Cybersécurité

- Pharmacien
- Évaluation en vie réelle des produits de santé
  - Statistiques appliquées à l'évaluation clinique des dispositifs médicaux (DM
  - Sécurité informatique dans les environnements de recherche et de santé
- Thèse de doctorat en Data-sciences
- Thèse d'exercice : "La sécurité informatique des données patient en officine"
- Enseignant-chercheur Institut des Sciences Pharmaceutiques et Biologiques (ISPB)

francois.bettega@univ-lyon1.fr

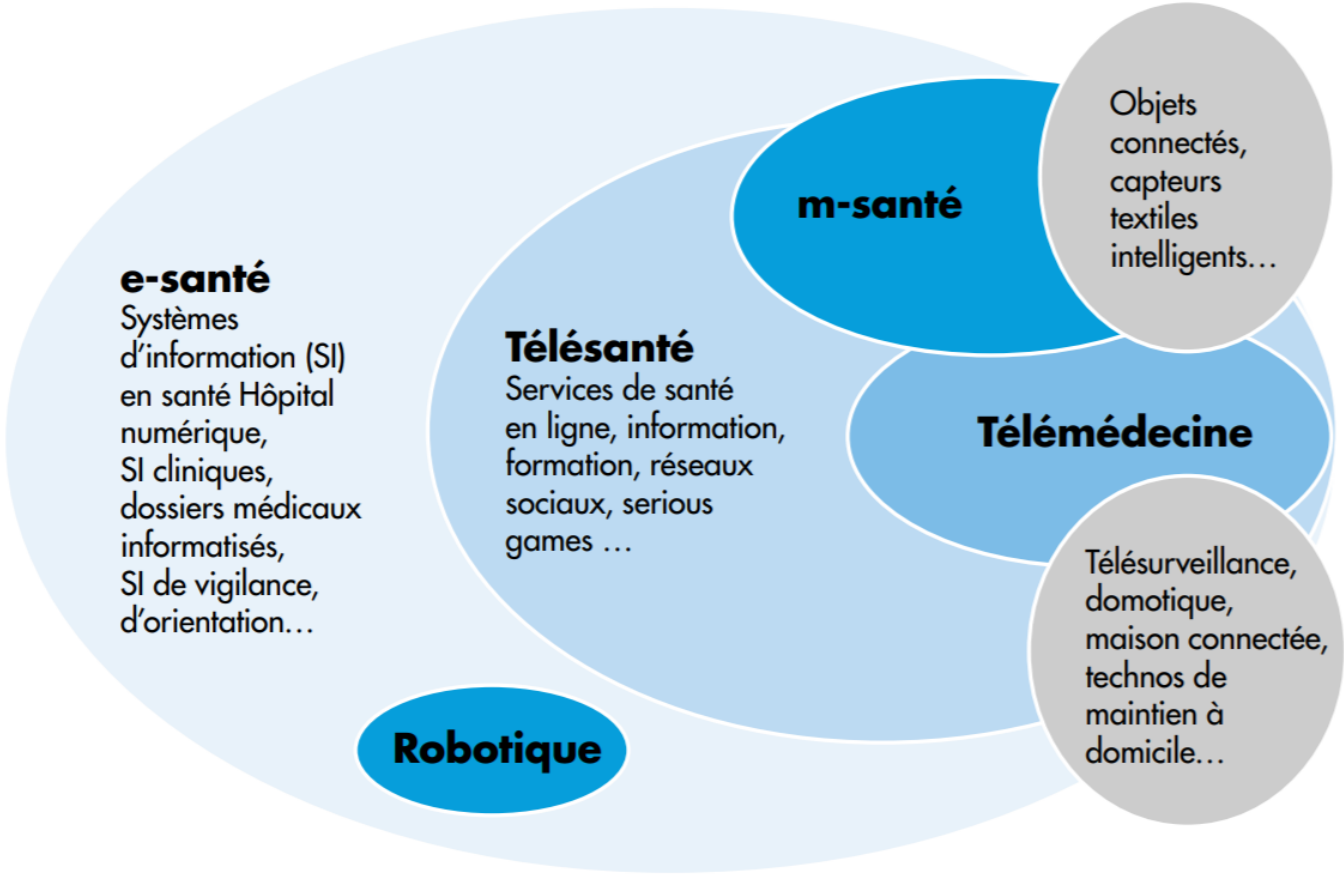
- Gestion de données de santé dans les pharmacie d'officine
- Gestion de données de santé dans les établissement de santé, recherche clinique
- Recherche clinique pour l'industrie pharmaceutique
- Recherche clinique, règlementaire dans les dispositifs médicaux
- Recherche clinique règlementaire dans les dispositifs médicaux de diagnostic in vitro
- Consulting réglementaire
- Laboratoire de biologie médicale

E Santé et pharmaciens

- E-santé et Cybersécurité
  - Avantages bien visibles
    - Accessibilité de l'information
    - Outils d'analyse
    - Prise en charge des patients ...
  - Risques liée a la cybersécurité
    - Méconnaissance des utilisateurs
- Objectifs vous sensibiliser aux risques liés à la sécurité informatique en lien avec la santé et en générale

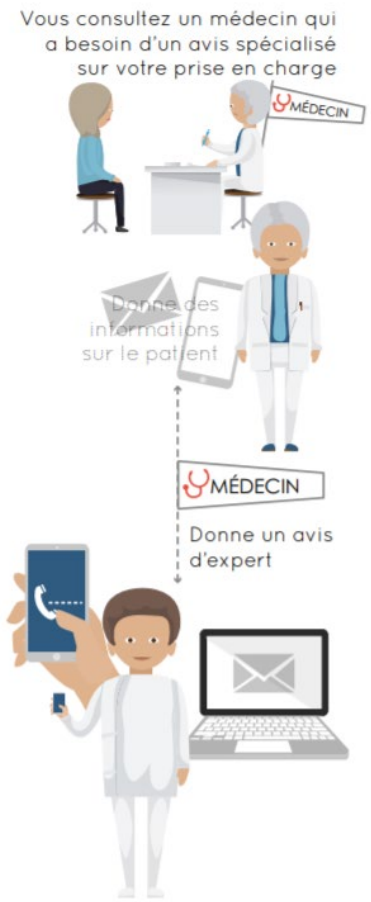
Cybersécurité

Sommaire


e-santé
Systèmes d'information (SI) en santé Hôpital numérique, SI cliniques, dossiers médicaux informatisés, SI de vigilance, d'orientation…
Télésanté
Services de santé en ligne, information, formation, réseaux sociaux, serious games …
m-santé
Objets connectés, capteurs textiles intelligents…
Télémédecine
Télésurveillance, domotique, maison connectée, technos de maintien à domicile…
Robotique

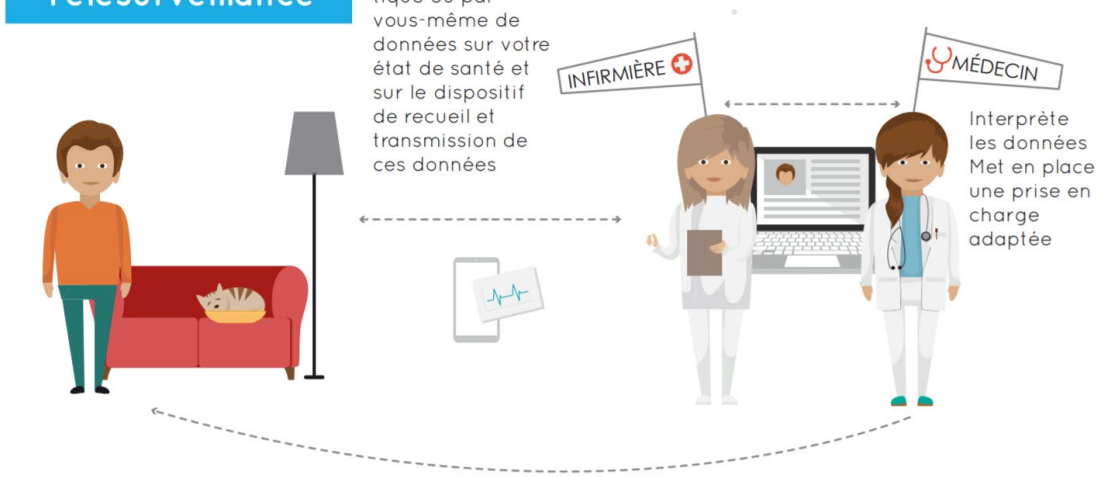
Téléconsultation

Téléexpertise



Télésurveillance

Recueil automatique ou par vous-même de données sur votre état de santé et sur le dispositif de recueil et transmission de ces données



Développement de la E-santé

Crise COVID accélérateur en e santé

Multiplication des acteurs: doctolib, qare, medadom

Teleconsultation 80000 en 2019, 19 millions en 2020

Médecins équipés: de 3500 à 30000

En 2020, plus de 350 000 applications concernant la santé étaient disponibles sur les différents magasins en ligne (App Store, Google Play Store, etc.)

Téléconsultation

Graphique 4 – Part des prestations des médecins généralistes libéraux réalisées en 2021 selon l'âge des patients						
						En %
	0-14 ans	15-29 ans	30-44 ans	45-59 ans	60-74 ans	75 ans et plus
Consultations	13,5	12,6	16,2	21,5	22,9	13,3
Visites	2,3	1,9	3,1	6,5	16,3	69,9
Téléconsultations	6,7	18,8	26,4	21,9	14,5	11,7

					En %
	Même commune	0-5 km	5-10 km	10-30km	Plus de 30 km
Consultations	49,6	13,1	16,0	15,3	6,0
Visites	52,8	13,3	15,3	12,3	6,4
Téléconsultations	44,6	14,0	14,4	16,1	10,8

Cadre législatif et support de l’information

Support de l’information

Supports de l’information historique

- Orale
  - *Conditionné à la seul éthique du praticiens Divulgation délibéré*
  - *Ephémère*

Supports de l’information historique

- Orale
  - *Conditionné à la seul éthique du praticiens Divulgation délibéré*
  - *Ephémère*
- Ecrits
  - *Existence physiques des documents*
    - Pertes/vols
    - stockages
    - Protections liée à l’existence physique de l’information

Supports de l’information historique

- Orale
  - *Conditionné à la seul éthique du praticiens Divulgation délibéré*
  - *Ephémère*
- Ecrits
  - *Existence physiques des documents*
    - Pertes/vols
    - stockages
    - Protections liée à l’existence physique de l’information
- Informatiques
  - *Accessible n’importe quand depuis n’importe ou*
  - *Difficulté de vérifier les interceptions lors de l’envoie*
  - *Outils de surveillance accessible et pas chère*

Cadre législatif

Cadre législatif

Loi informatique et liberté

- France a été en 1978 le 3eme pays d'Europe après l'Allemagne en 1971 et la Suède en 1973
- Article 1
- Chaque citoyen a des droits vis-à-vis des données collectées le concernant
  - droit de regard
  - droit d'opposition sauf obligation légale
  - droit de correction et de suppression

Cadre législatif CNIL

CNIL

- **Informer / protéger**
- **Accompagner /conseiller**
- **Contrôler et sanctionner**
- **Anticiper**


RGPD

General Data Protection Regulation (GDPR)

- RGPD, adopté par l'Union européenne le 14 avril 2016
  - diminuer les disparités entre règlements nationaux
- S'applique aussi aux entreprises non européennes traitant des données de citoyens européens
- DPO
  - Non obbligatoire en pharmacie
- Notion de sécurité par défaut
- Consentement **positif** et **explicite** aux stockages des données patients
- Droit à la portabilité (potentiellement difficile en pharmacie)

RGPD

RGPD est l'initiale de Réglement Général pour la Protection des Données et désigne la dernière réglementation européenne concernant les données personnelles, publiée en 2016 et devant entrer en application dans les états membres le 25 mai 2018

«**données à caractère personnel»,** toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale

« données concernant la santé», les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne

RGPD : Règlement général sur la protection des données

Le règlement no 2016/679, dit règlement général sur la protection des données (RGPD, ou encore GDPR, de l'anglais General Data Protection Regulation), est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel1.

Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne.

Il abroge la directive 95/46/CE

Données de santé

Données de santé

- Les données personnelles concernant la santé sont les données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne.
- Les informations collectées lors de l'inscription en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services (numéro, symbole ou élément spécifique attribué à une personne physique pour l'identifier de manière unique)
- Les informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle (y compris à partir de données génétiques, d'échantillons biologiques)
- Les informations concernant une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical (indépendamment de sa source : médecin ou autre PS, hôpital, dispositif médical ou test de diagnostic in vitro).
- Cette définition permet d'englober certaines données de mesure à partir desquelles il est possible de déduire une information sur l'état de santé de la personne.

« données génétiques», les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question;

«données biométriques», les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques;

Règlement RGPD

DÉFINITION DE LA DONNÉES DE SANTÉ

En France

- Pas de définition française légale
- ASIP Santé : « donnée susceptible de révéler **l'état pathologique de la personne** »

RGPD – art. 4 15)

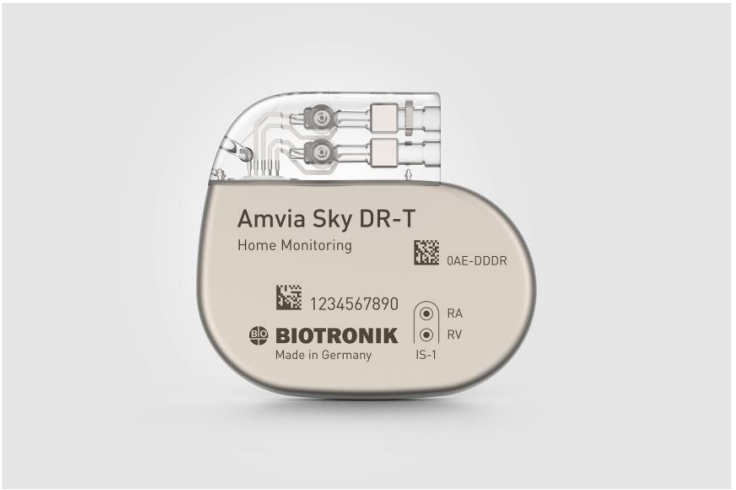
- « données à caractère personnel relatives à la santé **physique ou mentale** d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur **l'état de santé de cette personne** »

UN ORDINATEUR

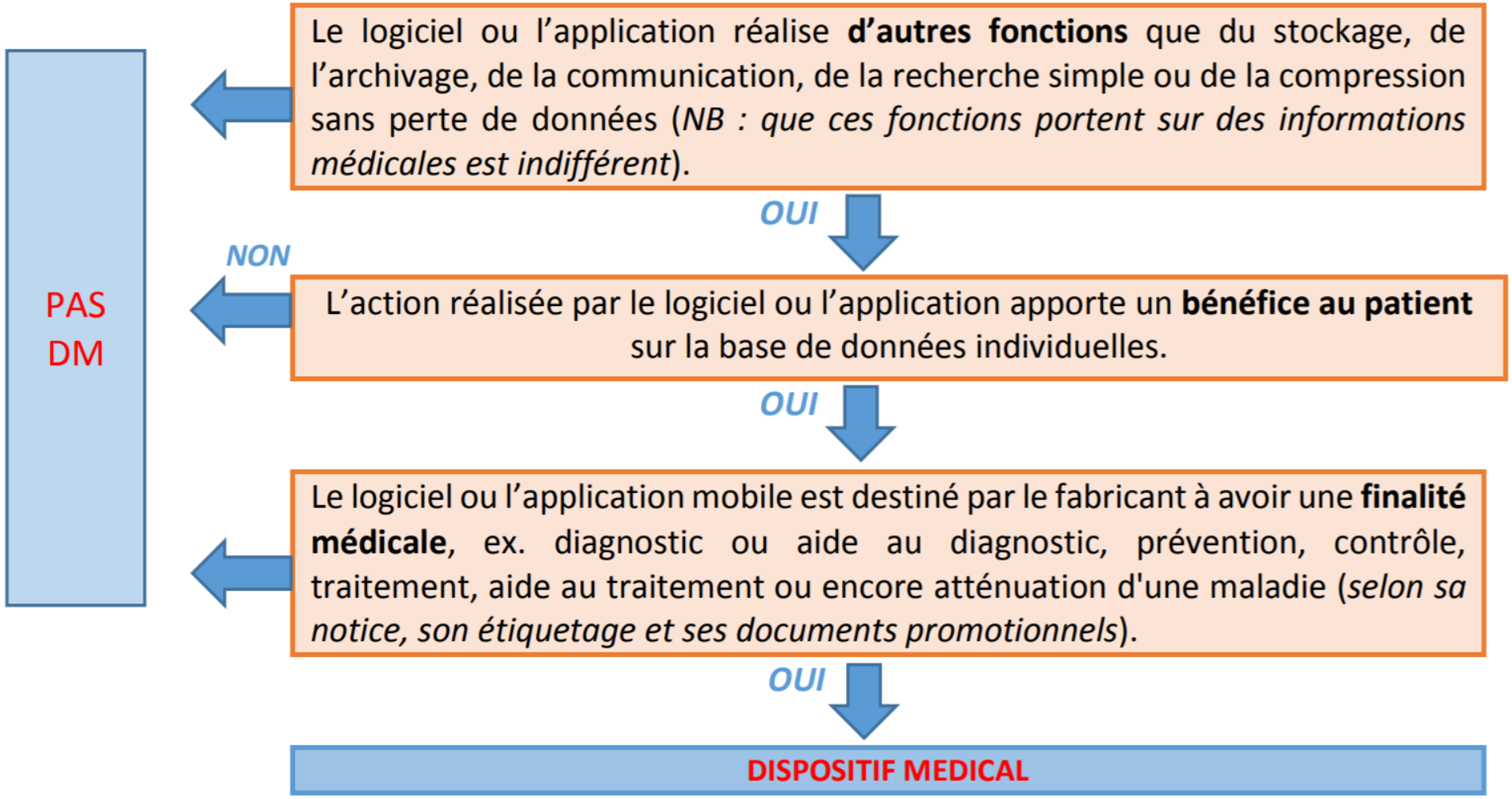
Un ordinateur est un système de traitement de l'information programmable tel que défini par Alan Turing et qui fonctionne par la lecture séquentielle d'un ensemble d'instructions, organisées en programmes, qui lui font exécuter des opérations logiques et arithmétiques.

Suis-je un ordinateur ?

Dispositif médicaux et informatique



Logicielle DM ou pas



Dispositif médicaux et informatique

- Problématique de cybersécurité pour le DM

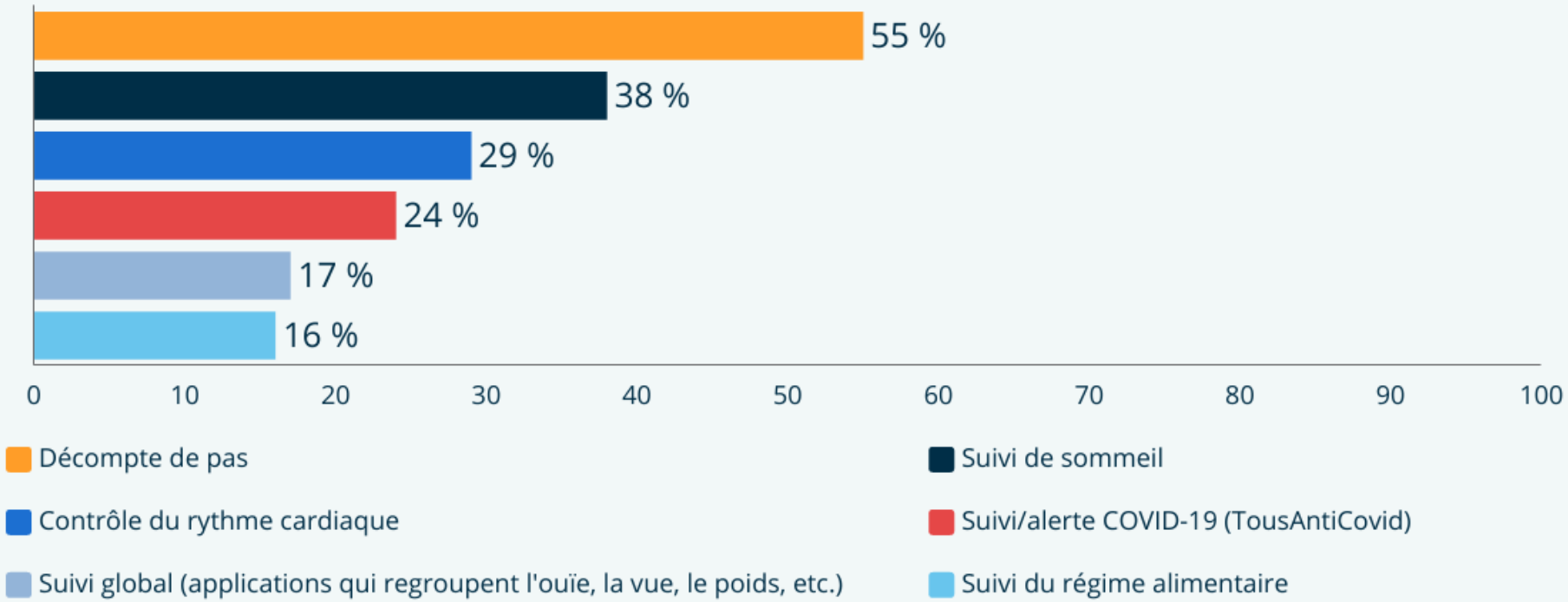
- Conséquence potentiellement grave
  - Pacemaker

- Question sur le self-hacking
  - Pompe a insuline
  - PPC
  - Pacemaker

Les applications

Pouvez vous me donner des exemples ou des informations semblant anonyme permettent de compromettre des données de santé ?

Quel type d'applications utilisez-vous ?



Source : Capterra Telemedicine Survey 2021.

Problème ? #StravaLeaks

- **Strava et la carte thermique mondiale**
  - **Série d'article du monde**
  - L'application de fitness Strava a publié une carte thermique mondiale basée sur les données GPS de ses utilisateurs
    - Identifier les périmètres des bases militaires secrètes en Syrie, Afghanistan, Irak, etc. , les itinéraires de patrouille, et les habitudes des militaires.
    - Membres de la sécurité présidentielle française et des agents du Secret Service américain : Risques de repérage des résidences officielles, hôtels, et routines opérationnelles.
    - Marins français ont utilisé des montres connectées avec Strava pour suivre leurs entraînements physiques. : Les données partagées ont permis de déduire les périodes de patrouille des sous-marins nucléaires.

Bonne pratique avec les données

Jeux de données

Jeux de données pas laisser trainer sur clef USB

- Chiffré les données

Eviter au maximum les duplications

- Script reproductible

Ne recueillir et saisir exclusivement les données absolument nécessaire

- **Il n’est jamais nécessaire de saisir les noms et prénoms**
  - Utilisation d’ID

Attention au mode de transmissions

Anonymisation

Anonymisation Vs Pseudonymisation

- Anonymisation irréversible
- En pratique irréaliste
  - Retrouvé un individu dans une base de données médicale en connaissant son sexe, code postal et sa date de naissance
  - Retrouvé un individu dans une base de données téléphoniques sur base de quatre points de géolocalisation
  - Retrouvé un individu dans une base de données de cartes bleues en connaissant quatre magasins et jours où celui-ci a utilisé sa carte

Source : https://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/
https://archive.wikiwix.com/cache/index2.php?url=http%3A%2F%2Fwww.sciencemag.org%2Fcontent%2F347%2F6221%2F536.abstract#federation=archive.wikiwix.com
https://archive.wikiwix.com/cache/index2.php?url=http%3A%2F%2Fwww.nature.com%2Fsrep%2F2013%2F130325%2Fsrep01376%2Ffull%2Fsrep01376.html

Pseudonymisation

Anonymisation Vs Pseudonymisation

- Pseudonymisation
  - La pseudonymisation est un traitement de données personnelles réalisé de manière à ce qu'on ne puisse plus attribuer les données relatives à une personne physique sans information supplémentaire.
  - Facile, Nécessaire mais insuffisant

La seul solution pour anonymiser des données et souvent l'aggrégations

Même si pas parfait il obligatoire de tous faire pour anonymiser les données

Source : https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles

Certification des hébergeurs de données de santé

Les modalités d'hébergement de données de santé à caractère personnel sont encadrées par l'article L.1111-8 du code de la santé publique :

- toute personne physique ou morale qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi médicosocial pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, doit être agréée ou certifiée à cet effet ;

- l'hébergement exige une information claire et préalable de la personne concernée par les données de santé hébergées et une possibilité pour celle-ci de s'y opposer pour motif légitime.

Quel type d'hébergement?

- l'hébergement de données de santé sur support papier, qui doit être réalisé par un hébergeur agréé par le ministre de la culture (procédure déjà existante – cf. décret 2011- 246) ;
- l'hébergement de données de santé sur support numérique dans le cadre d'un service d'archivage électronique, qui doit être réalisé par un hébergeur agréé par le ministre de la culture dans des conditions qui seront définies par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés et des conseils des ordres des professions de santé ;
- l'hébergement de données de santé sur support numérique (hors cas d'un service d'archivage électronique) qui doit être réalisé par un hébergeur certifié dans des conditions définies par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés et des conseils des ordres des professions de santé.

La certification et les référentiels

Deux types de certificats seront délivrés aux hébergeurs pour deux métiers d'hébergement distincts :

- un certificat « hébergeur d'infrastructure physique » pour les activités de mise à disposition de locaux d'hébergement physique et d'infrastructure matérielle ;
- un certificat « hébergeur infogéreur » pour les activités de mise à disposition d'infrastructure virtuelle, de mise à disposition de plateforme logicielle, d'infogérance et de sauvegarde externalisée.

Le référentiel de certification s'appuie sur des normes internationales :

- la norme ISO 27001 « système de gestion de la sécurité des systèmes d'information » ;
- des exigences de la norme ISO 20000-1 « système de gestion de la qualité des services » ;
- des exigences de protection de données à caractère personnel pour lesquelles une conformité à la norme ISO 27018 confère une présomption de conformité
- et des exigences spécifiques à l'hébergement de données de santé.

Zoom HDS

Décret n°2018-137 du 28 février 2018

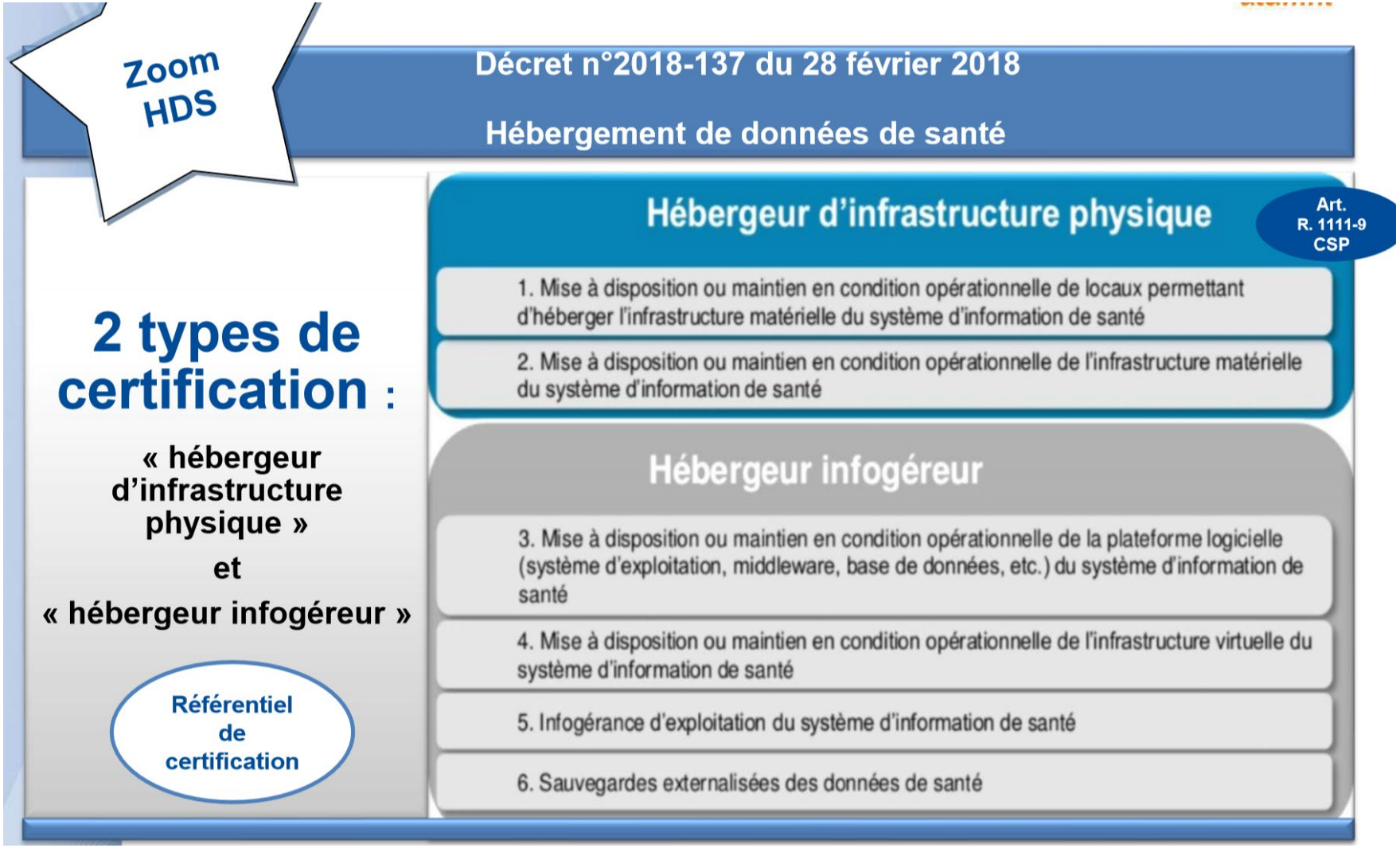
Hébergement de données de santé

Champ d'activités d'hébergement soumis à certification

(nouvel Art. R.1111-8 CSP):

« *l'activité d'hébergement de donnée de santé à caractère personnel* […] *consiste à héberger les données de santé recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales, responsables de traitement* […], *à l'origine de la production ou du recueil de ces données ou pour le compte du client lui-même* ».

Exception : « *ne constitue pas une activité d'hébergement, le fait de se voir confier des données pour une courte période par les personnes physiques ou morales, à l'origine de la production ou du recueil de ces données, pour effectuer un traitement de saisie, de mise en forme, de matérialisation ou de dématérialisation de ces données* ».


Zoom HDS
Décret n°2018-137 du 28 février 2018
Hébergement de données de santé
2 types de certification :
« hébergeur d'infrastructure physique »
et
« hébergeur infogéreur »
Référentiel de certification
Hébergeur d'infrastructure physique
Art. R. 1111-9 CSP
1. Mise à disposition ou maintien en condition opérationnelle de locaux permettant d'héberger l'infrastructure matérielle du système d'information de santé
2. Mise à disposition ou maintien en condition opérationnelle de l'infrastructure matérielle du système d'information de santé
Hébergeur infogéreur
3. Mise à disposition ou maintien en condition opérationnelle de la plateforme logicielle (système d'exploitation, middleware, base de données, etc.) du système d'information de santé
4. Mise à disposition ou maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information de santé
5. Infogérance d'exploitation du système d'information de santé
6. Sauvegardes externalisées des données de santé

La procédure de certification se fonde sur le processus standard de type système de management décrit dans la norme ISO 17021 :

- L'hébergeur choisit un organisme certificateur accrédité par le COFRAC (ou équivalent au niveau européen).

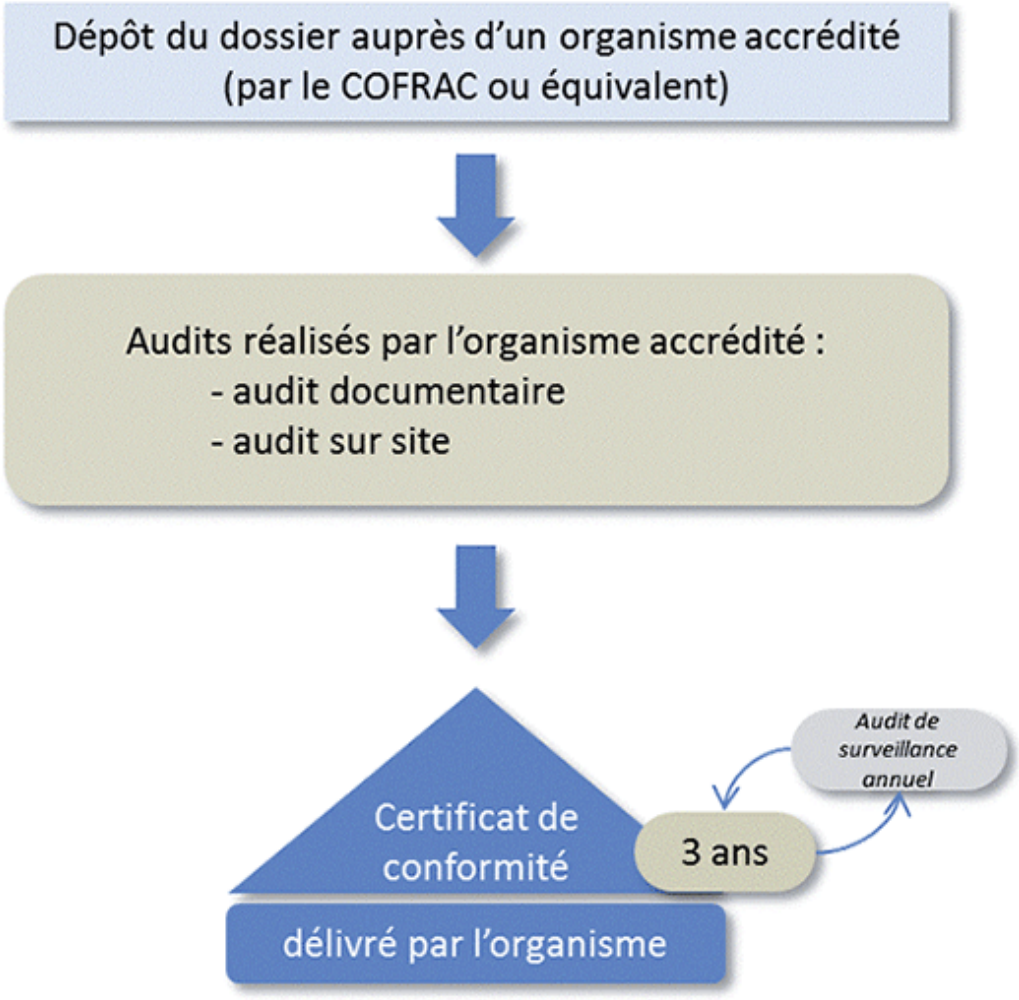
- Le cas échéant, l'organisme certificateur vérifie l'équivalence des éventuelles certifications ISO 27001 ou ISO 20000-1 déjà obtenues par l'hébergeur.

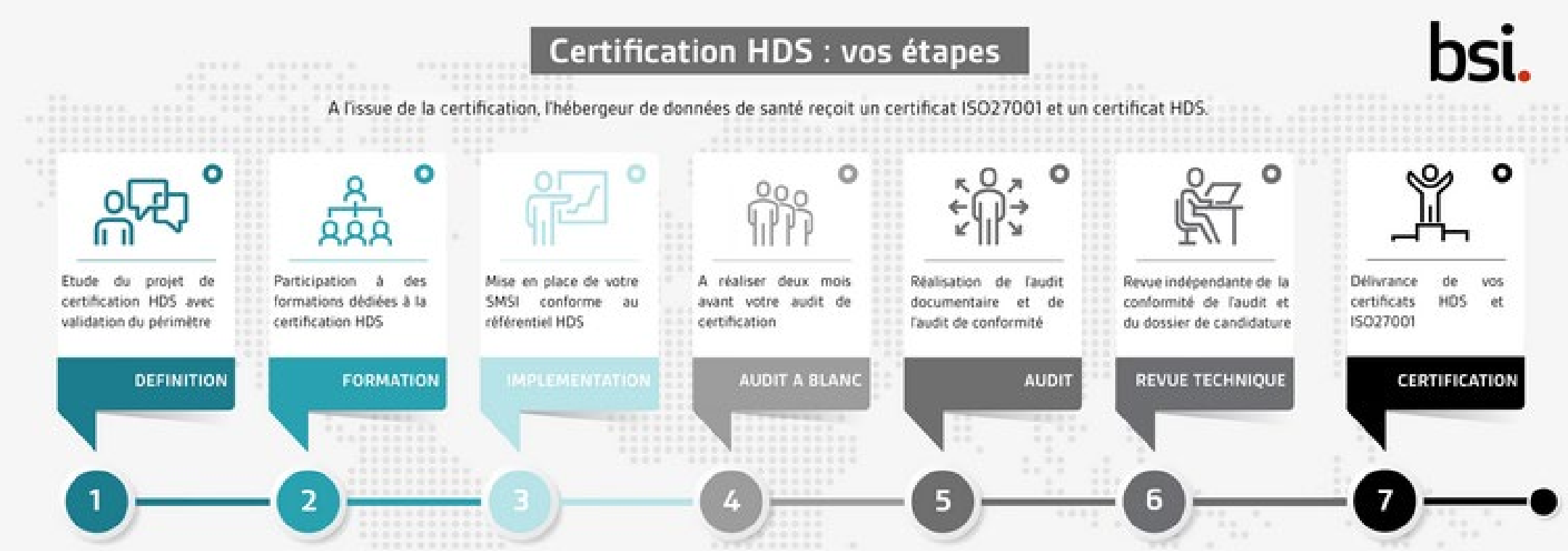
- Un audit en deux étapes conformes aux normes en vigueur est alors effectué :

  - **audit documentaire** L'organisme certificateur réalise une revue documentaire du système d'information du candidat afin de déterminer la conformité documentaire du système par rapport aux exigences du référentiel de certification

  - **audit sur site** Les preuves d'audit sont recueillies dans les conditions définies dans le référentiel d'accréditation. L'hébergeur dispose de trois mois après la fin de l'audit sur site pour corriger les éventuelles nonconformités et faire auditer les corrections par l'organisme certificateur. Passé ce délai et sans action de l'hébergeur, l'audit sur site devra être recommencé.

Le certificat est délivré pour une durée de trois ans, par l'organisme certificateur, lorsqu'aucune non-conformité n'est constatée. Un audit de surveillance annuel est effectué par l'organisme certificateur.


Dépôt du dossier auprès d'un organisme accrédité
(par le COFRAC ou équivalent)
Audits réalisés par l'organisme accrédité :
- audit documentaire
- audit sur site
Certificat de conformité
délivré par l'organisme
3 ans
Audit de surveillance annuel


Certification HDS : vos étapes
bsi.
A l'issue de la certification, l'hébergeur de données de santé reçoit un certificat ISO27001 et un certificat HDS.
Etude du projet de certification HDS avec validation du périmètre
DEFINITION
1
Participation à des formations dédiées à la certification HDS
FORMATION
2
Mise en place de votre SMSI conforme au référentiel HDS
IMPLEMENTATION
3
A réaliser deux mois avant votre audit de certification
AUDIT A BLANC
4
Réalisation de l'audit documentaire et de l'audit de conformité
AUDIT
5
Revue indépendante de la conformité de l'audit et du dossier de candidature
REVUE TECHNIQUE
6
Délivrance de vos certificats HDS et ISO27001
CERTIFICATION
7

RECHERCHE, ÉTUDE, ÉVALUATION DANS LE DOMAINE DE LA SANTÉ (ART. 54 IV LIL)

PARIS alumni

Déclaration de conformité

Ou

Autorisation

MR-001 recherches biomédicales

Méthodologies de référence

(déclaration de conformité)

MR-003 Recherches non interventionnelles

MR-002 études non interventionnelles de performances DM in vitro

Procédure simplifiée d'examen des catégories les plus usuelles de traitements de recherche dans la santé, non directement identifiantes: engagement de conformité à la méthodologie de référence, valable pour toutes les études présentes et à venir conduites dans les conditions prévues par la méthodologie et nécessitant donc pas de mise à jour annuelle.

Projet de loi Informatique & Liberté

Art. 62: « Au titre des référentiels mentionnés au II de l'article 54 de la présente loi, des méthodologies de référence sont homologuées et publiées par la Cnil. Elles sont établies en concertation avec l'INDS […] et des organismes publics et privés représentatifs des acteurs concernées.
Lorsque le traitement est conforme à une méthodologie de référence, il peut être mis en œuvre sans autorisation […], à la condition que son responsable adresse préalablement à la Cnil une **déclaration attestant de cette conformité** »
= Absence de modification

Recherches Impliquant la Personne Humaine (RIPH)

Recherches Interventionnelles

RIPH de Catégorie 1

Recherches interventionnelles qui comportent une **intervention sur la personne non justifiée par sa prise en charge habituelle**

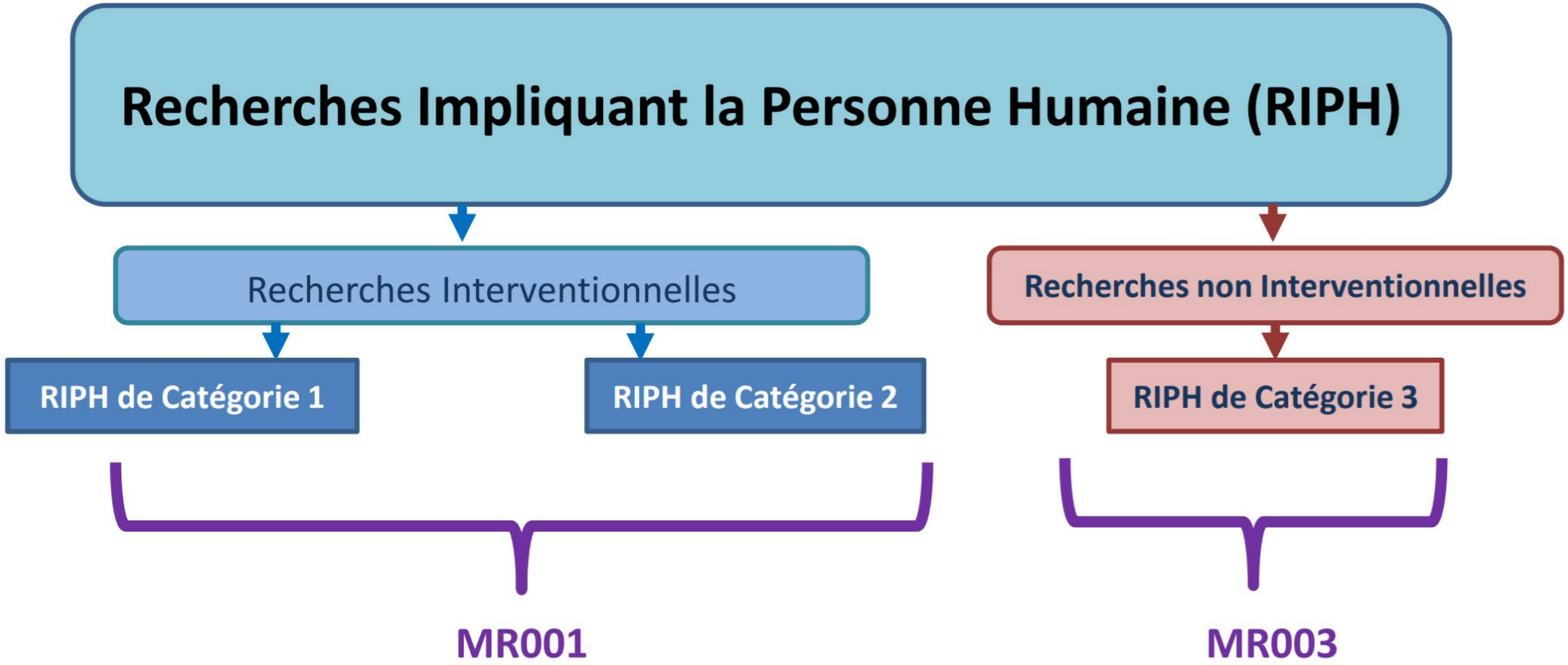
RIPH de Catégorie 2

Les recherches interventionnelles qui ne comportent que des **risques et des contraintes minimes, dont la liste est fixée par arrêté**

Recherches non Interventionnelles

RIPH de Catégorie 3

Les recherches non interventionnelles dans lesquelles tous **les actes sont pratiqués et les produits utilisés de manière habituelle**, sans procédure supplémentaire ou inhabituelle de diagnostic, de traitement ou de surveillance


Recherches Impliquant la Personne Humaine (RIPH)
Recherches Interventionnelles
Recherches non Interventionnelles
RIPH de Catégorie 1
RIPH de Catégorie 2
RIPH de Catégorie 3
MR001
MR003

Modèle de menace

Modèle de menace

- le **modèle de menace** est un processus par lequel des menaces potentielles, telles que les vulnérabilités structurelles peuvent être :
  - Identifiées
  - Énumérées
  - classées
- Par ordre de priorité
- Du point de vue de l'hypothétique agresseur

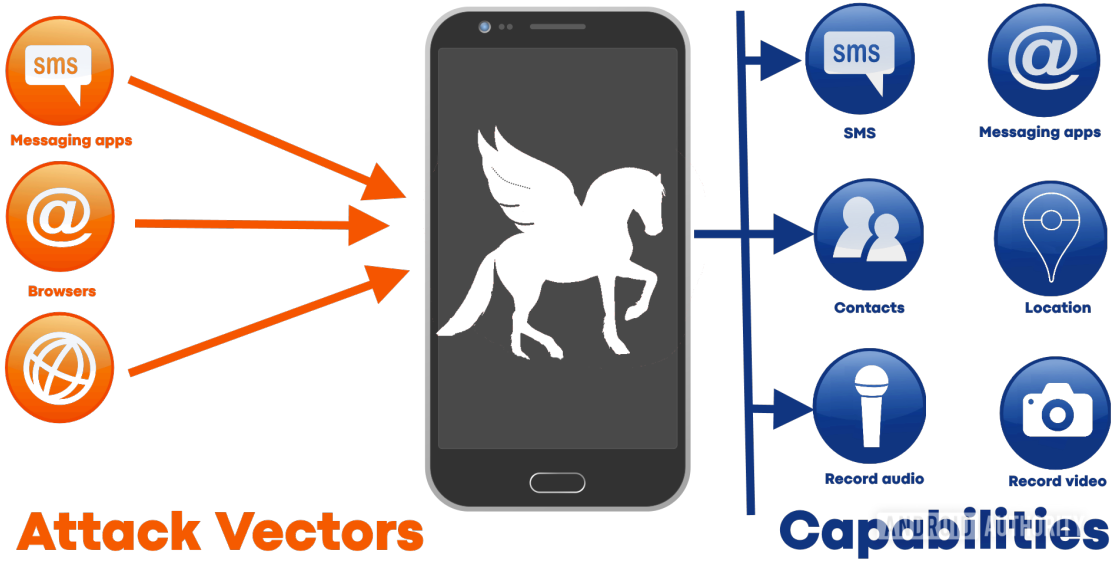
Source : nyder, Window., *Threat modeling*, Microsoft Press, 2004 (ISBN 0735619913, OCLC 54974565)

Pegasus

Spyware

société israélienne de cyberarmement NSO Group

Cible les téléphones portables



Il est impossible de se protéger contre tous les types d'attaques

En revanche vous êtes tenus pour responsables si le minimum n'est pas mis en place pour protéger les données.

C.A.I.D.

La sécurité des systèmes d'information vise les objectifs suivants (C.A.I.D.) :

1. Confidentialité : seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées (notions de droits ou permissions). Tout accès indésirable doit être empêché.
2. Authenticité : les utilisateurs doivent prouver leur identité par l'usage de code d'accès. *Il ne faut pas mélanger identification et authentification : dans le premier cas, l'utilisateur n'est reconnu que par son identifiant public, tandis que dans le deuxième cas, il doit fournir un mot de passe ou un élément que lui-seul connaît (secret)*. Mettre en correspondance un identifiant public avec un secret est le mécanisme permettant de garantir l'authenticité de l'identifiant. Cela permet de gérer les droits d'accès aux ressources concernées et maintenir la confiance dans les relations d'échange.
3. Intégrité : les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets. Cet objectif utilise généralement des méthodes de calcul de checksum ou de hachage.
4. Disponibilité : l'accès aux ressources du système d'information doit être permanent et sans faille durant les plages d'utilisation prévues. Les services et ressources sont accessibles rapidement et régulièrement.

C.A.I.D. (2)

1. La traçabilité (ou « preuve ») : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.
2. La non-répudiation et l'imputation : aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

Garantir ces propriétés

- Permission
- Chiffrement
- Protocole sécurisé
- Mot de passe fort
- Back-up

Souvent invisible pour vous

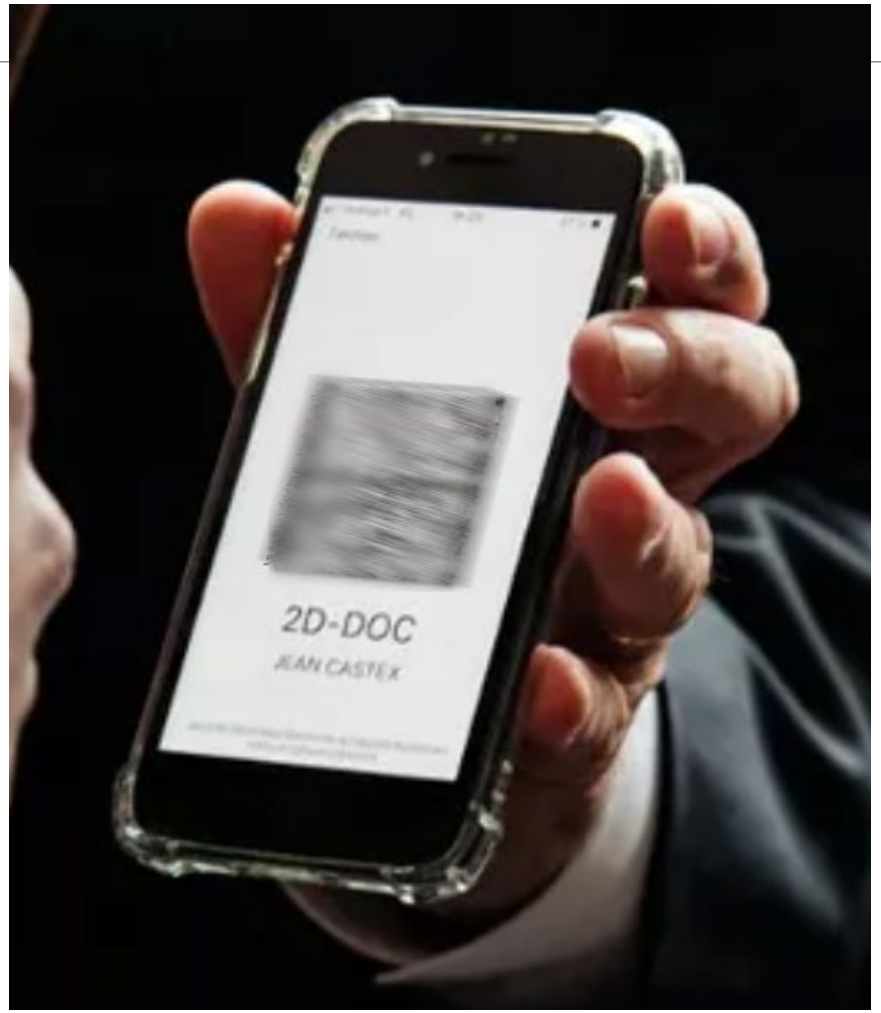
La sécurité informatique un problème humain

La sécurité informatique un problème humain

Problématique en dehors de l'informatique :

- Perte vols
- Facteur humains
- Négligence

Faire cela fasse à une caméra vous semble t’il une bonne idées ?



Passe sanitaire / Numéro de sécurité social

Numéro de sécurité social

- Sexe
- Année/mois de naissance
- Département et commune de naissance
- Clé (n’est en aucun cas une sécurité) très facilement re calculable et : 97 – ((Valeur numérique du NIR) modulo 97)

QR code Passe sanitaire

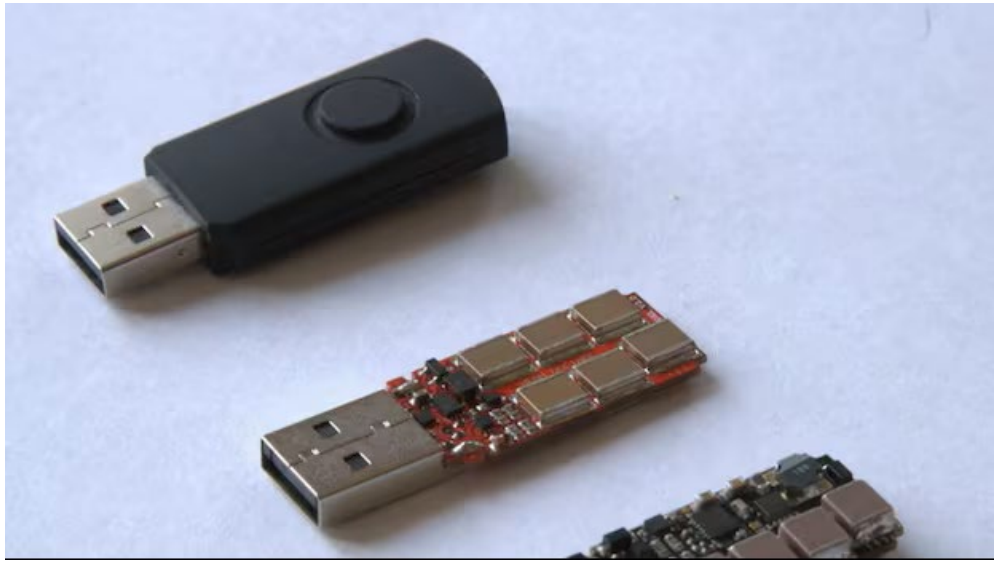
- nom / prénom
- date de naissance
- Test ou vaccin
- nombre de doses / vaccin employé
- date de la piqûre / test

Usurpation d’identité question de vie ou de mort

Exploitation de la négligence exemple

Kill USB Key

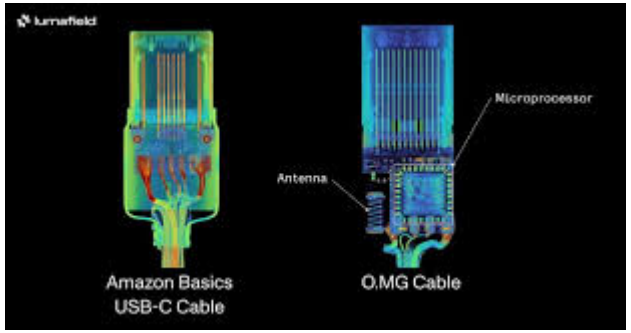
- **Dispositif destructeur** : Une clé USB conçue pour envoyer une décharge électrique et griller les composants d'un ordinateur.
- **Principe** : Stocke l'énergie puis la libère dans le port USB, endommageant la carte mère.
- **Objectif** : Sabotage matériel, souvent utilisé pour détruire des systèmes.
- **Risques** : Perte totale de données et panne irréversible.
- **Prévention** : Ne jamais brancher de périphériques inconnus ; utiliser des bloqueurs USB physiques.



Exploitation de la négligence exemple

Câble de charge malveillant

- **Apparence trompeuse** : Ressemble à un câble USB classique.
- **Fonction cachée** : Intègre un microcontrôleur pour exécuter des commandes malveillantes.
- **Attaque typique** : Injection de scripts pour voler des données ou installer des malwares.
- **Utilisation courante** : Attaques ciblées dans des lieux publics (ex. bornes de recharge).
- **Prévention** : Utiliser ses propres câbles et adaptateurs ; éviter les stations de recharge inconnues. (utilisation de « préservatif »



Exploitation de la négligence exemple

Keylogger

- **Définition** : Logiciel ou matériel qui enregistre les frappes clavier.
- **Objectif** : Vol d'identifiants, mots de passe et données sensibles.
- **Types** : Logiciel (installé sur l'OS) ou matériel (branché entre clavier et PC).
- **Risques** : Compromission totale des comptes et systèmes.
- **Prévention** : Antivirus, surveillance des périphériques, authentification multi-facteurs.

Chiffrement

Importance du chiffrement

Le chiffrement : une protection des données

- Le chiffrement transforme des données lisibles (texte clair) en données illisibles (texte chiffré).
- Il permet de protéger la confidentialité des informations, même si elles sont interceptées.
- Il est essentiel dans les domaines de la santé pour sécuriser les données médicales.

Importance du chiffrement

- **Chiffrement symétrique**
  - Une seule clé est utilisée pour chiffrer et déchiffrer les données.
  - Rapide et efficace pour de grandes quantités de données.
  - Exemple : AES (Advanced Encryption Standard).
  - Problème principal : il faut partager la clé de manière sécurisée.
- **Chiffrement asymétrique**
  - Utilise **deux clés différentes** :
    - Une **clé publique** pour chiffrer.
    - Une **clé privée** pour déchiffrer.
  - Permet d'échanger des données de manière sécurisée sans partager de clé secrète.
  - Exemple : **RSA (Rivest–Shamir–Adleman)**.
  - Plus lent que le chiffrement symétrique, mais très utile pour les échanges sécurisés.

cryptographie asymétrique base d’internet

- HTTPS : Sécurisation des sites web.
- Emails chiffrés : Protocoles comme PGP.
- Signatures numériques : Vérification d’intégrité et d’identité.
- Cryptomonnaies : Portefeuilles et transactions.

Sécurité par l'obscurité limite

Failles de sécurité exemples CV

- Jusqu'en 2006 les informations personnel contenue dans les cartes vitales était stocké dans une zone non chiffré
- Possibilité de créer des clones fonctionnels ou de fausse cartes
- Risque évoqué depuis 2002
- Démontré en pharmacie en 2006 par un ingénieures informatiques

Source : https://www.zdnet.fr/actualites/la-securite-de-la-carte-vitale-prise-en-defaut-39264579.htm ; https://www.apmnews.com/freestory/10/151294/le-gie-sesam-vitale-s-engage-a-corriger-la-faille-de-securite-de-la-carte-vitale-au-premier-semestre-2006

Ergonomie

- Accès aux données personnelles de 700 000 personnes testées pour le Covid-19
- les noms, prénoms, dates de naissance, adresses, numéros de téléphone, numéros de sécurité sociale et adresses électroniques
- un mot de passe qui peut être trouvé, en clair

- Francetest n'a pas été approuvé par la DGS.
- Mais cette plateforme était plus ergonomique que les plateformes approuvées.

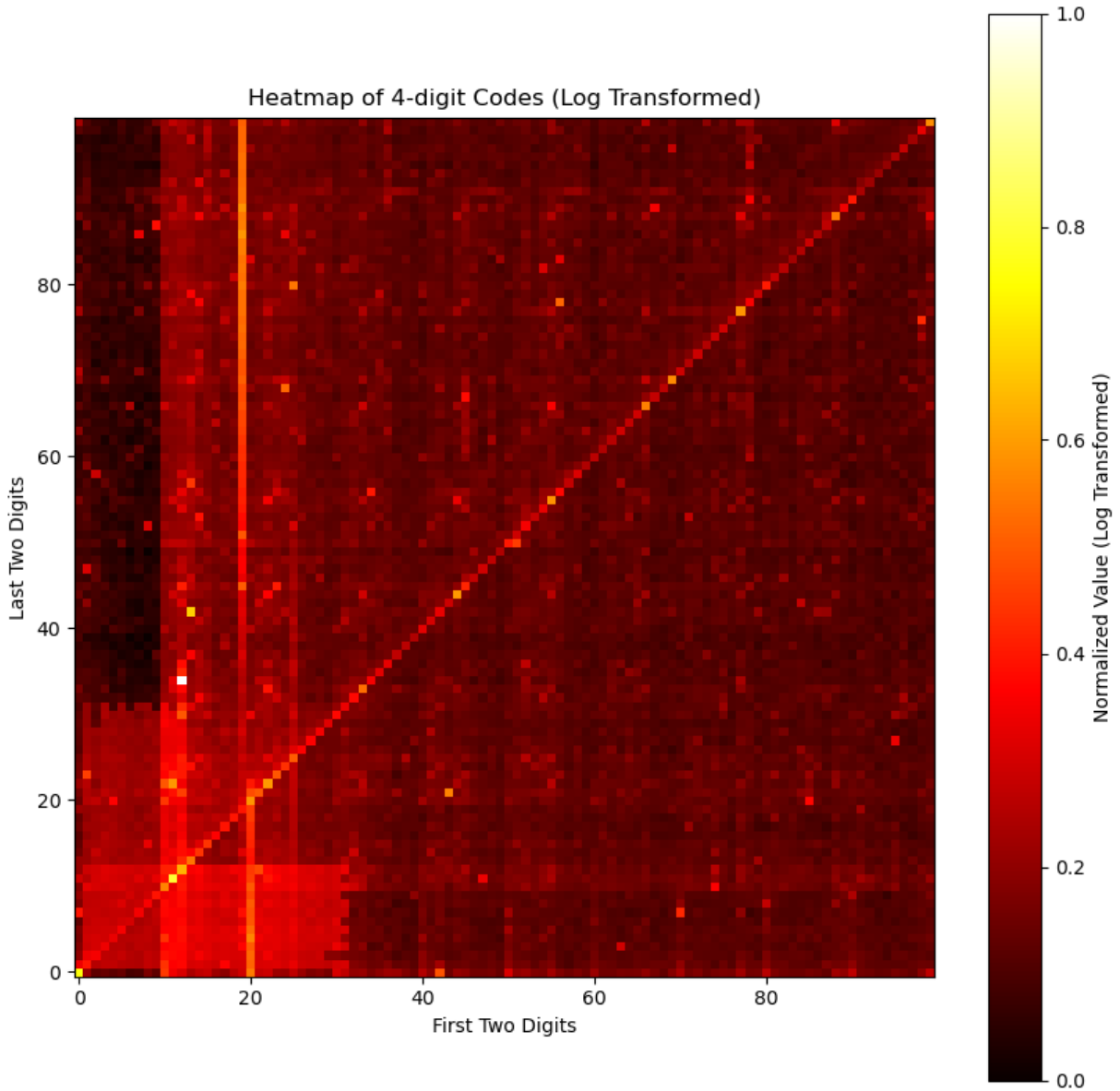
- **Si les mesures de sécurité sont trop restrictives pour les utilisateurs, ils essaieront de les contourner.**
- **Intérêt de sensibiliser les utilisateurs à l'importance de la sécurité informatique comme avec ce cours**

Ergonomie (2)

Toutes les mesures de sécurité représente une contrainte pour les utilisateurs

Mots de passes

- Mode d'attaques courant
  - Brute force
    - Mot de passe complexes
  - Dictionnaires
    - Pas d'utilisations des mots courants seul
    - Eviter les mots de passes très utilisez :
      - « AZERTY »
      - « QWERTY »
- Une solution possible
  - phrases de passes
  - Gestionnaire de mdp


Heatmap of 4-digit Codes (Log Transformed)
Last Two Digits
First Two Digits
0
20
40
60
80
Normalized Value (Log Transformed)
0.0
0.2
0.4
0.6
0.8
1.0

Pourquoi les mots de passe ?

Authentification et traçabilité

Importance de l'authentification

- Contrôles de qui accède à quoi (Habilitation)
  - « brise glace »
  - Protections pour l'utilisateurs
  - Limiter les accès a ce qui est nécessaire pour l'exercice professionnels
    - Exemple SUDO
- Responsabilité

Traçabilité

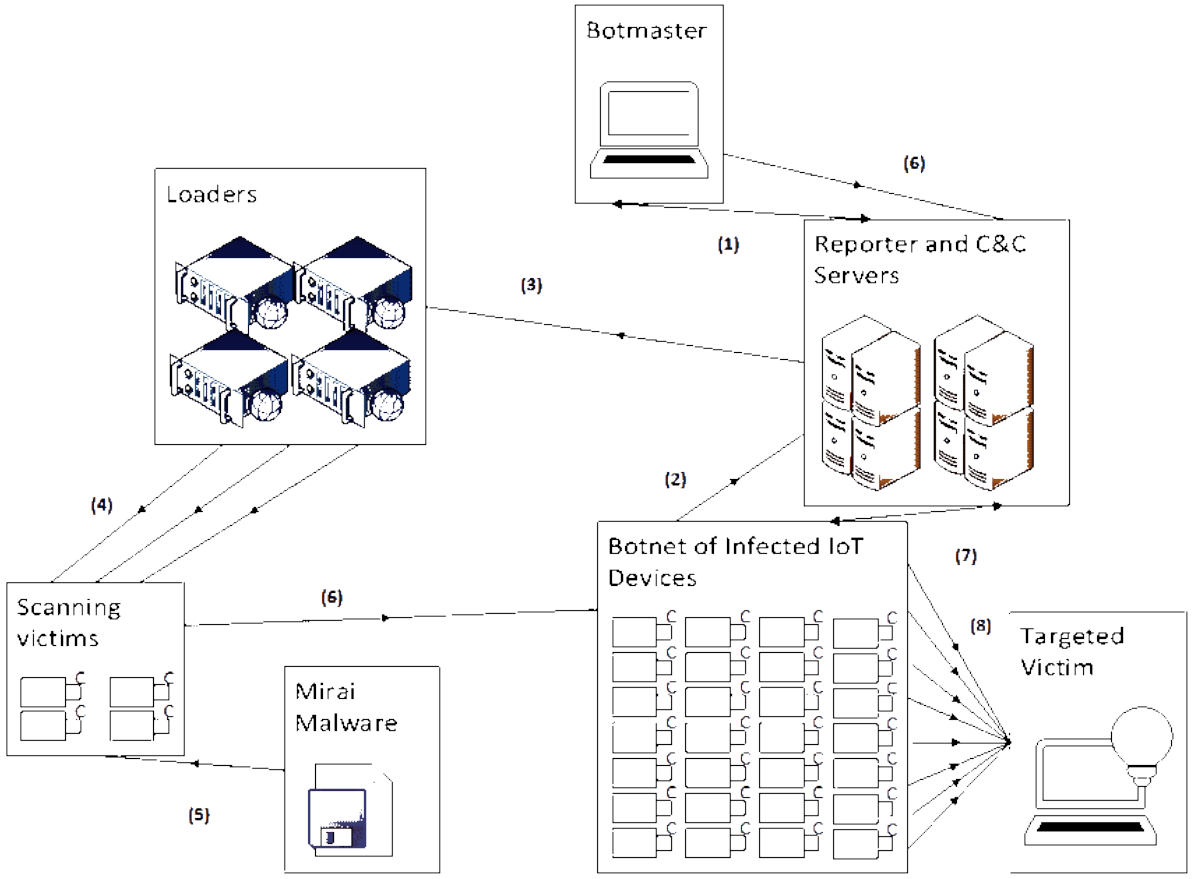
- Obligation légale
- Conserve les consultations modifications suppression et maintenance

CHU de Grenoble : Schumacher

Mirai

- Logiciel malveillant qui transforme les appareils en réseau (caméras IP et routeurs domestiques) fonctionnant sous Linux en robots contrôlés à distance et pouvant être utilisés dans le cadre d'un réseau de robots.
- Infecte les appareils en utilisant des combinaisons de connexion par mot de passe par défaut et, une fois l'appareil infecté, le sécurise.
- DDOS : Denial-of-service attack

Changez toujours les noms d'utilisateur et les mots de passe par défaut



hash cryptographique

- **Fonction mathématique** : Transforme une donnée (ex. un mot de passe) en une empreinte unique appelée *hash*.
- **Taille fixe** : Peu importe la longueur du texte d'origine, le hash a toujours la même taille (ex. 256 bits).
- **Non réversible** : Impossible (en pratique) de retrouver le texte original à partir du hash.
- **Déterministe** : Le même mot de passe donnera toujours le même hash.
- **Résistant aux collisions** : Deux entrées différentes ne doivent pas produire le même hash.

Stockage des mots de passe

- **Stockage sécurisé** : Les sites ne gardent pas le mot de passe en clair, mais son hash.
- **Vérification** : Lors de la connexion, le mot de passe saisi est hashé et comparé au hash stocké.
- **Protection contre vol de base de données** : Même si les hashes sont volés, il est très difficile de retrouver les mots de passe.

Transmission de l’information

Transmission information

Fax

- Devrait être proscrit
- Faille de sécurité potentielle (point d'entrée d'attaques)
- Potentiellement transmission non chiffré (dépends du protocoles)
- Risques d'erreurs de saisie

Aujourd'hui Fax = 2 boites mail connecté a des imprimantes

Utilisez une messagerie sécurisé pour vos communications professionnels

Transmission information

- Mail
- Signatures ?
  - Attention a l'expéditeur
- Chiffrement
- Problématique champ visible pour l'utilisateur ≠ de celui utiliser (SMTP)

Utilisez une messagerie sécurisé pour vos communications professionnels

Les propriétés CAID qui vous semblent indispensable a une messagerie sécurisé ?

Messagerie

- Chiffrement de bout en bout
- Meta data associé aux message
  - Whatsapp
- Ce qui est stocké

Confidentialité Mailiz MSS santé

https://pharmagest.com/tout-savoir-sur-la-mssante-loutil-indispensable-de-coordination-de-soins/

https://www.mssante.fr/ps/medecing/bouchand

lettres de Jérusalem

Lettres de Jérusalem

- 16eme siècles « prisonnière espagnole »
- François Vidocq 19 siècles : « Ouvrage qui dévoile les ruses de tous les fripons et destiné à devenir le vade-mecum de tous les honnêtes gens »
- Prison de Bicêtre « rue de Jérusalem » longeait les murs.
- Version moderne : « *arnaque nigériane* »
- Erreur de forme sont « volontaire »

Hameçonnage

- Conséquence directe des fuites de données.
- Technique frauduleuse visant à obtenir des informations sensibles (identifiants, mots de passe, données bancaires) en se faisant passer pour une entité légitime.
- Utilise des émotions forte
  - Suspension de comptes
  - Perte financière
  - …

Solution formation a la sécurité informatique

Importance de comprendre a minima les outils utilisez

Apprendre a lire une URL

- https://www.bette.ga/pharmacie
- https://www.fraude.fr/bette.ga/pharmacie

https://www.google.com.scam.com/

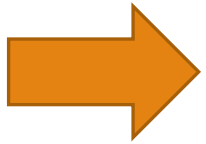
VPN

- Définitions
  - Un VPN est un service qui crée un tunnel sécurisé entre votre appareil et Internet.
  - Il chiffre vos données pour protéger votre confidentialité et votre sécurité en ligne.
- Utilisable comme un proxy
  - Composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges.
- Permet de contrer les problématique de la confidentialité vis-à-vis des FAI
- Attention pas un outils magique

Mise a jour et failles de sécurité

Mise a jour et sécurité

- Prime offerte par les entreprise pour la détections de failles
- Détection en interne



- Patche pour corriger les vulnérabilités

Publications de la faille X mois ou années après selon le contrat avec l'entreprise et la prime.

Importance critique d'avoir mis a jour le système avant que la vulnérabilité soit rendu publique

Mise à jour

Les données de 500 000 patients français ont été diffusées.

volées entre 2015 et 2020

Trentaine de laboratoires d'analyse

utilisé un logiciel obsolète appelé Mega-Bus

Il est de votre responsabilité de ne pas utiliser d'outils présentant des vulnérabilités connues.

Mise à jour (WannaCry)

Systèmes d'exploitation en officines

- 12 % Utilisez un système d'exploitation obsolètes

WannaCry :

- 05/2017
- Ransomware
- Ciblé les ordinateurs pré Windows 10 n'ayant pas effectué les mise à jour de sécurité

Conséquences importantes sur les entreprises avec potentiellement arrêt des activités

Importances de déclarer les failles de sécurité


Wanna Decryptor 1.0
Ooops, your files have been encrypted!
Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28
Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files for free. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
How Do I Pay?

Sécurité different de vie privée

- **sécurité** protège contre les intrusions externes, tandis que la **vie privée** concerne l'usage interne des données.

- Sécurité ≠ Confidentialité
  - Chiffrement des données
  - Sauvegarde
- Données utilisées
  - fins commerciales
  - Usage interne
  - Entrainement de modèle

IQVIA traitement des données de pharmacie d’officine

IQVIA utilise des outils d’analyse statistiques pour apporter des solutions et du conseil au acteurs du systèmes de santé

IQVIA affirme :

- « respecte les droits des patients et se conforme strictement aux règles applicables »
- Données agrégées et anonymisées
- Information personnel : genre et âge

Problématique le droit de rétractions

- La fonctionnalité à été ajouter au logicielle après le reportage de cash investigation

Le pharmacien est responsable

- De contrôler que ses sous-traitant respecte la loi
- Il est responsable de l’informations et du recueille du consentement

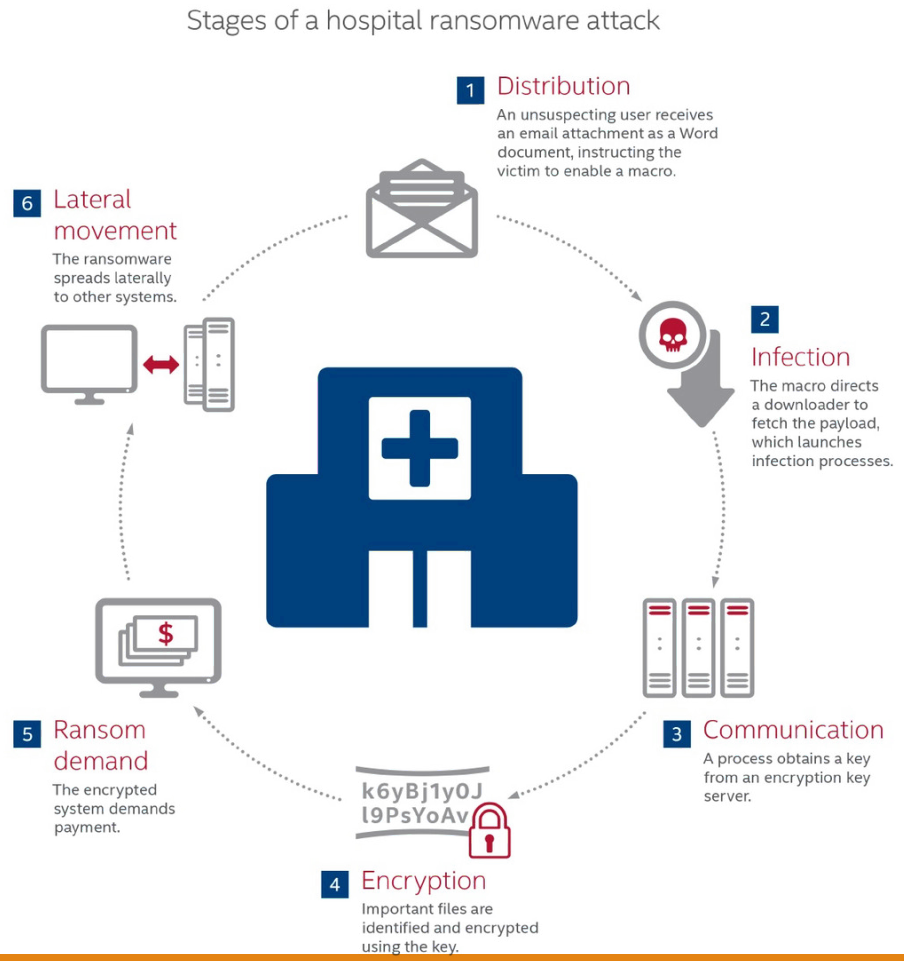
Cyber-attaques contre les hôpitaux

Au moins 9 cyberattaques contre des hôpitaux français entre février 2020 et 2021.

Nécessité de mettre hors service tout ou partie des systèmes informatiques.

Des conséquences sanitaires potentiellement graves pour les patients

Aujourd'hui, les hôpitaux disposent de plans d'urgence



AP-HP Fuite test-covid

Fuite / Vol de données sur l'été 2021 identifié en septembre : 1 400 000 dossiers de résultats de tests en Ile-de-France

Numéro de sécurité sociale

Caractéristiques et résultat du test réalisé

Cible de l'attaque :

- « service sécurisé de partage de fichiers hébergé et utilisé par l'AP-HP, qui lui permet d'assurer le stockage et le partage sécurisé de fichiers, en interne et en externe »

Obligation de déclarations des vols de données

Conséquences des défauts de sécurité

Des sanctions judiciaires lourde

- En pratiques peu de condamnations pour négligence
  - 2 médecins ont été condamnés respectivement à 3.000 et 6.000 euros d'amende
    - Radio et données patients directement accessible sur internet
  - 200 000 euros à la société Optical Center : « *insuffisamment sécurisé les données de ses clients* »

Des condamnations pour faute professionnel

- Vente aux enchères de la radio d'une blessée du 13-Novembre sur une plateforme de vente de NFT

En revanche des conséquences très lourdes sur le fonctionnement des entreprises

Digression LLM

LLM

- **LLM = Large Language Model**: Ce sont des modèles qui prédisent le mot suivant en se basant sur des milliards d'exemples.
- Pas de magie, que des maths : Ils utilisent des réseaux de neurones et des probabilités, pas de pensée consciente.
- Entraînés sur des montagnes de texte : Livres, articles, sites web… pour apprendre les structures du langage.
- Ils ne "savent" rien : Ils ne comprennent pas comme un humain, ils calculent des corrélations.
- Capables de générer du texte fluide : Répondre à des questions, écrire des histoires, résumer des documents.

LLM

- Pas infaillibles : Ils peuvent inventer des infos (hallucinations) ou se tromper.
- Pas connectés à la vérité : Leur “connaissance” dépend des données d’entraînement, pas d’une base factuelle vivante.
- Besoin de puissance énorme : Entraînement = supercalculateurs, consommation énergétique massive.
- Applications variées : Chatbots, traduction, rédaction, analyse de données, aide à la programmation.

LLM -> Package Spoofing

- **Définition** : Création de paquets logiciels malveillants imitant des packages légitimes.
- **Vecteur** : Dépôts publics (ex. PyPI, npm) avec noms proches des originaux.
- **Objectif** : Installer du code malveillant chez les développeurs.
- **Risques** : Exfiltration de secrets, compromission de projets.
- **Prévention** : Vérifier les auteurs, utiliser des gestionnaires de dépendances sécurisés, activer la signature des packages.

LLM

- Limite attention donne la réponse la plus probable
  - Invention de l'aviation
  - Echec
- Outils puissant
  - Ne fait pas le travail a votre place
  - Attention a vérifier
- Enorme problème de confidentialité
- Problème générale liée au Machine learning -> Droit a l'oublis

Pour aller plus loin en vidéo

Defekator : 🔒 **TUTO : Ne PAS se FAIRE PIRATER – DEFAKATOR :** https://www.youtube.com/watch?v=5LYUq4Le3Q8

Micode : https://www.youtube.com/channel/UCYnvxJ-PKiGXo_tYXpWAC-w

BACKSEAT - S04E25 - La dernière ! Spéciale Cybersécurité : https://www.youtube.com/watch?v=vzl_10Q1AAw