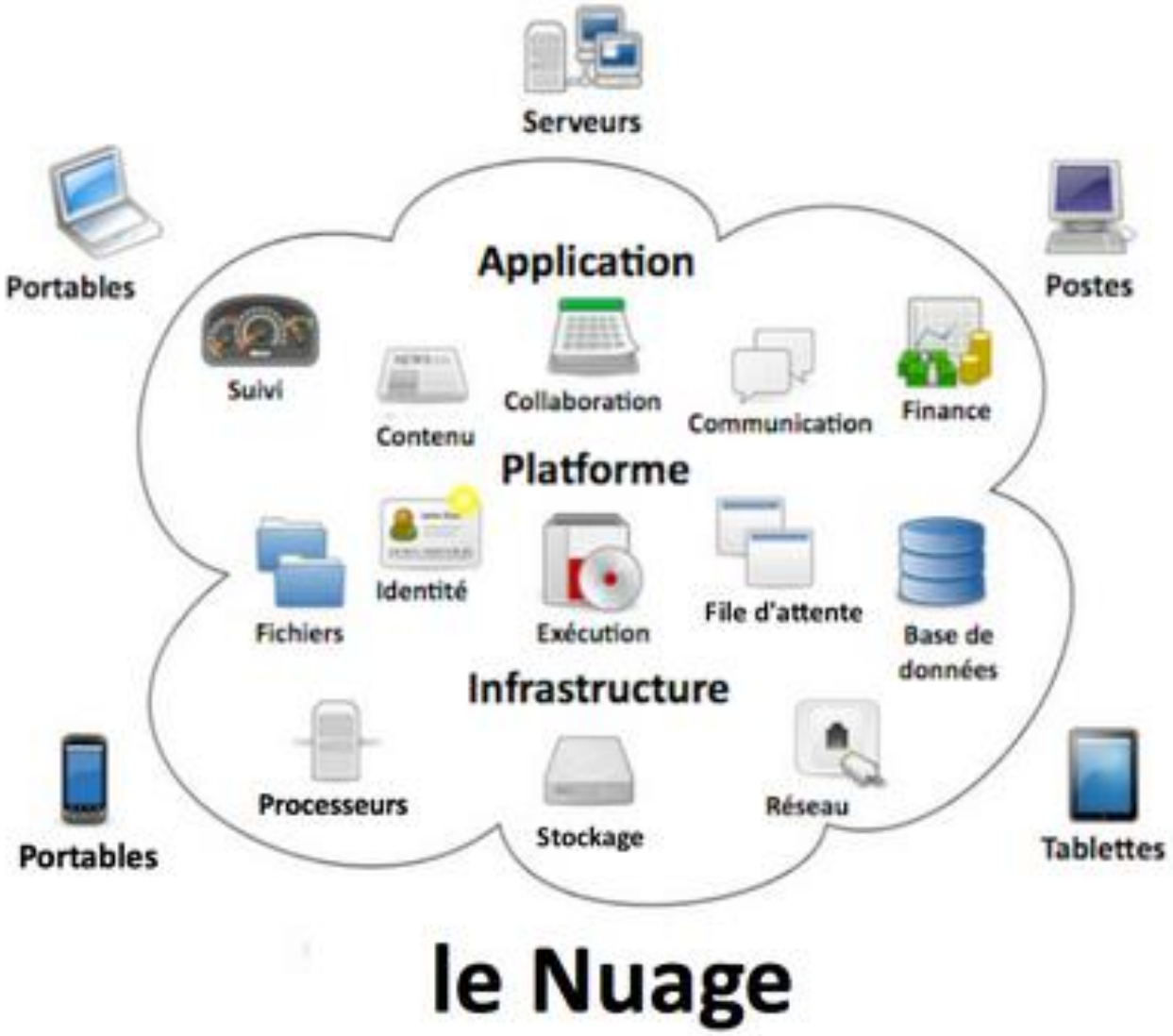
Le Cloud c'est quoi ?

- Le cloud computing est l'exploitation de la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement Internet

- Le cloud computing est l'accès via un réseau de télécommunications, à la demande et en libre-service, à des ressources informatiques partagées configurables. Il s'agit donc d'une délocalisation de l'infrastructure informatique

- Le cloud computing est un basculement de tendance : au lieu d'obtenir de la puissance de calcul par acquisition de matériel et de logiciel, le consommateur se sert de puissance mise à sa disposition par un fournisseur via internet.

Le Cloud c'est quoi ?



Le Cloud c’est quoi ?

- IaaS (Infrastructure as a Service, en anglais)

- le système d'exploitation et les applications sont installés par les clients sur des serveurs auxquels ils se connectent pour travailler comme s'il s'agissait d'un ordinateur classique

- Le fournisseur de service ne met à disposition que le matériel virtuel

Le Cloud c’est quoi ?

- PaaS (Platform as a Service, en anglais)

- dans ce mode, c'est le fournisseur du service cloud qui administre le système d'exploitation et ses outils. Le client peut installer ses propres applications si besoin.

- Le fournisseur de service met à disposition le matériel et l’OS virtuels

Le Cloud c’est quoi ?

- SaaS (Software as a Service, en anglais)

- les applications sont fournies sous forme de services clés en mains auxquels les utilisateurs se connectent via des logiciels dédiés ou un navigateur Internet.

- Pour le grand public, il s'agit par exemple de messageries électroniques type Gmail, Yahoo, Outlook.com ou de suites bureautiques type Office 365 ou Google Apps.

Le Cloud, quels sont les risques ?

- L'existence de brèches de sécurité tant sur l'une des couches logiques du Datacenter que celles issues d'erreurs humaines ;

- La fragilité dans la gestion des accès et des identités, bien que certains fournisseurs renforcent les interfaces d'authentification avec d'autres moyens tels que les certificats, les smartcards, la technologie OTP et bien d'autres ;

- L'utilisation d'API non sécurisées pour l'intégration des applications avec les services cloud ;

Le Cloud, quels sont les risques ?

- L'exploit de vulnérabilités des systèmes d'exploitation sur les serveurs du cloud et même sur les applications hébergées ;

- Le piratage de compte, qui est un vieux type d'attaque informatique, vient avec une forte recrudescence depuis l'avènement d'Internet et encore celui du cloud computing ;

- Une action malveillante initiée en interne dans les effectifs du fournisseur. Une personne malveillante dans l'équipe de gestion du Datacenter peut facilement nuire à la confidentialité et l'intégrité des environnements hébergés ;

Le Cloud, quels sont les risques ?

- Les menaces persistantes avancées (en anglais, APT : Advanced Persistent Threats) qui consistent en une forme d'attaque où le hacker réussit à installer d'une façon ou d'une autre un dispositif dans le réseau interne de l'organisation, à partir duquel il peut extirper des données importantes ou confidentielles. C'est une forme d'attaque difficile à détecter pour un fournisseur de services cloud ;

- La perte de données qui peut être causée par une attaque informatique (logique) du Datacenter, une attaque physique (incendie ou bombardement), une catastrophe naturelle, ou même simplement à un facteur humain chez le fournisseur de services, par exemple en cas de faillite de la société ;

Le Cloud, quels sont les risques ?

- Les insuffisances dans les stratégies internes d'adoption ou de passage au cloud. Les entreprises ou les organisations ne prennent pas souvent en compte tous les facteurs de sécurité liés à leur fonctionnement avant de souscrire à un service cloud. Certaines négligences, tant au niveau du développement d'application qu'au niveau de l'utilisation basique, leur sont parfois fatales ;

- Utilisation frauduleuse des technologies cloud en vue de cacher l'identité et de perpétrer des attaques à grande échelle. Généralement, il s'agit de comptes créés pendant les périodes d'évaluation (la plupart des FAI proposent 30 jours d'essai gratuits) ou des accès achetés frauduleusement ;

Le Cloud, quels sont les risques ?

- Le déni de service qui est une attaque qui consiste à rendre indisponible un service par une consommation abusive des ressources telles que les processeurs, la mémoire ou le réseau. L'idée, pour le pirate, c'est de réussir à surcharger les ressources du Datacenter en vue d'empêcher d'autres utilisateurs de profiter des services ;

- Les failles liées à l'hétérogénéité des technologies imbriquées dans l'architecture interne du cloud, et l'architecture externe d'interfaçage avec les utilisateurs.

Sécurité du Cloud, les enjeux

- Appliquer rigoureusement une composante IAM (Identity and access management) va permettre de contrôler les accès et d'éviter l'utilisation infondée des comptes à privilèges.

- Le chiffrement des données au repos va créer une isolation logique supplémentaire par rapport aux mesures techniques et procédurales mises en œuvre par les prestataires.

Sécurité du Cloud, les enjeux

- La mise en place d'un nouveau plan de contrôle de la sécurité redonnera la visibilité et les compétences d'automatisation à des équipes dont le périmètre d'intervention a évolué et qui sont éventuellement déstabilisées par le passage au cloud.

- Sauvegarder toutes les données dans un domaine d'erreur distinct permet de s'affranchir des incidents toujours possibles chez un prestataire. Souvent, il suffira d'opter pour une réplication dans une autre région géographique. Dans certains cas, il conviendra de recourir à un second prestataire.

Sécurité du Cloud, les enjeux

- Assumer la responsabilité des instances et des applications en utilisant des outils de tests dynamiques et statiques pour identifier et éliminer les vulnérabilités des applications.

- Faire réaliser des audits de conformité par des tiers permet de certifier la pile applicative dans la continuité de la conformité fournie par le prestataire (SOC 1/2/3, ISO 27001, PCI, FedRAMP, etc.).

Sécurité du Cloud, les enjeux

- Il s'agit de segmenter et de contenir le trafic, en utilisant des contrôles de filtrage et de réseau virtuel. Les prestataires de services de cloud computing ont ajouté des contrôles au niveau du réseau en créant des clouds privés virtuels (AWS) ou des réseaux virtuels (Azure), en plus de limitations par type de trafic (Internet, VPN, etc.).

- En revanche, ils ne fournissent pas toujours les fonctions de journalisation, de détection et de prévention d'intrusion, ou encore l'intégration aux consoles fournies au sein des pare-feu traditionnels. Le client devra donc considérer des dispositifs particuliers pour opérer ces fonctions.

Sommaire

partie 1 : Big Data

partie 2 : Cloud

partie 3 : SDN

partie 4 : IoT

partie 5 : DevOps

SDN, Kesako ?

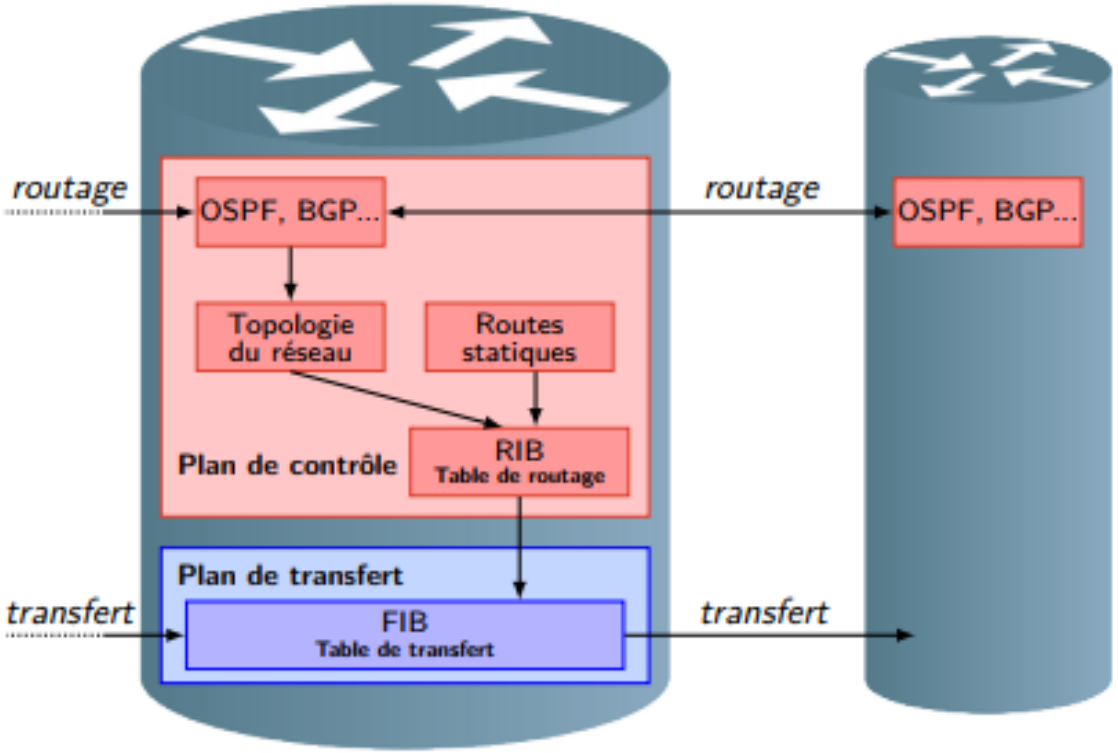
NV, NFV et SDN

- Virtualisation du réseau (Network Virtualization, NV) qui tente de créer des segments logiques dans un réseau déjà existant en divisant le réseau logique au niveau du débit. Il créé un tunnel à travers un réseau pour connecter deux domaines indépendamment des infrastructures.

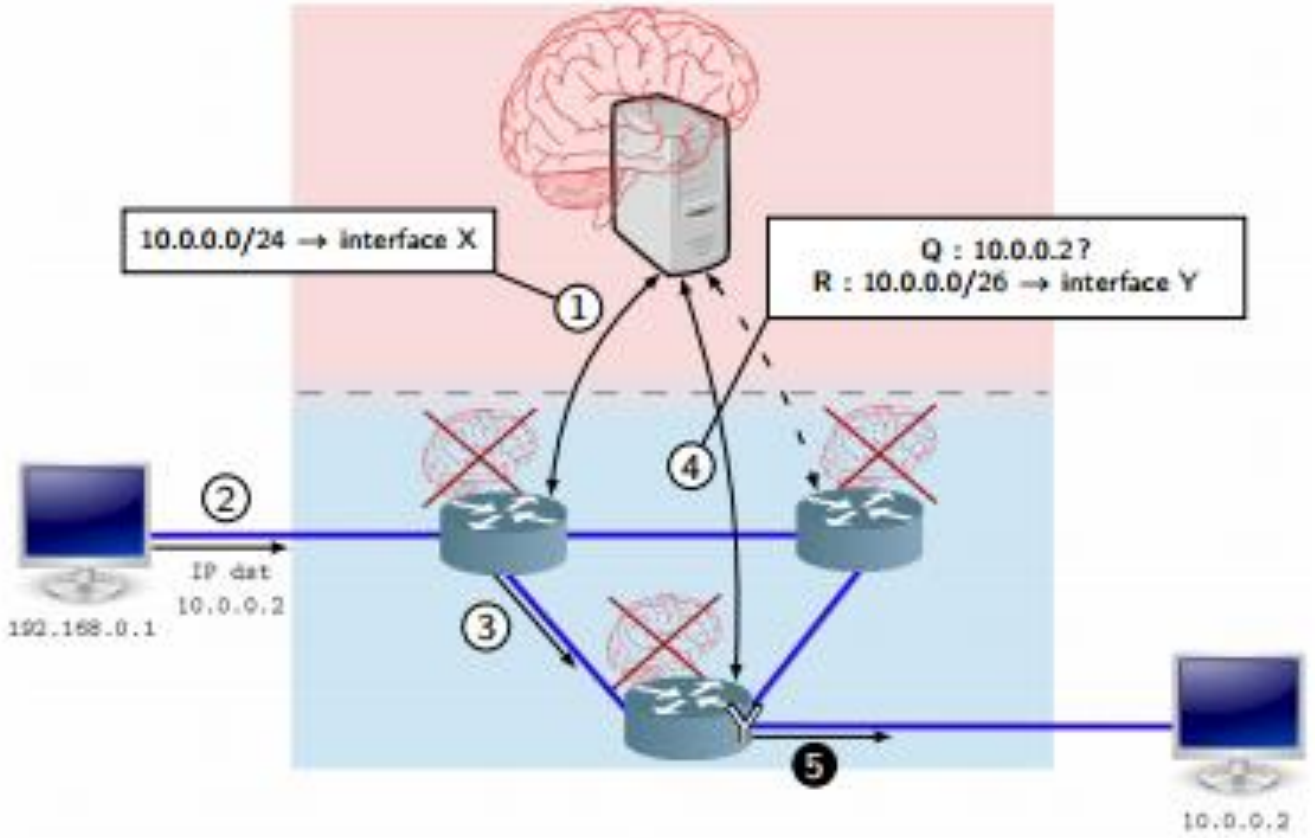
- Les fonctions de réseau virtualisées (Network Functions Virtualization, NFV) permettent quant à elles de mettre un service sur un tunnel.

- Le SDN n'ajoute pas de fonction ou tunnel virtuel sur le réseau physique mais le modifie en le rendant programmable.

Routage traditionnel



Routage SDN



Les avantages du SDN

- Les SDN ont pour but pratique de rendre programmables les réseaux par le biais d'un contrôleur centralisé

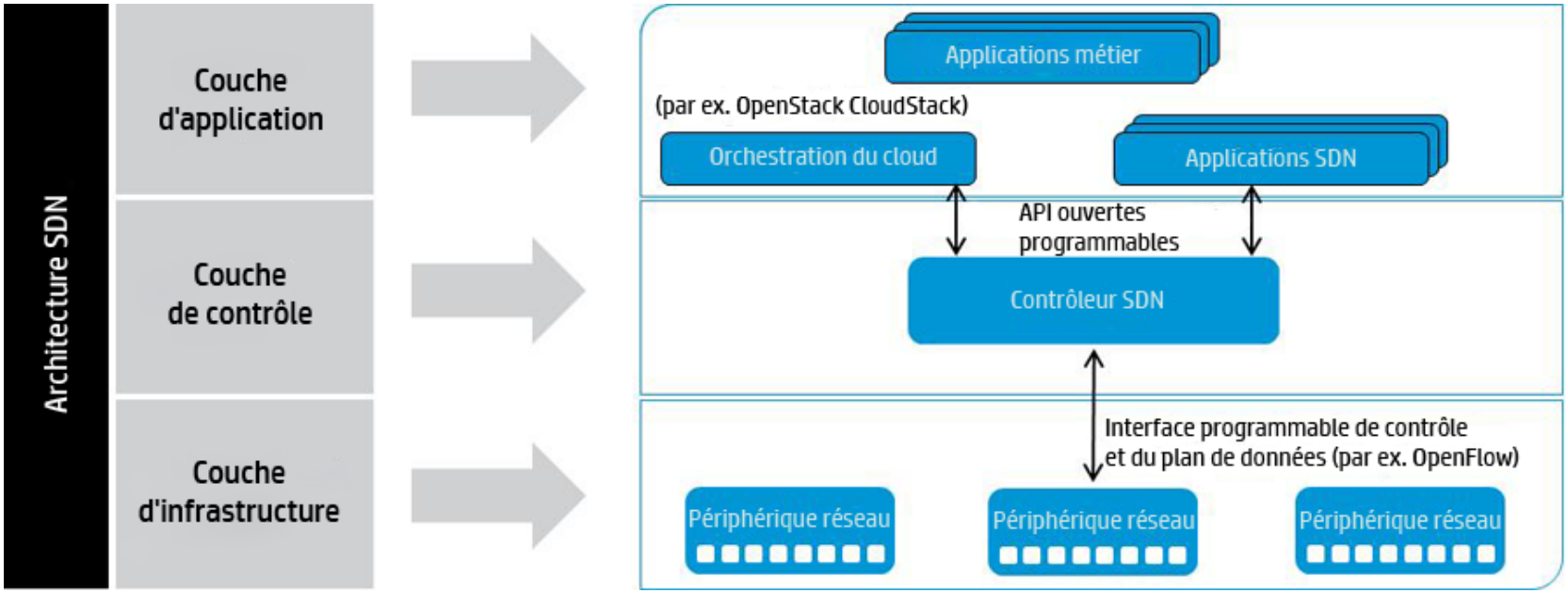
- Aujourd'hui les commutateurs et les routeurs calculent leurs tables de forwarding localement, ce qui signifie que les périphériques réseau prennent leurs propres décisions en interne sur la meilleure façon d'aiguiller le trafic

- Ces décisions s'appuient sur les informations distribuées collectées par des protocoles de routage comme OSPF et BGP

Les avantages du SDN

- Centralisation du contrôle du réseau
- Le principe réside dans la séparation du plan de contrôle du plan de transfert
- Permettant notamment le déploiement sur des plateformes de plus grande capacité que les classiques commutateurs réseau.

Les avantages du SDN



Les avantages du SDN

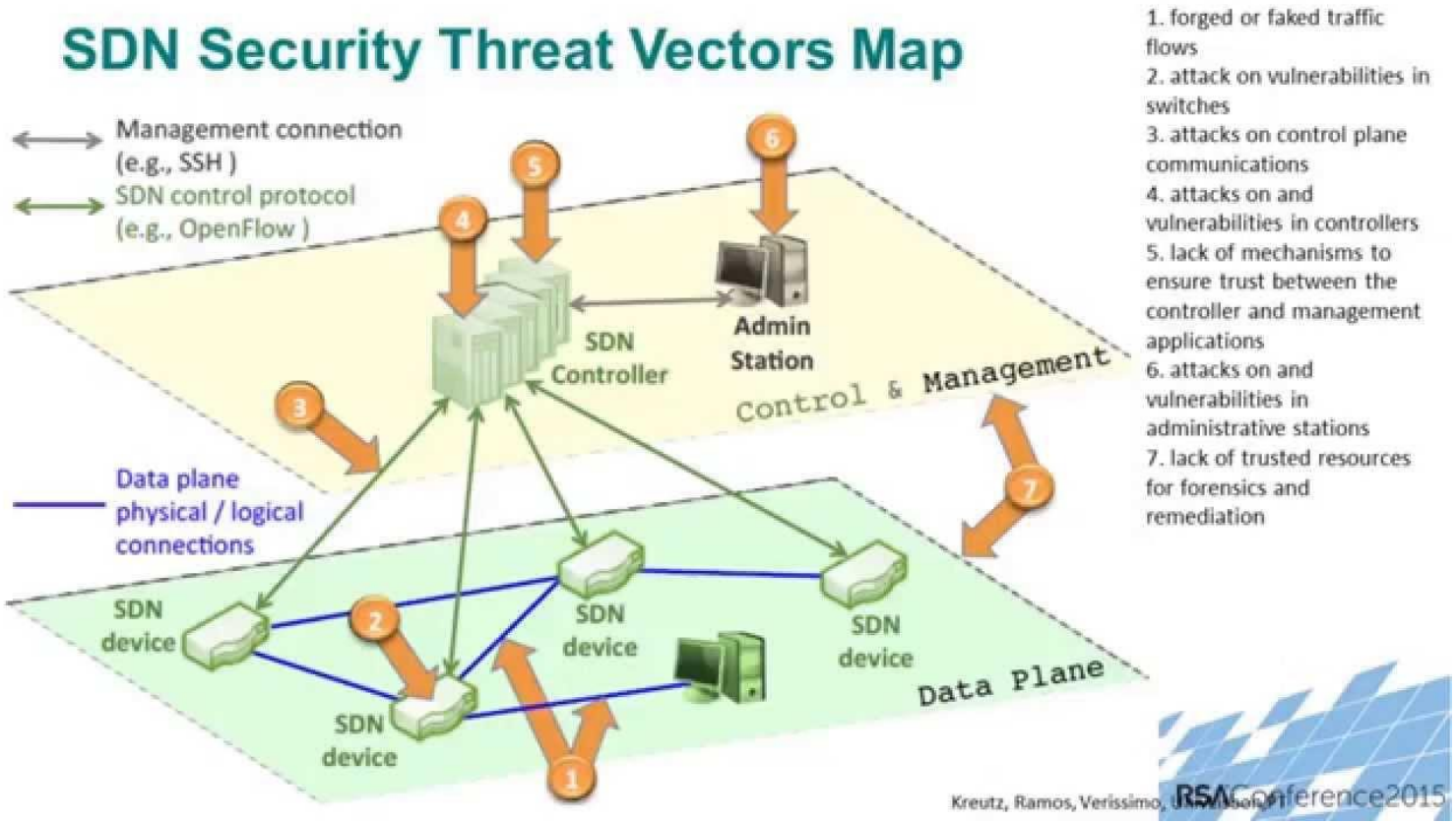
- Efficacité : optimise les applications, infrastructures et réseaux existants
- Elasticité : permet de propager rapidement des applications et services existants
- Innovation : permet de créer et fournir de nouveaux types de business models, applications et services

Le SDN pourquoi ?

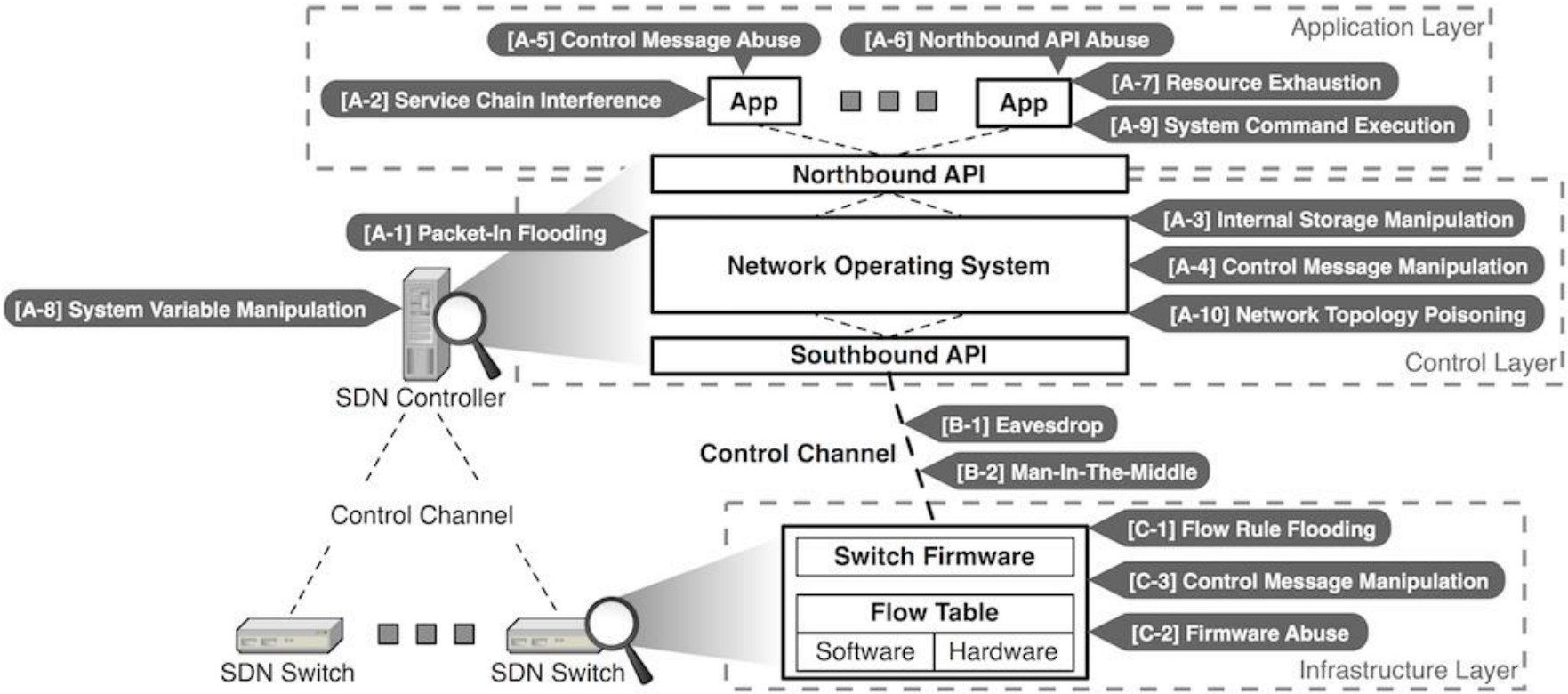
- Selon IDC, SDN deviendra un marché à 12,5 milliards de $ en 2020

- IDC prévoit une augmentation de son de usage de 90% par an

SDN, les enjeux



SDN, les enjeux



SDN, les enjeux

- Manque de système d'authentification et de chiffrement permettant d'administrer en toute sécurité les données

- Failles logicielles (XXE) qui permettent à un attaquant de prendre l'accès aux changements de configuration réseau

- Attaques DoS spécifiques utilisant des paquets qui ne correspondent à aucune règle établie provoquant la déconnexion des commutateurs du réseau

- Faiblesses dans le host spooffing un attaquant peut prendre la place d'un nœud et ainsi rediriger le trafic vers un lieu « non-sûr »

SDN, les enjeux

- La gouvernance du réseau

Sommaire

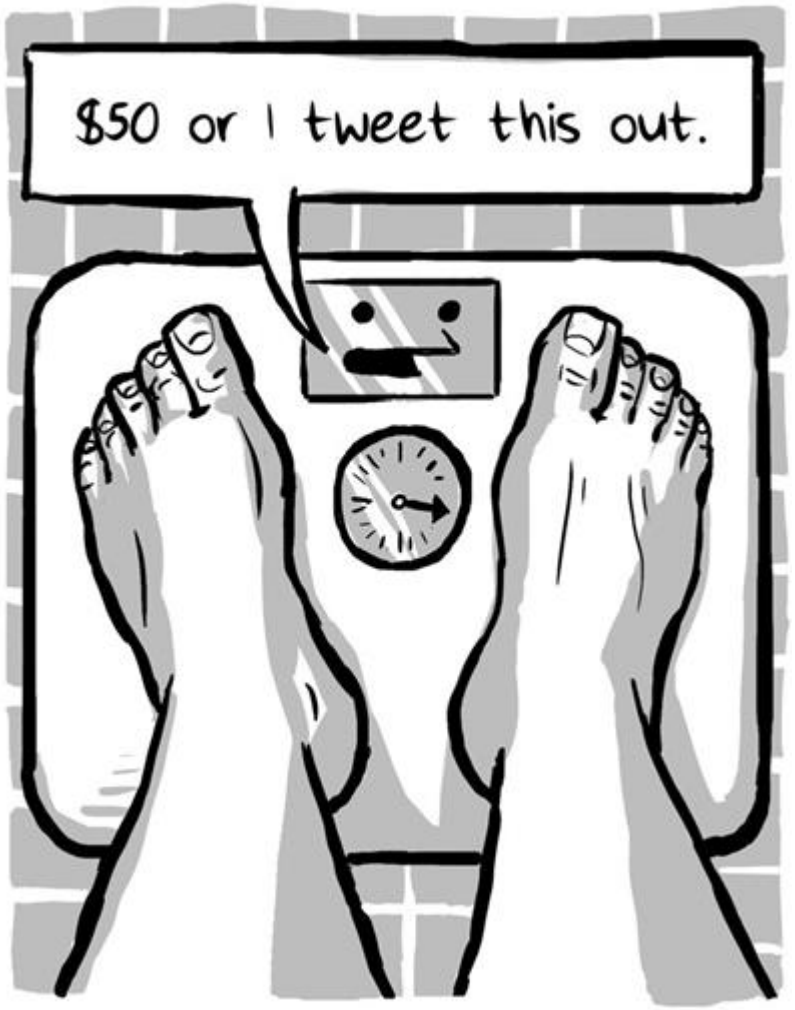
partie 1 : Big Data

partie 2 : Cloud

partie 3 : SDN

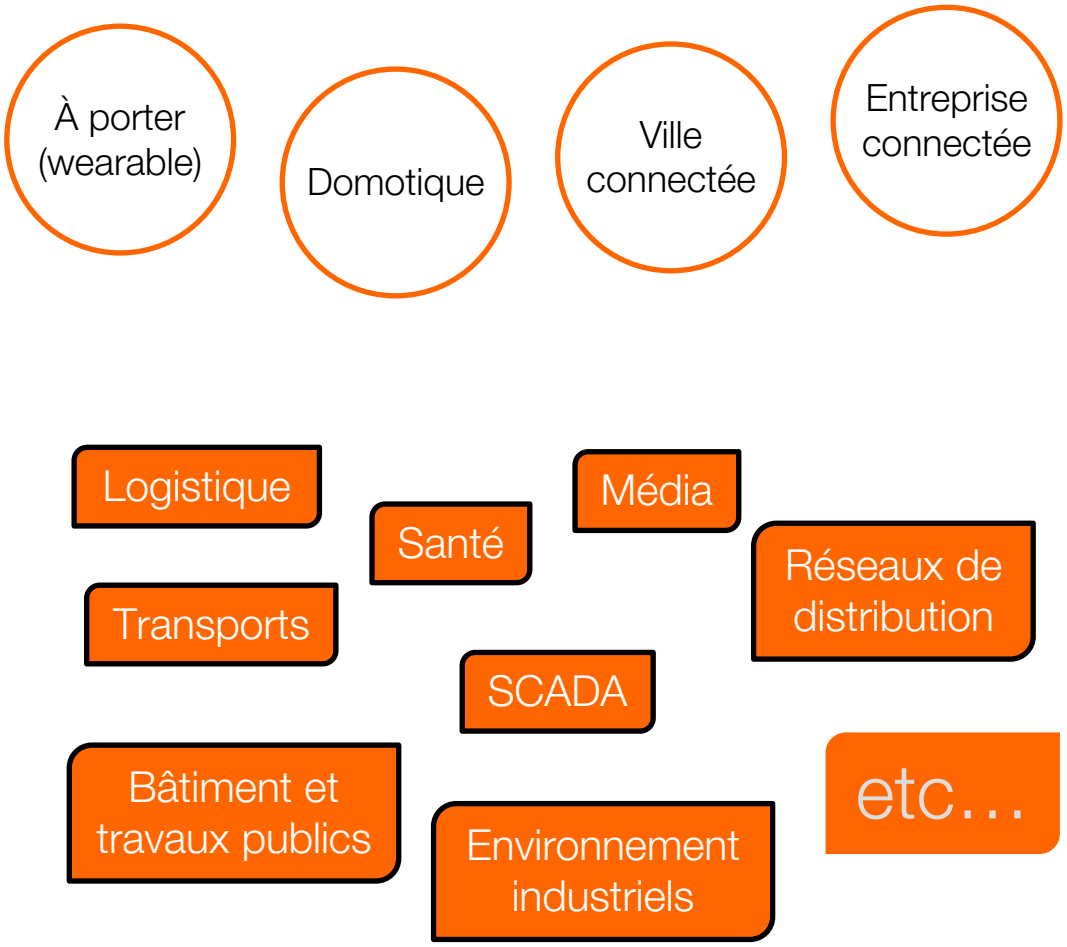
partie 4 : IoT

partie 5 : DevOps



IoT, Kesako ?

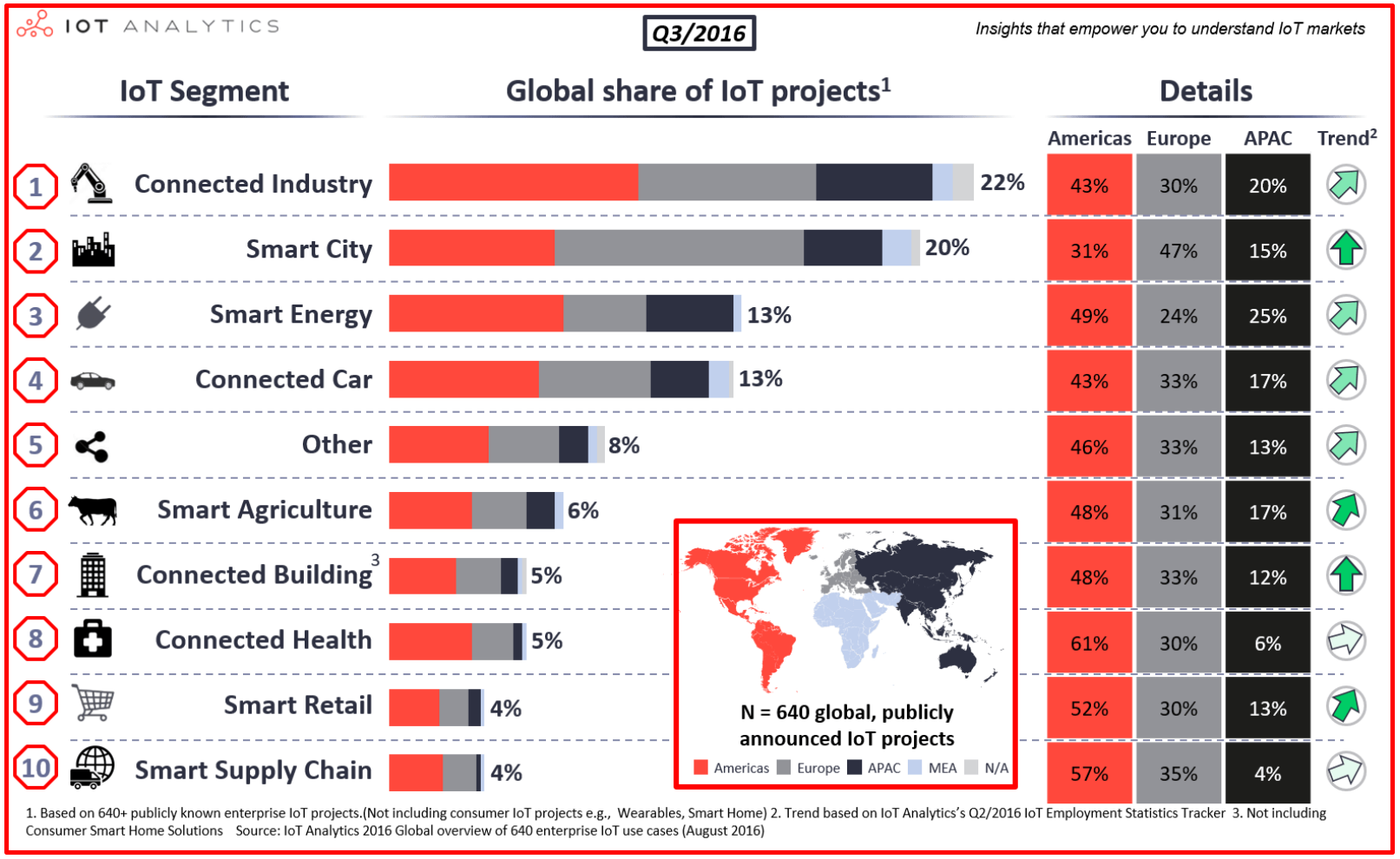
Les domaines de l'IoT



Ce n'est pas un nouveau domaine technologique, mais plutôt plusieurs domaines technologiques assez anciens qui voient s'ouvrir des opportunités d'innovation.

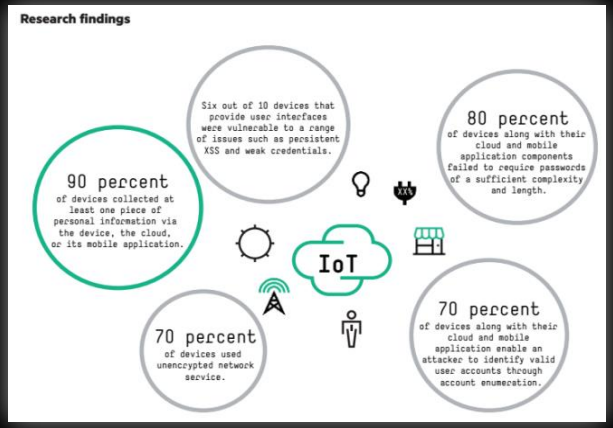
Il n'y pas de « domaine IoT » unique, mais plutôt une multitude de domaines avec des usages et des contraintes technologiques très différentes.

Les domaines de l'IoT



L'Internet des objets fait peur…

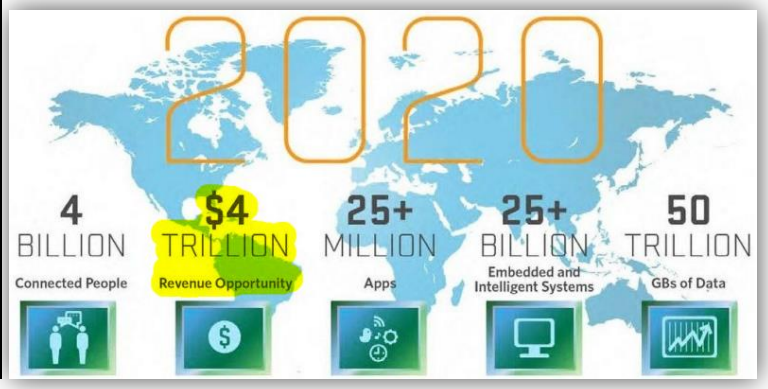
… alors qu'il promet beaucoup



Des développements « effrayants »

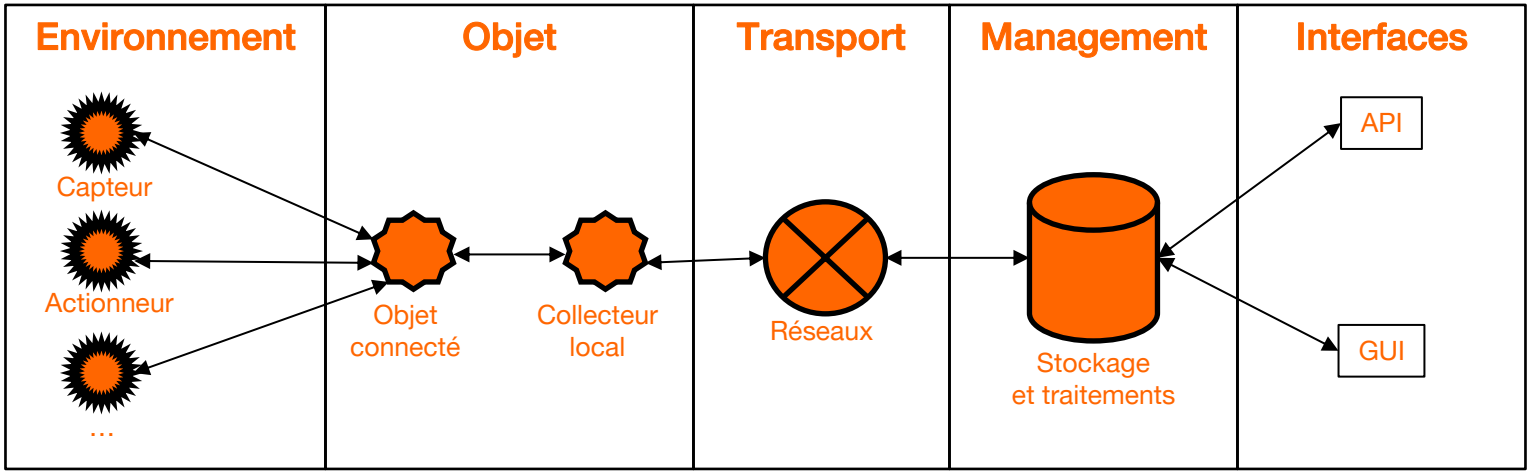
Mais selon Guillaume Poupard, directeur général de l'ANSSI, la situation serait particulièrement préoccupante dans le domaine de la santé. *« La santé numérique va avoir un impact absolument incroyable. Par contre, avec les yeux de l'informaticien expert cyber, c'est juste effrayant. Quand on voit la quantité d'informations récoltées, quand on voit l'action que tout cela peut avoir sur les patients, il y aura des morts demain »*, estime-t-il. Pour autant, il ne s'agira pas nécessairement d'assassinats ciblés, mais plutôt de dégâts collatéraux, dans la mesure où « *ces appareils vont se faire polluer par des attaques qui ne leur étaient pas destinées* ».

Comment éviter ce scénario catastrophe ? Une première



Qu’est-ce que l’IoT ?

Le système IoT



IoT, les problèmes

- Les technologies utilisées sont jeunes… les vulnérabilités qui vont être découvertes ces prochaines années vont être légion.

- Il n'est pas non plus dit que l'aspect sécurité ait été pris réellement en compte par certains constructeur en tirant partie de l'expérience des ordinateurs/internet.

- Les objets connectés sont souvent oubliés par les utilisateurs… et même parfois les éditeurs qui publient même pas de mise à jour de sécurité ; Pour les entreprises, c'est un vrai casse tête pour maîtriser les appareils et les données qui peuvent en sortir.

- Au bout de la chaîne, il reste les masses de données récupérées.

IoT, les problèmes

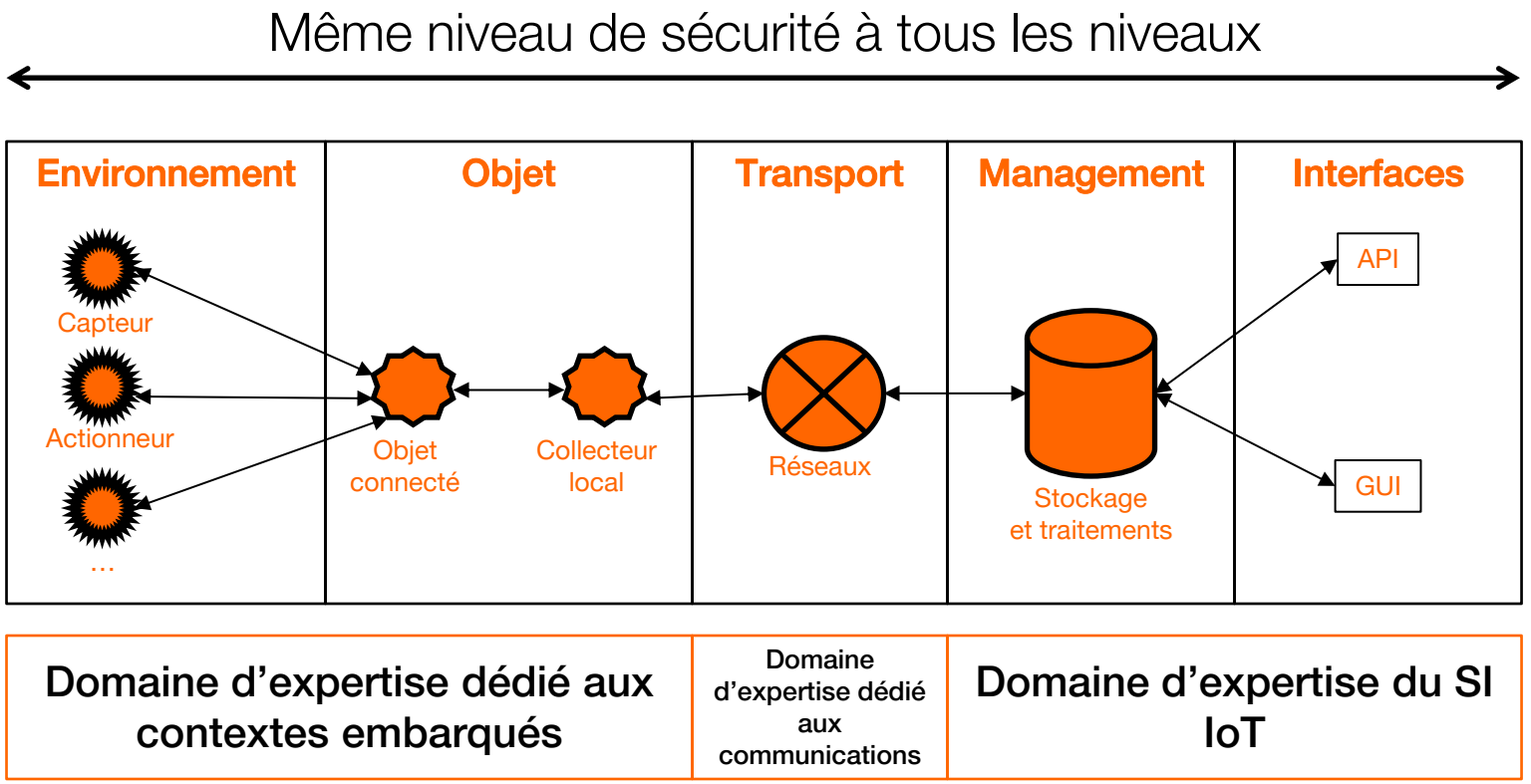
- « Les vulnérabilités ne concernent que les objets »

- La sécurité de l'IoT ne se résume pas à que la sécurité des objets connectés, ou du réseau, ou des utilisateurs

- La surface d'attaque de l'IoT n'est pas qu'une simple surface d'attaques, ce sont des surfaces d'attaques réparties sur toute la chaine de traitement des données de l'IoT

- Il est nécessaire d'évaluer chacune des surfaces d'attaques de l'IoT

Le système IoT à sécuriser



Sécurité de l'IoT, les enjeux

Sécurité de l'IoT, les enjeux

- Tous ces éléments doivent être considérés
  - L'objet connecté
  - Le Cloud
  - L'application mobile
  - Les interfaces réseau
  - Les logiciels
  - L'utilisation de la cryptographie
  - L'utilisation de l'authentification
  - La sécurité physique
  - Les ports USB

Sécurité de l'IoT, les enjeux

- Adopter une approche globale de la sécurité : Il s'agit de vérifier que les données sont protégées et chiffrées du datacenter ou du cloud jusqu'au terminal et à chaque étape intermédiaire.
  - Contrôle de la sécurité des terminaux, la sécurité du réseau, la gestion des identités et des accès, etc.

- Analyser les appareils : Comprendre l'impact des terminaux connectés sur les réseaux, les données qu'ils collectent et communiquent, leur origine, et ce que dévoilent toutes les évaluations de vulnérabilités ou les éventuelles certifications des dispositifs concernés.

Sécurité de l'IoT, les enjeux

- Faire un audit du réseau : Réaliser un état des lieux en amont de l'installation d'un appareil pour bien comprendre son impact sur le trafic réseau.
  - Organiser un audit pour obtenir une vision globale des dispositifs qui ont accès au système, quand, ce qui se produit au moment de l'accès aux données et ce qui est communiqué à telle personne et à tel endroit.

- Compartimenter le trafic : Adopter une politique « zéro confiance » vis-à-vis des dispositifs IoT. Rassembler ces objets sur un segment du réseau ou un VLAN séparé de telle sorte qu'ils ne puissent pas accéder ni interférer avec des données stratégiques.

Sécurité de l'IoT, les enjeux

- Former les équipes : Au gré de l'évolution de l'écosystème IoT, il est impératif de veiller à ce que les équipes responsables des services informatiques, de la sécurité et du réseau
  - soient formées à utiliser les nouveaux équipements,
  - qu'elles connaissent les standards et les problèmes fréquents.

Sommaire

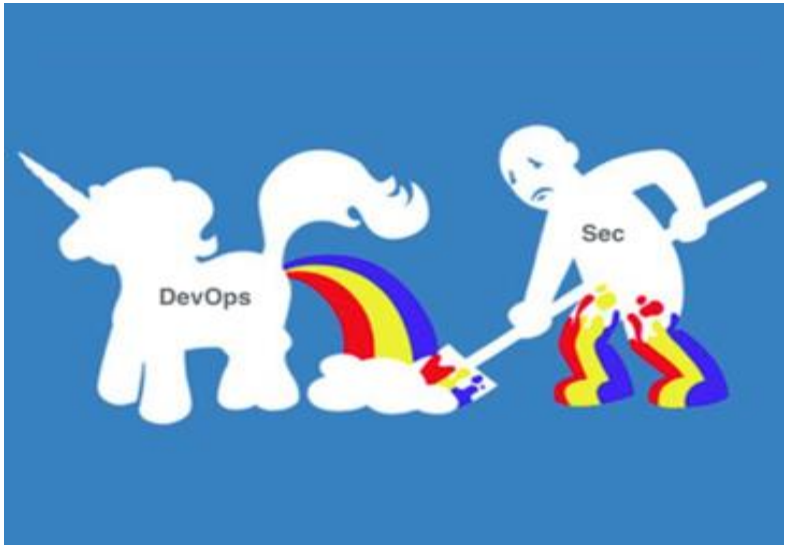
partie 1 : Big Data

partie 2 : Cloud

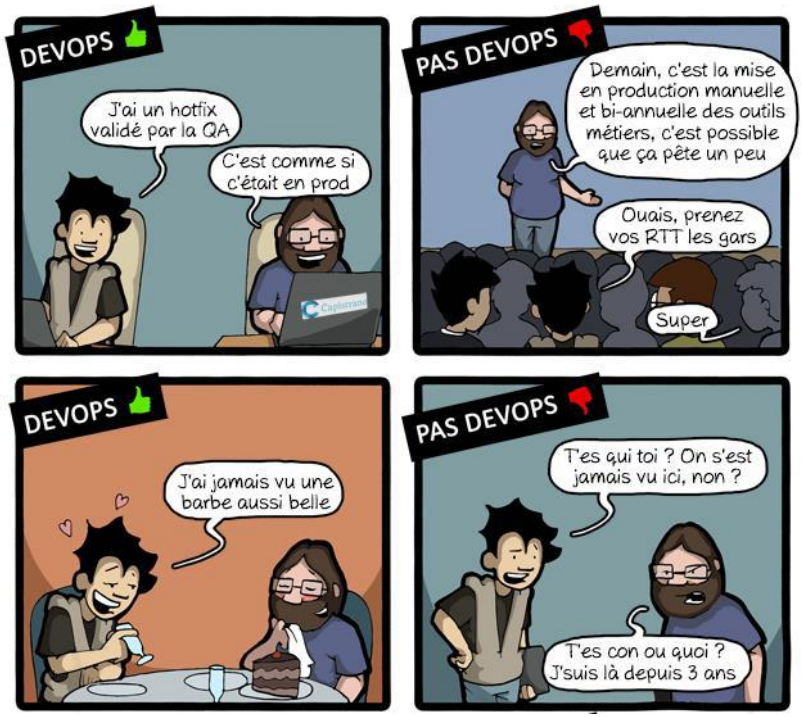
partie 3 : SDN

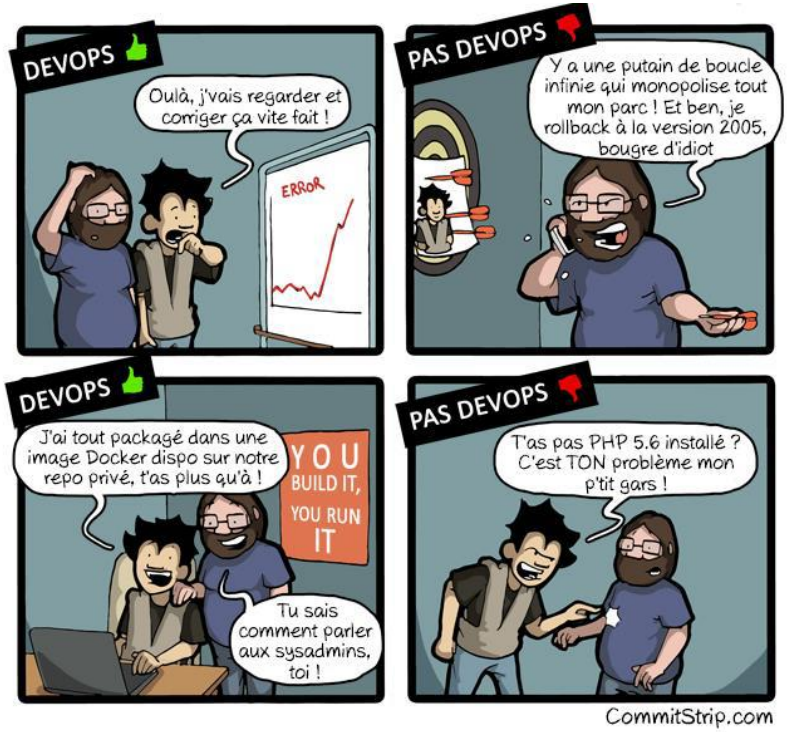
partie 4 : IoT

partie 5 : DevOps

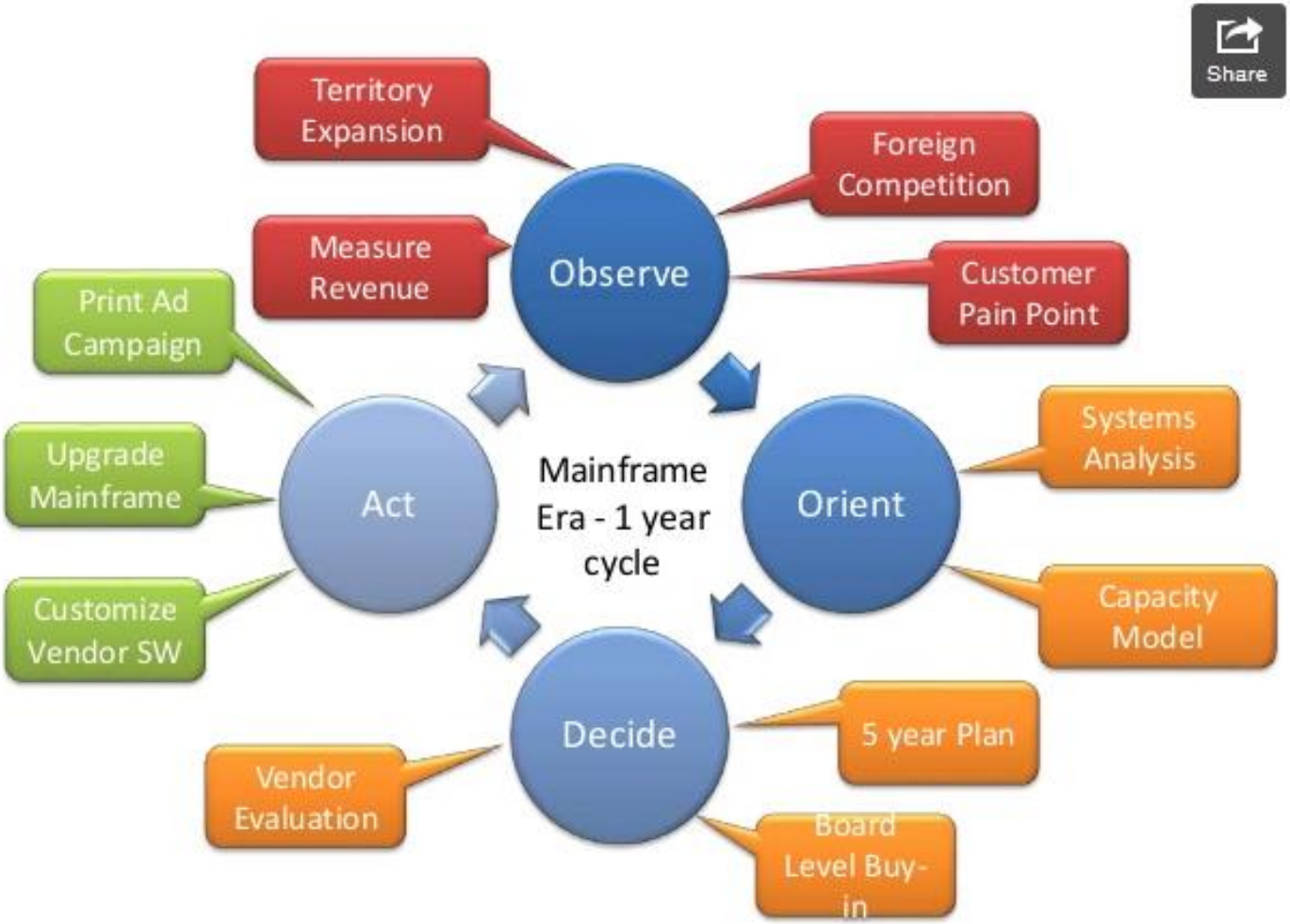


DevOps, kesako ?

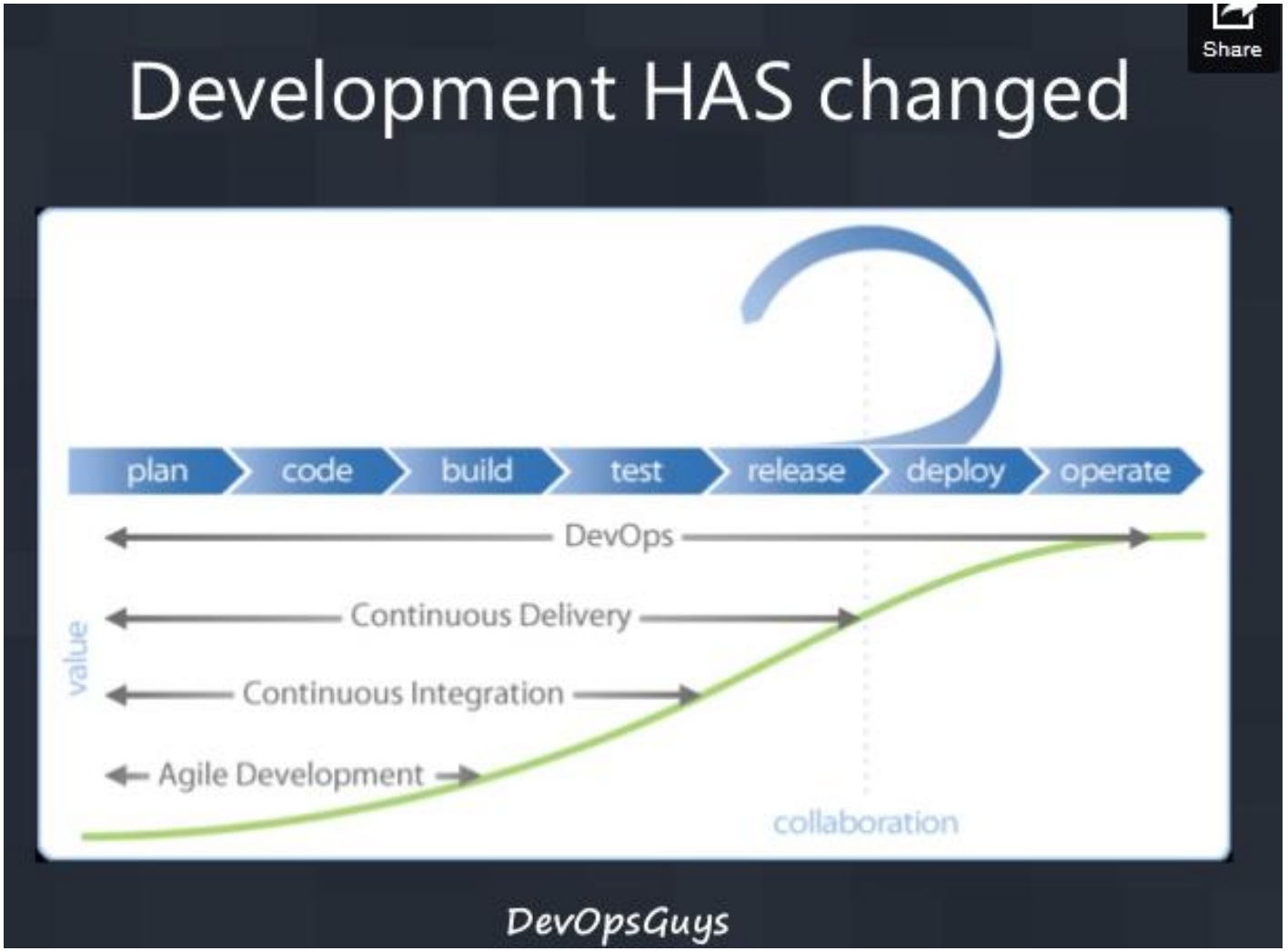




Pourquoi DevOps ?



Pourquoi DevOps ?



Les déploiements ne sont plus des évènements

Endless possibilities

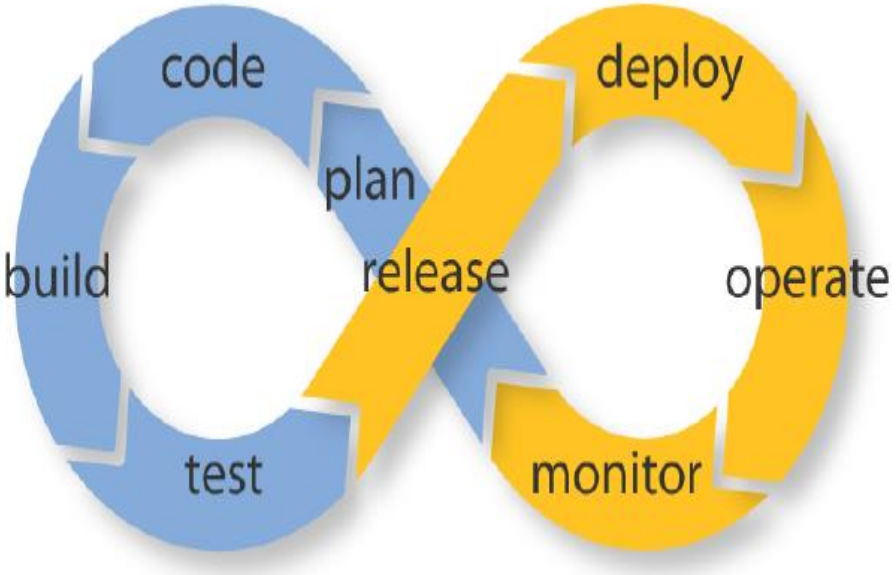
DevOps can create an infinite loops of release and feedback for all your code and deployment targets

Lean

Focus on producing value for the end-user, small batch sizes.

Trust

Having a high-trust culture has a strong impact on both IT performance and organizational performance.



Culture

People and process first. If you don't have culture, all automation attempts will be fruitless

Automation

Trunk-based development, continuous integration, and automated testing measurably improve both IT performance and organizational performance.

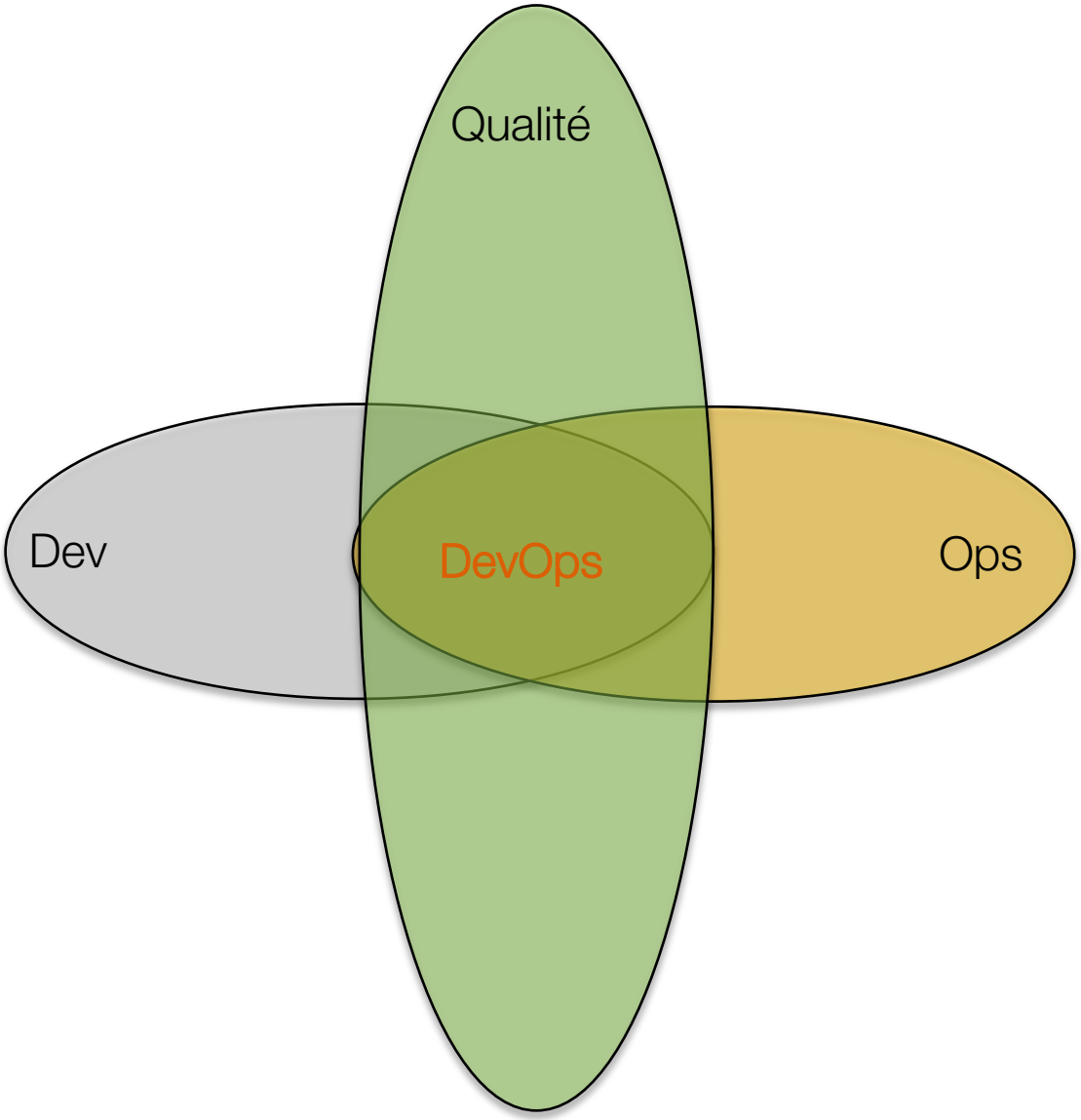
Measurement

If you can't measure, you can't improve. A successful Devops implementation will measure everything it can as often as it can… performance metrics, process metrics, and even people metrics.

Sharing

Sharing is the loopback in the CAMS cycle. Creating a culture where people share ideas and problems is critical.

DevOps au croisement



DevOps, les écueils

- « La sécurité ne peut pas fonctionner avec le DevOps »

- Le DevOps est l'outil "ultime" pour la sécurité des développements. Les personnes responsables de la sécurité peuvent injecter, à l'aide des outils et mécanismes idoines, de la sécurité plus tôt dans les phases de développement

- Afin d'améliorer la sécurité globale du code qui est mis en production.

DevOps, les écueils

- « Adopter le DevOps permet de se passer d'experts en sécurité »
- La plupart des développeurs ne sont pas des experts en sécurité.
- Les experts en sécurité sont nécessaires, plus que jamais, afin de collaborer avec des personnes qui ont d'autres compétences.

DevOps, les écueils

- « Les entreprises et le DevOps sont comme l'eau et l'huile »

- Les entreprises fonctionnent en DevOps, tout comme elles fonctionnent avec les méthodologies Agiles.
- Le but de DevOps est de réduire le "Time To Market", tout en conservant
  - la qualité,
  - la disponibilité,
  - la sécurité

- C'est ce qui est recherché dans tout business.

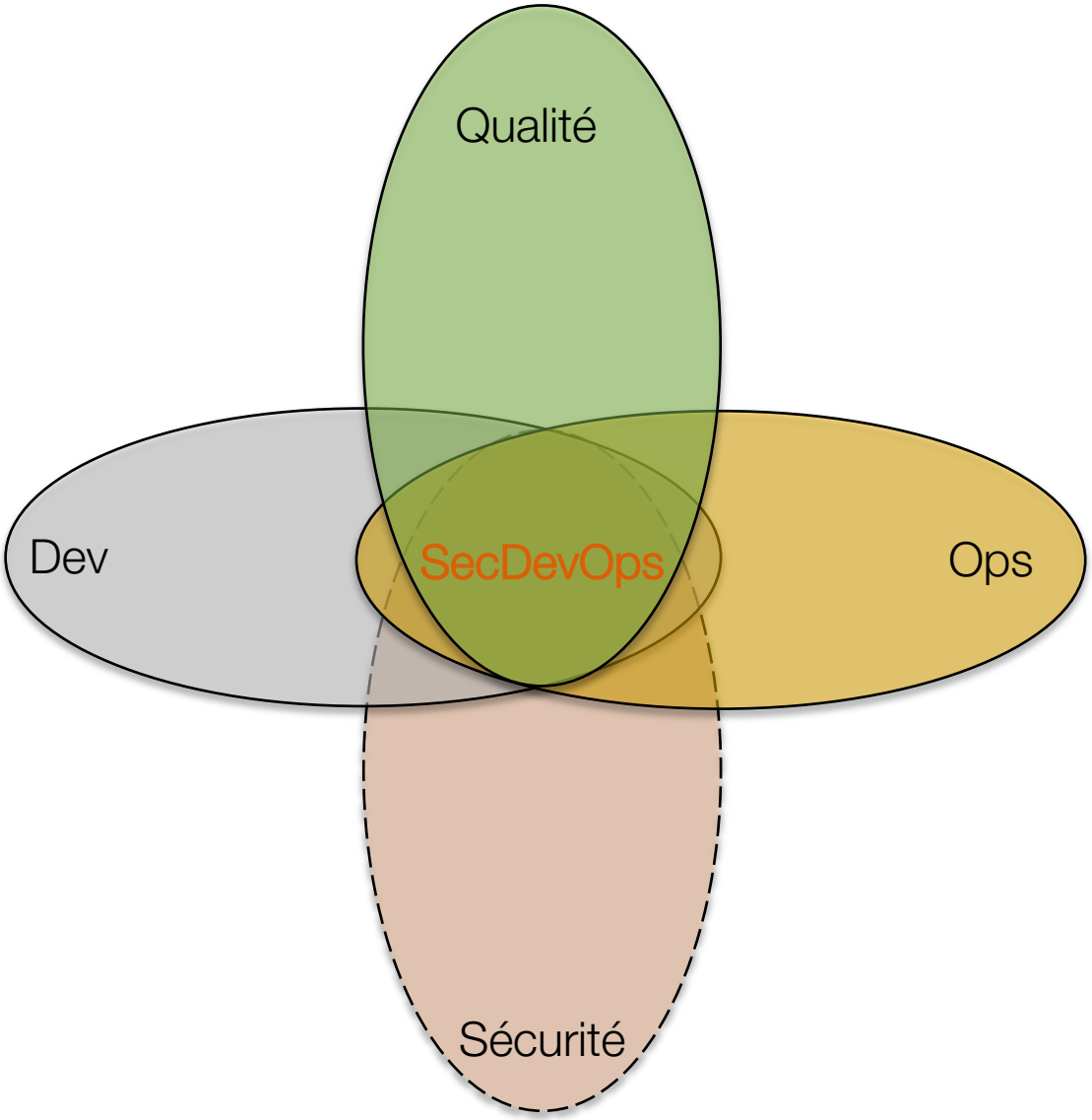
DevOps, les écueils

- « Si on peut faire du DevOps on faire facilement du SecDevOps »

- Changer le nom sans changer les méthodes ne fonctionne pas
- Utiliser les principes DevOps en conservant la sécurité dans son périmètre fonctionnel oublie un point essentiel :
  - l'intégration inter-fonctionnels

- Les experts sécurité doivent travailler en coopération avec les équipes du projet et depuis le début du projet.
- Tous comme les Ops, les Devs et la qualité doivent s'adapter à ces méthodes, les experts sécurité doivent aussi adopter ces nouveaux paradigmes.

SecDevOps au croisement



SecDevOps, les avantages

- Adopter le DevOps peut permettre de plus grands changements que les méthodes qui ont vu le jour dans le passé :
  - Ajouter des outils d'analyse de code dans les process de développement et permettre des corrections avant même le déploiement
  - Automatiser les outils d'attaque sur des applications en pré-production et ainsi empêcher les applications d'être déployées si elles présentent des vulnérabilités
  - Continuellement tester l'environnement de production pour y rechercher automatiquement des faiblesses
  - Adopter la future génération d'outils de tests de sécurité pour améliorer la qualité intrinsèque des développement
  - Les outils de centralisation de la configuration des systèmes et des applications permettent d'avoir une vision de la plate-forme complète en un coup d'œil.

Questions

Merci