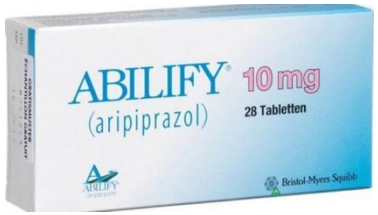
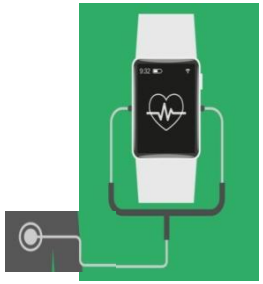
sécurité et IOT
dans l'univers de la santé

1er constats et pistes d'étude

L'IoT : la médecine sans médecin* ?

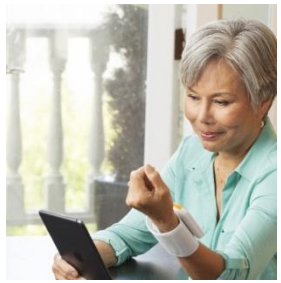
confort à 20 ans
santé à 60 ?





professionnels

perso



omniprésents

learning machine

Blockchain

traitement médical

B2B
B2B2C

UBER

* Guy Vallancien (Gallimard)

Impact :
sur la sécurité des SI

Fuites de données sensibles

LA VOIX DU NORD

Région > Béthune et ses environs > Béthune

Béthune : des dossiers médicaux en accès libre sur le web depuis au moins trois jours

PUBLIÉ LE 18/02/2016

Paralysie / Indisponibilité

Les systèmes de l'établissement psychiatrique d'Allonnes et du Pôle Santé du Bailleul ont été infectés. Pas simple d'éliminer les virus, mais les dossiers des patients sont saufs

ouest france

Pays de Loire – publié le 27/02/2016 à 05:57

- Monétisation des données dérobées :
  - Un dossier médical piraté se revend jusqu'à 200 dollars sur le Dark Web en 2016
  - Des intérêts évidents : assureurs, laboratoires, industries pharmaceutiques
- Un rapport de force à l'avantage des cyberattaquants :
  - Des SI de santé faiblement sécurisés, nettement moins sécurisés que ceux du secteur bancaire par exemple
  - Une relative impunité des cyberattaquants (actions extraterritoriales)
  - Des outils de hacking disponibles à foison sur Internet

Sécuriser les SI de santé :
des obligations …

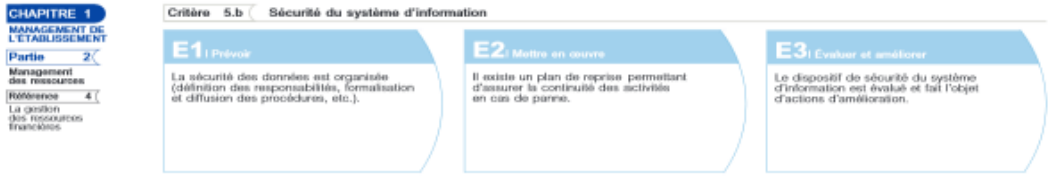
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales

Arrêté du 1er octobre 2015

HAS
HAUTE AUTORITÉ DE SANTÉ

Certification des établissements de santé



asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

Agrément des hébergeurs de données à caractère personnel

- Article L1111-8 du code de la santé public :
  - Environ 90 hébergeurs de données de santé agréés à date
  - Référentiel d'exigences de sécurité (formulaire P6)
- Evolution prochaine du dispositif :
  - courant 206 : agrément → certification
  - Référentiel d'exigences : ISO 27001 avec compléments ISO 27018 et spécificités santé

RÉPUBLIQUE FRANÇAISE
JOURNAL OFFICIEL
LOIS ET DÉCRETS

Loi Santé n° 2016-41 du 26 janvier 2016

- Création des GHT (groupement hospitalier de territoire) :
  - mutualisation des SI autour d'établissements référents

Sécuriser les SI de santé :
une incitation

Programme Hôpital Numérique

- Objectif : Elever le niveau de maturité IT des établissements sanitaires et sociaux
- Atteinte d'un niveau minimum : 3 prérequis dont l'un est la confidentialité
- Dépôt dossier jusqu'au 31/12/2016 : soutien financier de l'ARS pour les sélectionnés

Guides et bonnes pratiques des agences du secteur

- ASIP Santé :
  - guides et référentiels
- ANSSI :
  - guides et référentiels
- ANAP :
  - Accompagner le secteur médico-social
  - Piloter l'établissement
  - Externaliser son SI

Association pour la promotion de la sécurité des systèmes d'information de santé

- réseau de professionnels actifs contribuant au développement de la sécurité des SI de santé
- promotion des outils élaborés par les Instances Nationales : ANSSI, DGOS, ASIP Santé

Les obligations de cybersécurité :
(pour mémoire les OIV)

ANSSI

L'article 22 de la Loi de Programmation Militaire (LPM) a introduit des dispositions spécifiques à la sécurité pour la protection des Systèmes d'Information d'Importance Vitale (SIIV)

12 secteurs d'activité critiques pour environ 230 Opérateurs d'Importance Vitale

1 Appliquer aux SIIV des règles de sécurité

2 Notifier à l'administration les incidents

3 Soumettre les SIIV à des contrôles de sécurité

4 Mettre en place des mesures d'urgence décidées par le Premier ministre

20 règles de sécurité génériques fixées dans les arrêtés sectoriels à paraitre

L'Etat s'organise :
aujourd'hui en France

Sanction pécuniaire prononcée par la CNIL à l'encontre de Google

Par une délibération du **10 mars 2016**, la CNIL a prononcé une sanction pécuniaire publique à l'encontre de la société Google pour non-respect de la mise en demeure publique du 21 mai 2015 qui l'enjoignait de mettre en œuvre la procédure de déréférencement sur l'intégralité des extensions du nom de domaine de son moteur de recherche. La CNIL a constaté que la solution proposée par Google consistant à circonscrire le déréférencement sur l'intégralité des extensions de son moteur de recherche aux seules requêtes émanant du pays du demandeur, "*déterminé (…) par l'adresse IP de l'utilisateur*", demeure incomplète. Selon la CNIL, "*seule une mesure s'appliquant à l'intégralité du traitement lié au moteur de recherche, sans distinction entre les extensions interrogées et l'origine géographique de l'internaute effectuant une recherche*" permettrait de rendre effectif le droit au déréférencement.

Loi de santé

Art. L. 1111-8-2. – Les établissements de santé et les organismes et services exerçant des activités de prévention, de diagnostic ou de soins signalent sans délai à l'agence régionale de santé les incidents graves de sécurité des systèmes d'information. Les incidents de sécurité jugés significatifs sont, en outre, transmis sans délai par l'agence régionale de santé aux autorités compétentes de l'État.

La CNIL définit précisément les principes clés de la protection de données personnelles (http://www.cil.cnrs.fr/CIL/spip.php?article1390 ou http://www.cnil.fr)

Les Etats s'organisent :
demain dans la communauté européenne

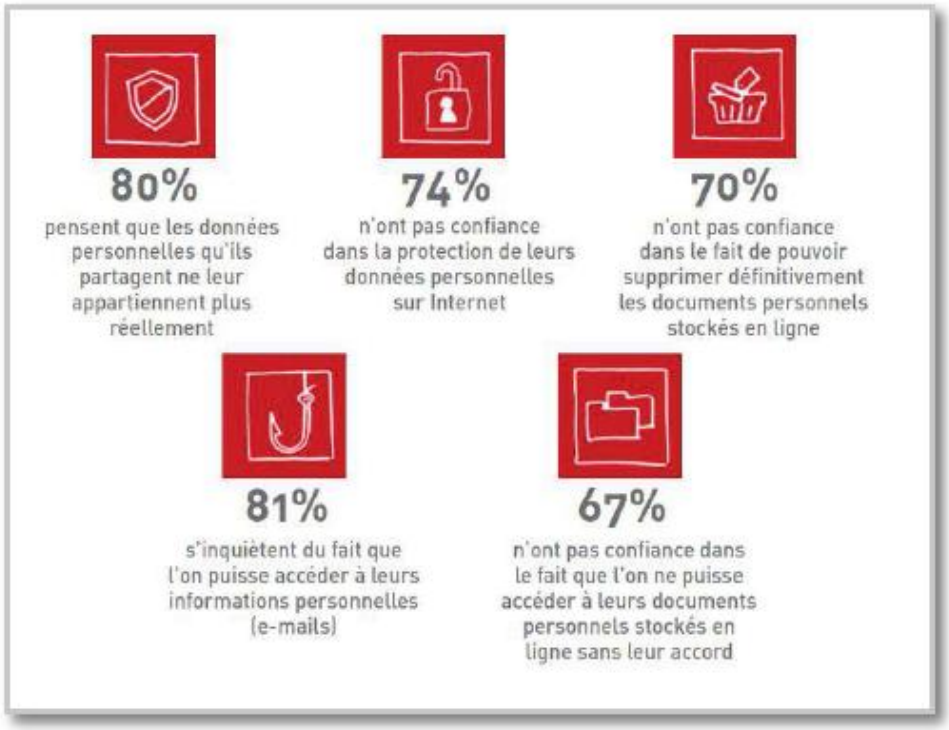
Le Règlement européen « eIDAS » sur l'identification électronique et les services de confiance a été publié dans le journal officiel européen

Au niveau européen, la protection des données à caractère personnel est couverte par deux directives principales : la directive sur la protection des données (directive 95/46/CE) et la directive relative à la vie privée et aux communications électroniques (2002/58/EC)

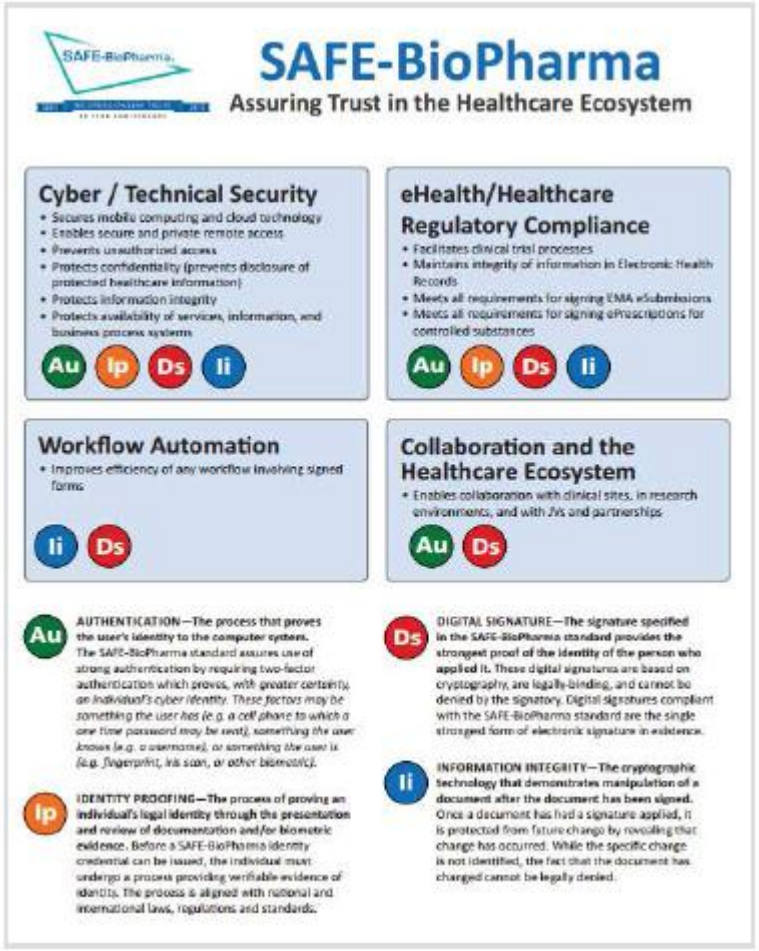
L'UE a approuvé le 15 décembre au soir le règlement sur la protection des données (RGDP ou GDPR), qui renforce considérablement les pouvoirs de sanction des Cnil nationales.

Remarque : Un nouveau règlement sur la protection des données personnelles vient d'être adopté par le parlement européen le 14 avril dernier. l'adaptation des niveaux de **confiance** et de **sécurité** au degré de **risque.**

Sécurité et confiance :
rassurer et montrer



Source : TNS Sofres-LaPoste



Source : https://www.safe-biopharma.org/

de quoi parle t'on ?
multiplication des acteurs

un ex.
le mobile

praticiens

traitement du patient

utilisation des données

traitement des données

réseaux (fil)

constructeurs

IT (propriétaire)

capteurs

cerveaux d'oeuvre

maitre d'œuvre

médecin | autres | patient

utilisation (pro) | utilisation (autres) | utilisation (perso)

traitement données (interne) | traitement données (externe)

réseaux (fil – wifi – BT – LTE - LoRa - Sigfox …)

IT (propriétaire) | IT (ouvert)

IoT

praticiens + patients + nouveaux entrants

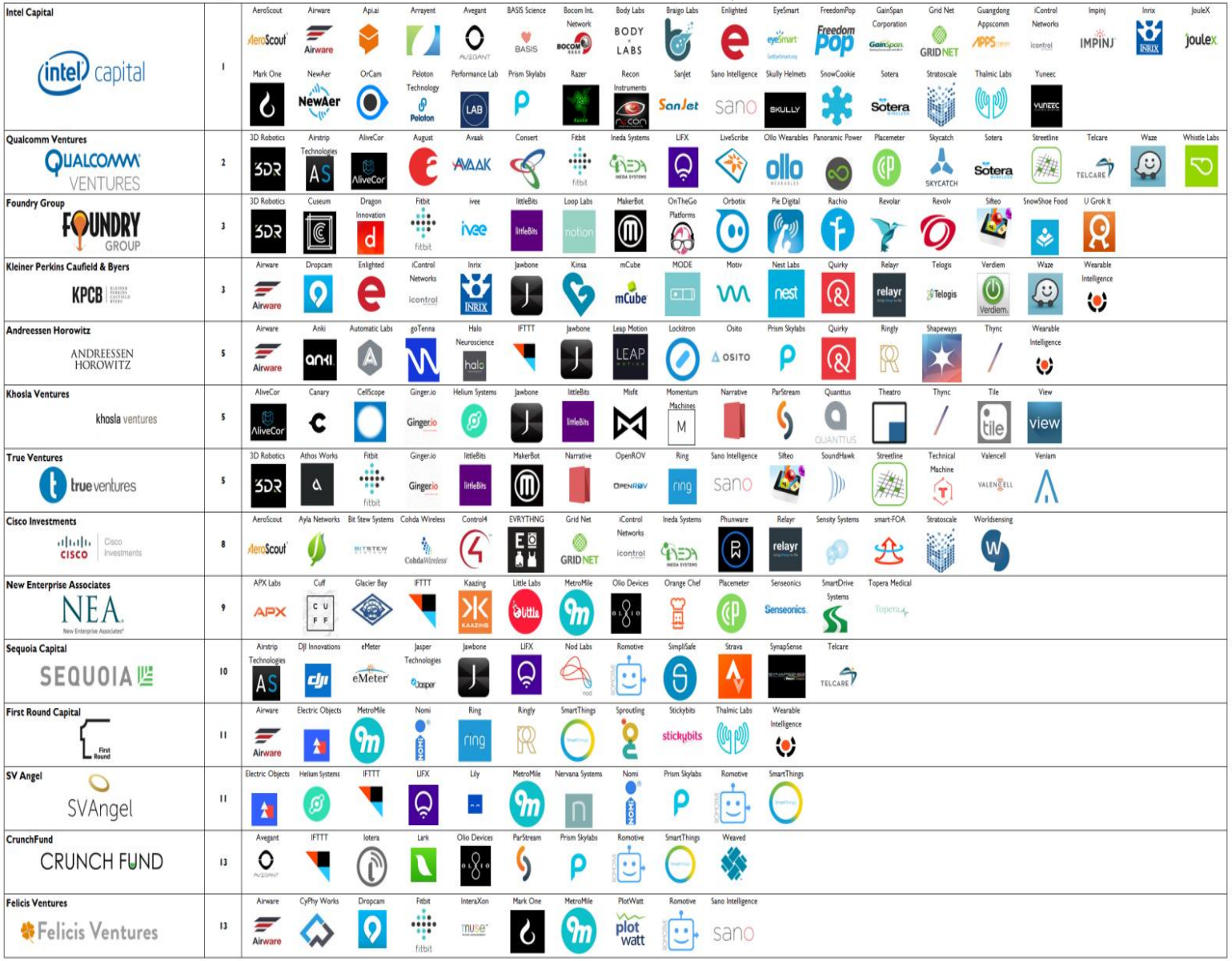
constructeurs + nouveaux entrants

hier → demain

de quoi parle t'on ?
multiplication des investisseurs

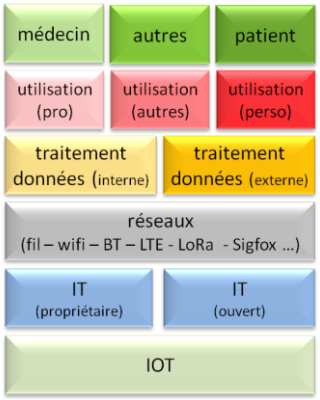
The Most Active IoT Investors

VCs Ranked by Unique IoT Investments, 2010 - 2015 YTD (11/24/15)



CB INSIGHTS

mais encore ?
sécu, confiance, risques, business



risques :
sur les données : exactitude, intégrité, perte, détournement, usurpation … ;
sur les objets : toxicologiques, interférence, identité … ;
fake sur pusshy et pub à venir => ciblage ??;
acceptation des risques, acceptation de l'écosystème.

confiance :
celui qui traite les données;
celui qui utilise pour le diagnostique;
le praticien;
le patient.

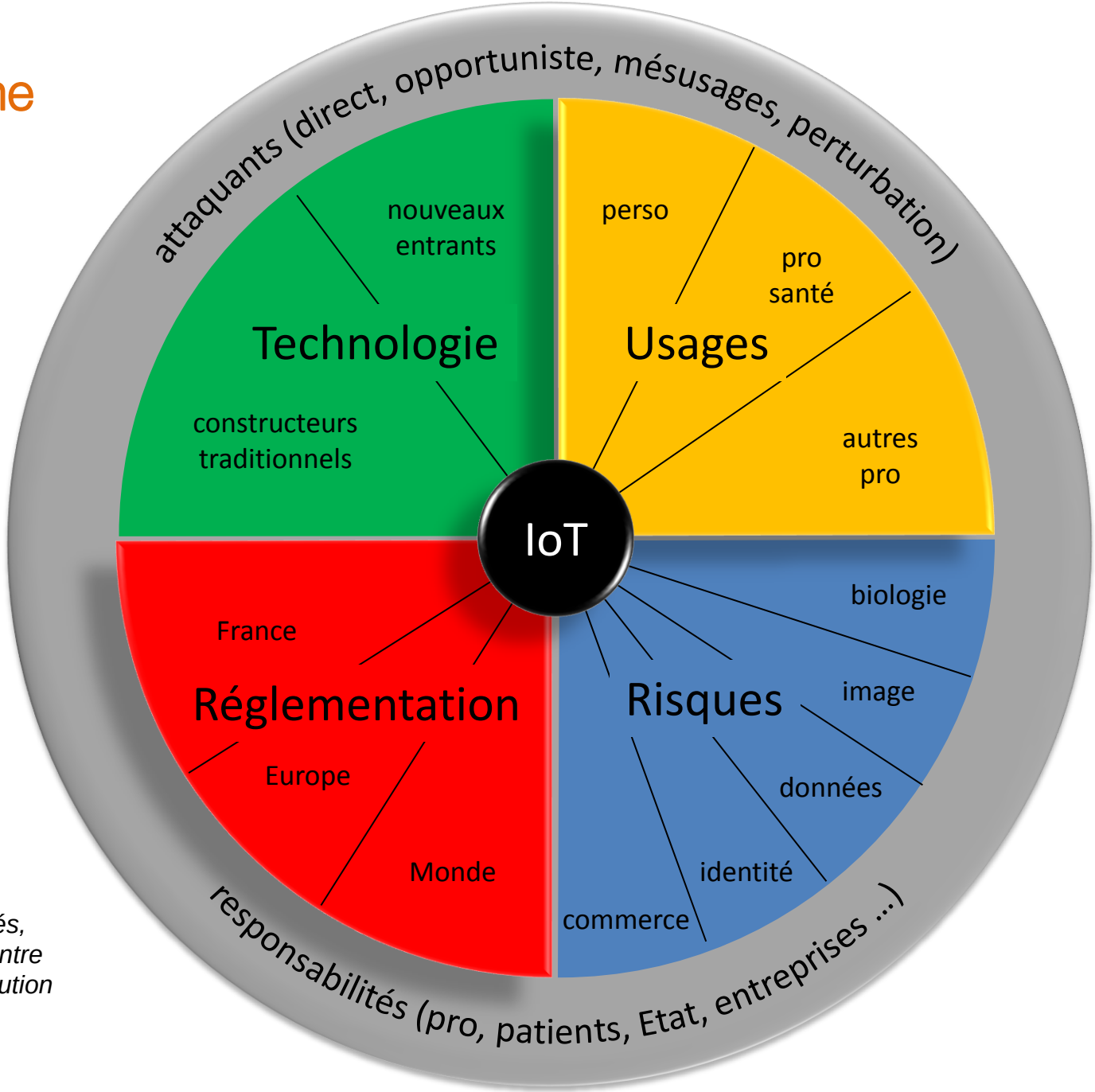
sécurité :
des dispositifs;
de la transmission d'informations;
du traitement et du stockage;
de l'utilisation des données;

business :
business vs santé ?;
nouvelles sources de revenus ? pour qui ? comment ?;
source d 'économie ? pour qui ? (pro, patient, Etat);
Blockchain Uber, maisons médicales (bénéfices patients)

Impact
sur l'écosystème

1,2M d'objets connectés
100000 trackers
vendus en Décembre
dont 50% en IdF

GFK : en France en 2015



« avec la santé connectée, nous réduisons les temporalités, développons la coordination entre les acteurs et le suivi de l'évolution des maladies chroniques »
(Novartis)

les acteurs nouveaux entrants
sécurité vs business

IoT Endpoint Security

- Protect operational hardware platform
- Protect legacy & new applications/SW
- Protect privacy of operators and data

Gateway Security

- Securely connect devices to cloud
- Monitor/Manage security of legacy/brownfield devices
- Monitor/Manage connected device data flow and access

Network Security

- Secure network devices
- Manage security across network boundaries
- Integrate network security policy and process with Gateway and Cloud security policy

Cloud & Data Center Security

- Protect DC infrastructure platform
- Managed security for data access between applications and operators/users
- Security and management for on-premise and cloud
- Protect Big Data Infrastructure

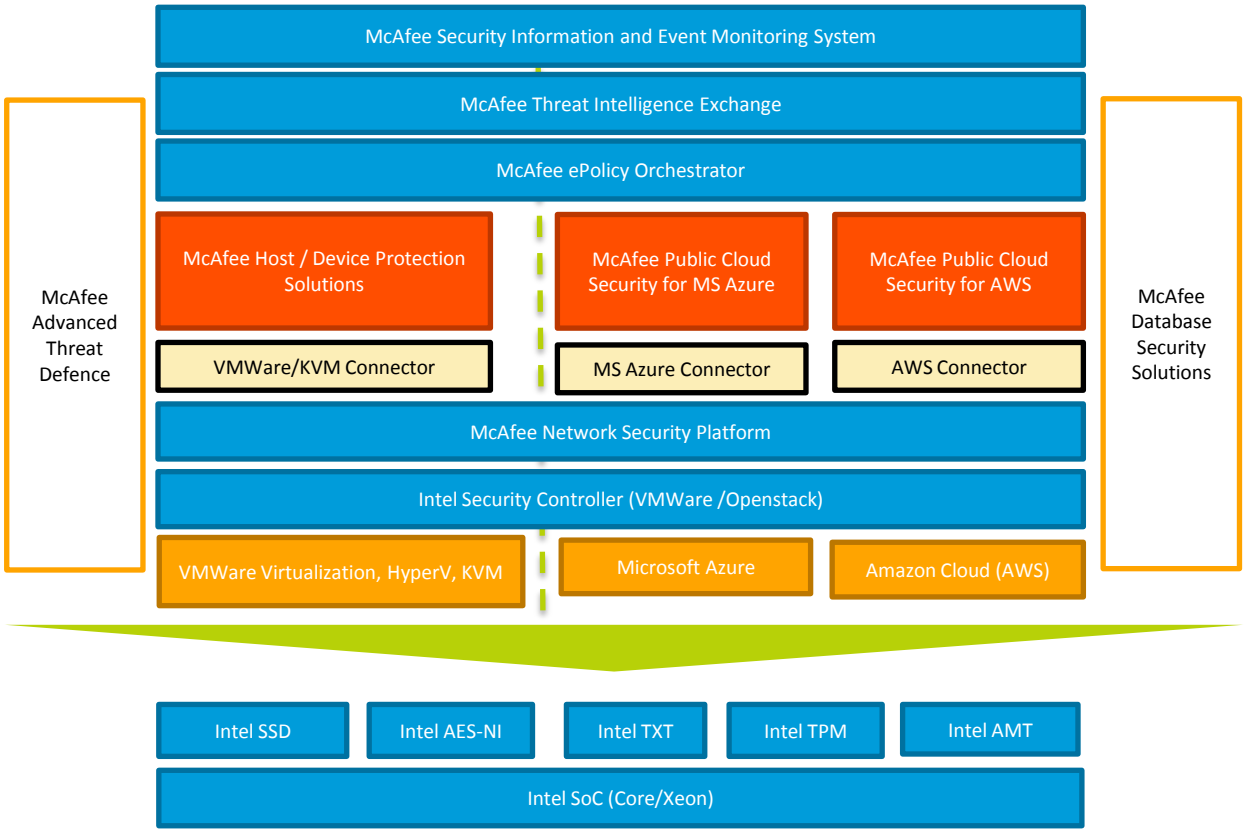
IoT Security Requirements End to End

les acteurs nouveaux entrants
sécurité vs business

vision :
Intel met l'emphase sur la fourniture de bout en bout de solution IoT qui ciblent les objets quelque soit le réseau et l'environnement (filaire, Wifi, Cloud)

plus value :
Intel fédère et simplifie la connectivité et la sécurité de l'IoT

points clés :
Intel est un des plus gros investisseurs dans l'IoT.
Intel possède une double casquette fondeur et éditeur très complémentaire.



les acteurs nouveaux entrants
sécurité vs business

Notre vision :

- « Porte d'entrée » pour dans les SI des entreprises
- Frontière de plus en plus poreuse entre le monde personnel et professionnel
- Ecosystème de l'objet connecté complexe : matériel/applicatif/réseau/Cloud
- 1er Objet connecté non sécurisé : le Smartphone : Plus de 5 Milliards dans le monde
- Croissance exponentielle non maîtrisé des risques potentiels
    - Pour les Entreprises : Vol de données/ Piratage/ chantage
    - Pour les Personnes : usurpation d'identité, vol jusqu'à « l'assassinat »(Pacemaker)

Notre Positionnement / Plus Value

- Vison de la sécurité à 360° : du réseau à l'objet et de l'application au serveur
- 2 axes majeurs :
    - Sécurisation des réseaux et des Cloud
    - Sécurisation des terminaux « ouverts » : Smartphone/ Montres connectées…
- Partenariat technologique : Security By Design

Une solution disponible aujourd' hui pour Smartphone et Tablettes : Mobile Threat Prevention

- Protection contre les applications malveillantes :Facebook Malicious Chat
- Protection contre les attaques réseaux : Man in the Middle
- Protection contre les Exploit OS

Plan d'action :

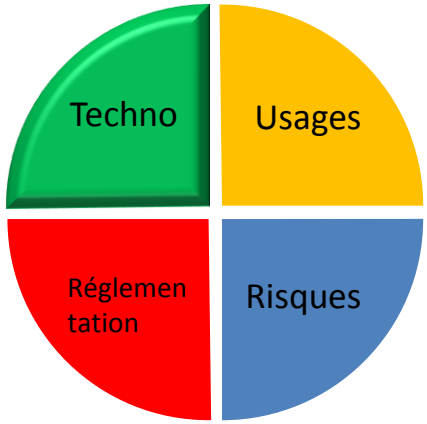
Développer les partenariats pour vous protéger:

Check Point and Argus Cyber Security develop solution to car hacking

A car accident in Tokyo, Japan. Photo credit: Torsodog / Flickr

This project brings together two sets of teams who have built a name for expertise in their fields, protecting the public against automotive mischief

Zoom
Techno

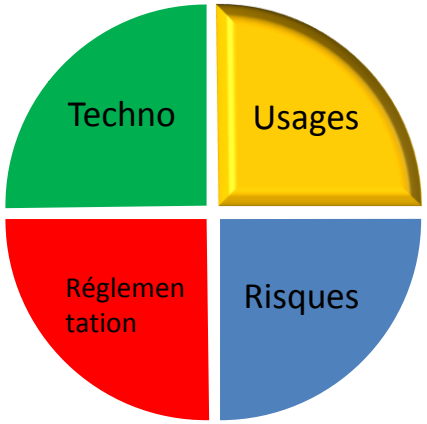


Constats :
n’est plus réservée aux seuls professionnels
le grand public a accès à des solutions pro très facilement
les solutions sont « tout en un » le détecteur, le diagnostique, la solution
production massive d’informations … non contrôlées
Smart building, Smartcity
Machine Learning
Blockchain …
réseaux, l’infra, (Lifi)

Recommandations :
réglementaire
au niveau des équipementiers
médias

Actions
veille, observation, POC

Zoom
Usages

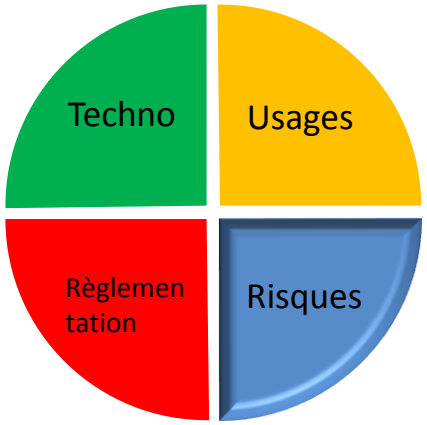


Constats :
utilisation de plus en plus importante des objets connectés par les pro
mais surtout par les individus
usages : confort, sport, médecine en fonction de la personne
voir étude Apssis
confiance justifiée ou non
IoT = c'est moi
IoT vs IoPro

Impacts :
l'utilisation facile des données font perdre à celle-ci leurs notions de « précieux et personnel»
droits d'utilisation

Actions :
veille, observation
sensibilisation via les différents acteurs ?
règlementation ? (plus forte ?)

Zoom
Impacts

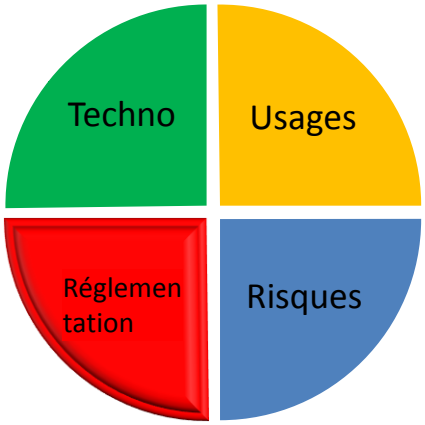


ratio impacts / risques

1. sur les missions (fort / fort)
2. sur la capacité de décision (moyen / fort)
3. sur la sécurité des personnes (fort / fort)
4. sur le lien social interne (moyen / fort)
5. sur le patrimoine intellectuel ou culturel (moyen / fort)
6. sur l'image (fort / fort)
7. sur la non conformité (fort / fort)
8. juridiques (fort / fort)
9. sur l'environnement (moyen / moyen)
10. financier (fort / fort)

Zoom
Légal

à qui appartient une donnée de santé ?



Constats:
peu de normes communes et règlementation pas vraiment en phase avec l'écosystème actuel. Le grand public n'est pas cohérent, situation paradoxale. Les entreprises s'accommodent des lois, l'Etat sous influence ?

Reco :
besoin de normes et de lois internationales au niveau des objets, des modes de transport et de stockage. Elargir l'écosystème de santé.

Actions :
organiser des RDV d'information vers les utilisateurs. Etudier les travaux du domaine

"Nurse, get on the internet, go to SURGERY.COM, scroll down and click on the 'Are you totally lost?' icon."

pour l’instant …

rdv pour la 2ème partie à venir

Merci

ont proposé cette étude :

orange™ Business Services

avec la participation de :

intel Security

Check Point SOFTWARE TECHNOLOGIES LTD.

points de contacts :
philippe.loudenot@sq.social.gouv.fr
philippe.landeau@orange.com
guillaume.hamrit@intel.com
mmontariol@checkpoint.com