Lambda CYBERSÉCURITÉ

L'intelligence derrière les technologies d'affaires

L'Insécurité de l'Internet des objets @ ISACA

14 janvier 2021

Par Rémikya Hellal

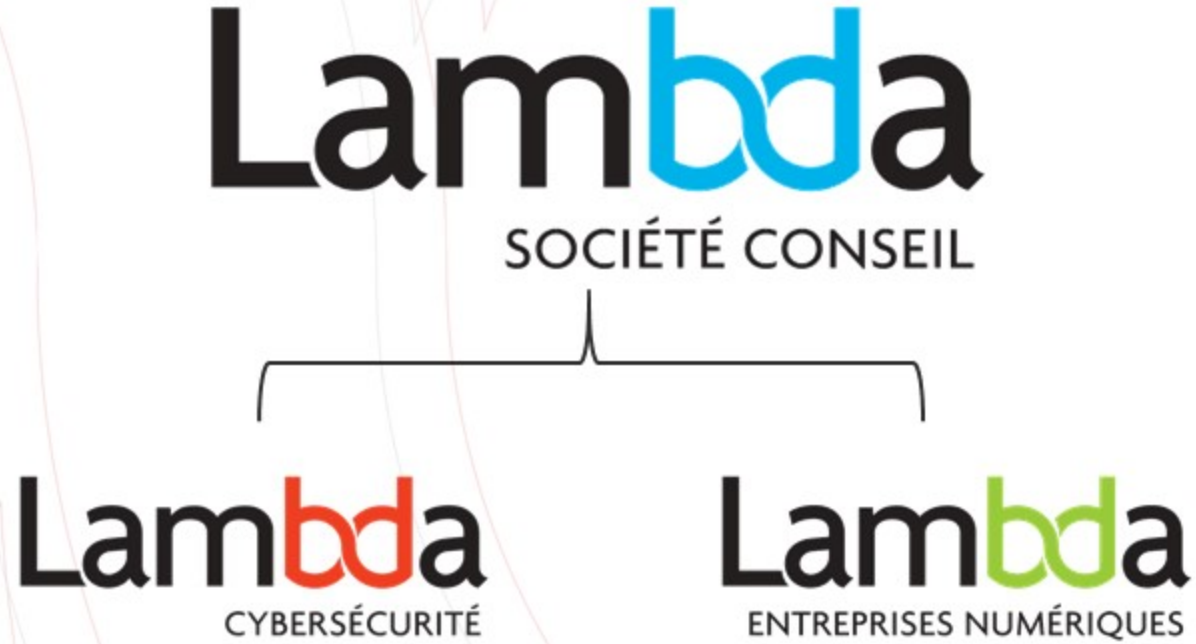
L'Insécurité de l'Internet des objets

Plan

- Remerciements
- Présentations
- Introduction à l'Internet des objets
- Les problématiques de sécurité de l'internet des objets
- Les impacts
- Audit des vulnérabilités et tests d'intrusions
- Démonstration
- Conclusion

Qui sommes-nous?

- **Lambda Société-conseil**
- Spécialisée dans les technologies d'affaires
- Depuis **35 ans**
- Regroupe **4 départements**
- En veille technologique constante

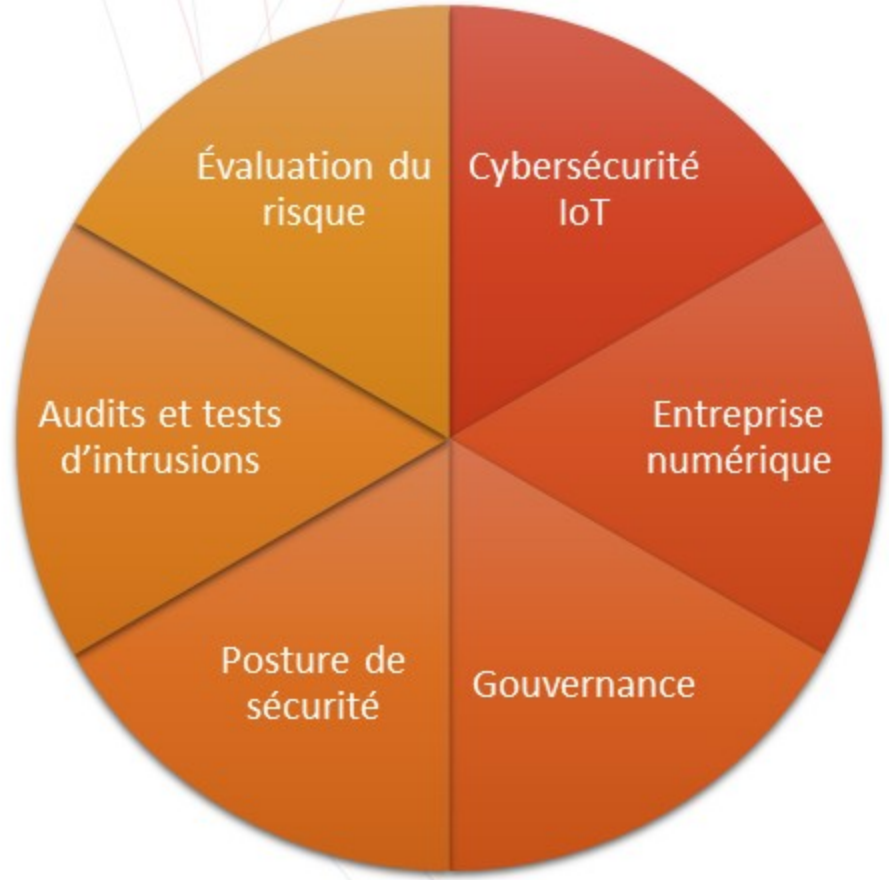


Qui sommes-nous?

Lambda Cybersécurité

Lambda CYBERSÉCURITÉ

L'intelligence derrière les technologies d'affaires



Qui suis-je?

Rémikya Hellal

- Conseillère cybersécurité - Internet des objets (IoT)
- Développement des services cybersécurité des IoT
- Plusieurs conférences
- Polyvalente
- Technophile

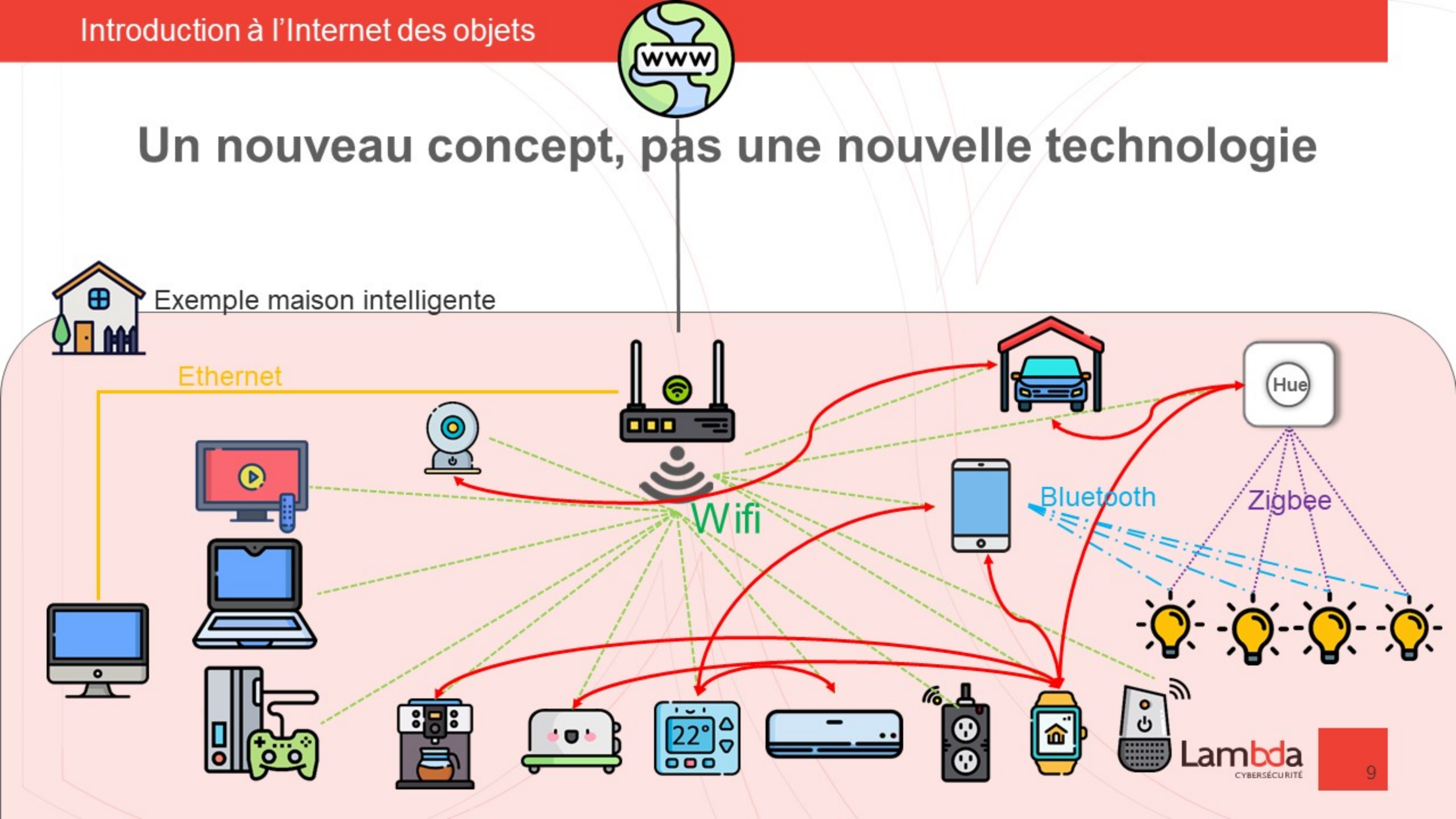
Introduction à l'Internet des objets

Définition

L'Internet des objets est la **connexion** à Internet des objets physiques ou numériques **autonomes** ayant des **actions** dans le monde réel.

Lambda CYBERSÉCURITÉ

Un nouveau concept, pas une nouvelle technologie



Les composants d'un objet connecté

La recette simplifiée.

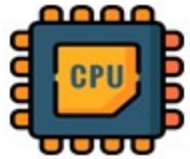
Capteurs

Actionneurs

Communication

Objet connecté

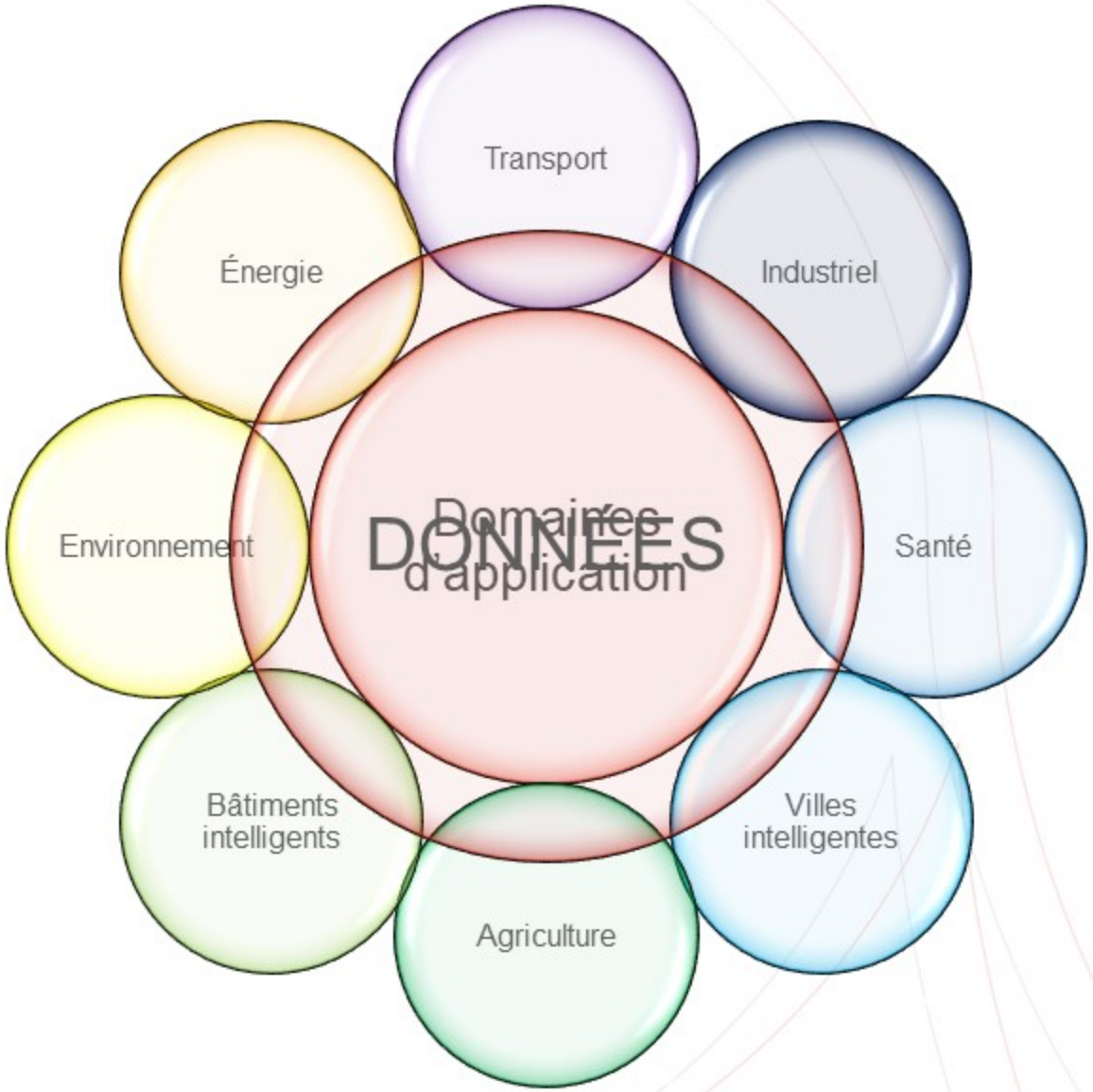
Alimentation



Carte mère

Emballage

Les capteurs dans un téléphone intelligent



Les **données** au cœur de l'Internet des objets

Les problématiques de sécurité de l'Internet des objets

Chaîne d'approvisionnement

Fournisseurs

Matériaux physiques

- Capteurs
- Actionneurs
- Modules de communication
- CPU
- Carte mère
- Alimentation …

Matériaux logiques

- Firmware
- Librairies
- APIs
- Plateforme Cloud
- Applications de tierces-partie
- Bases de données …

Manufacture

- Assemblage
- Configuration
- Adaptation

Distribution

Vente au détail

Consommateur

Objectifs

- **Moindres coûts**
- **« First to Market »**

TODO:

- **Comment obtenir la sécurité dès l'étape de conception?**

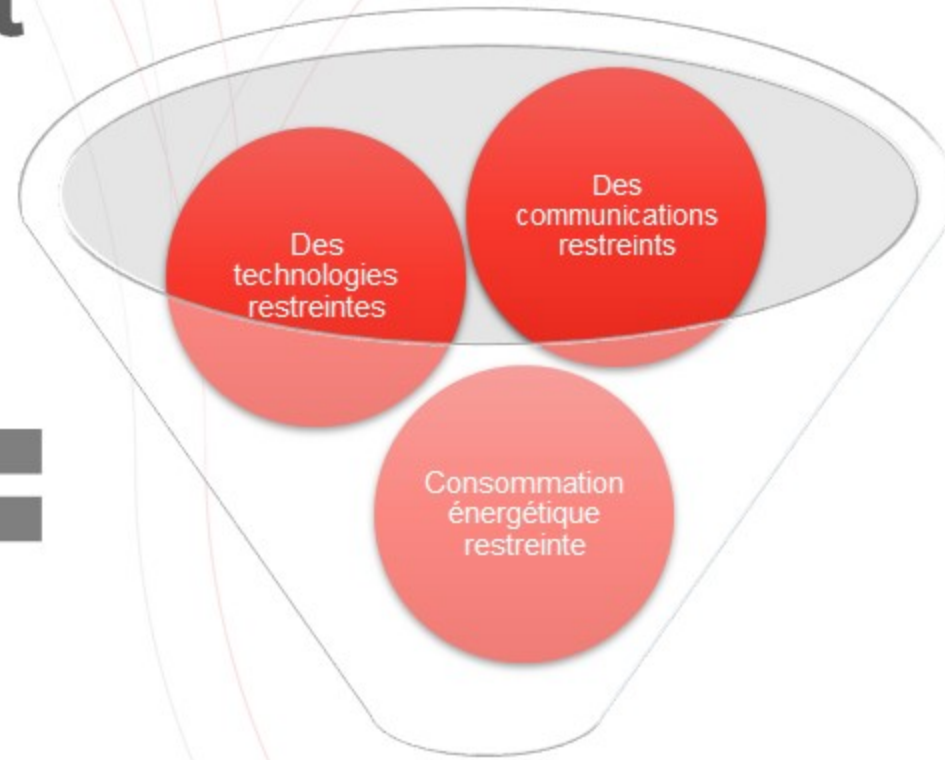
Environnement restreint

Pourquoi?

Batterie d'une durée limitée

Batterie rechargeable

=

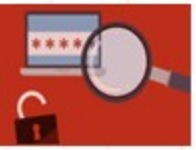


Limitation énergétique !

(low power, constrained)

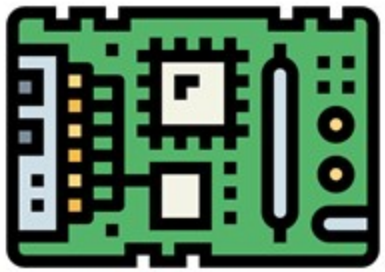
Environnement restreint

OWASP TOP 10 des vulnérabilités IoT

1. Mots de passe faibles, devinables ou codés en dur 
2. Des services réseaux non sécurisés 
3. Des interfaces utilisateurs non sécurisées 
4. Absence de mécanisme de mise à jour sécurisé 
5. Utilisation de technologies insécurisés ou obsolètes 
6. Protection insuffisante de la vie privée 
7. Transfert et stockage de données non sécurisés 
8. Manque de gestion des dispositifs 
9. Paramètres par défaut non sécurisés 
10. Absence de durcissement physique 

https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf

Les vulnérabilités IoT en bref



Hardware
(physique)

Firmware
(micro logiciel)

Communications

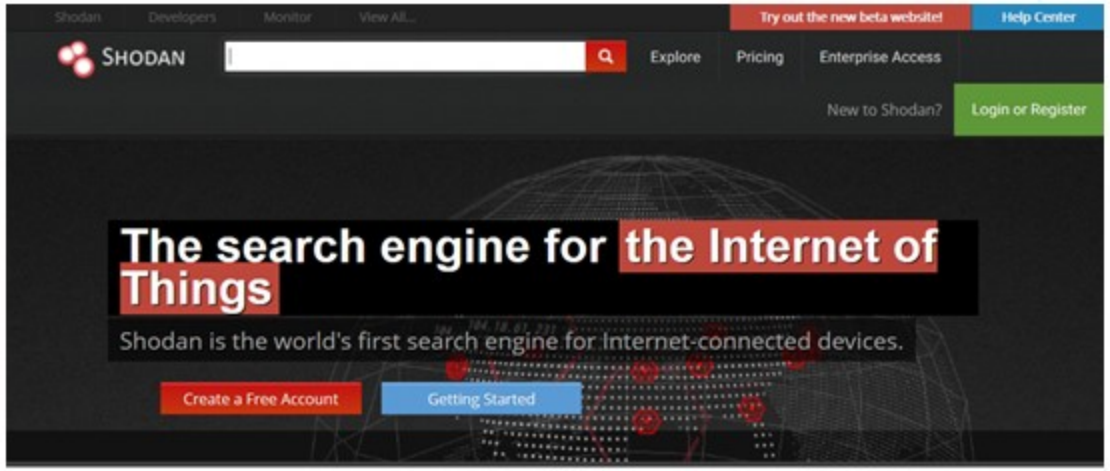
Applications

Exemples 1/2

- De l'Internet des objets au *Botnet* des objets
- Comment?
  - Scan de ports ***Telnet*** ouverts
  - *Bruteforce* avec une liste de **61** noms et mots de passe communs
- Des conséquences sur **OVH** et **Dyn** en 2016

Exemples 2/2

Shodan.io



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

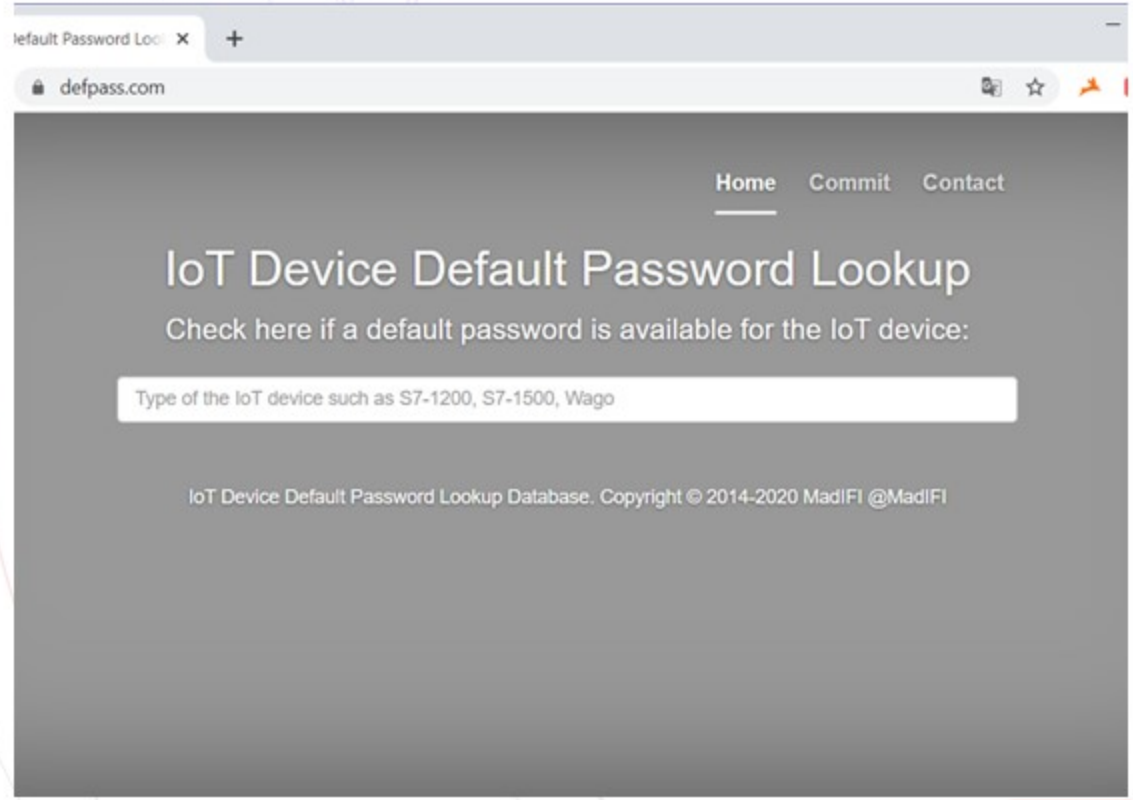
Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

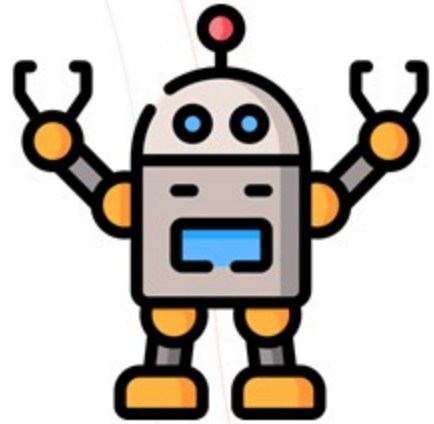
Despass.com



Les impacts

Des impacts sur tous les plans

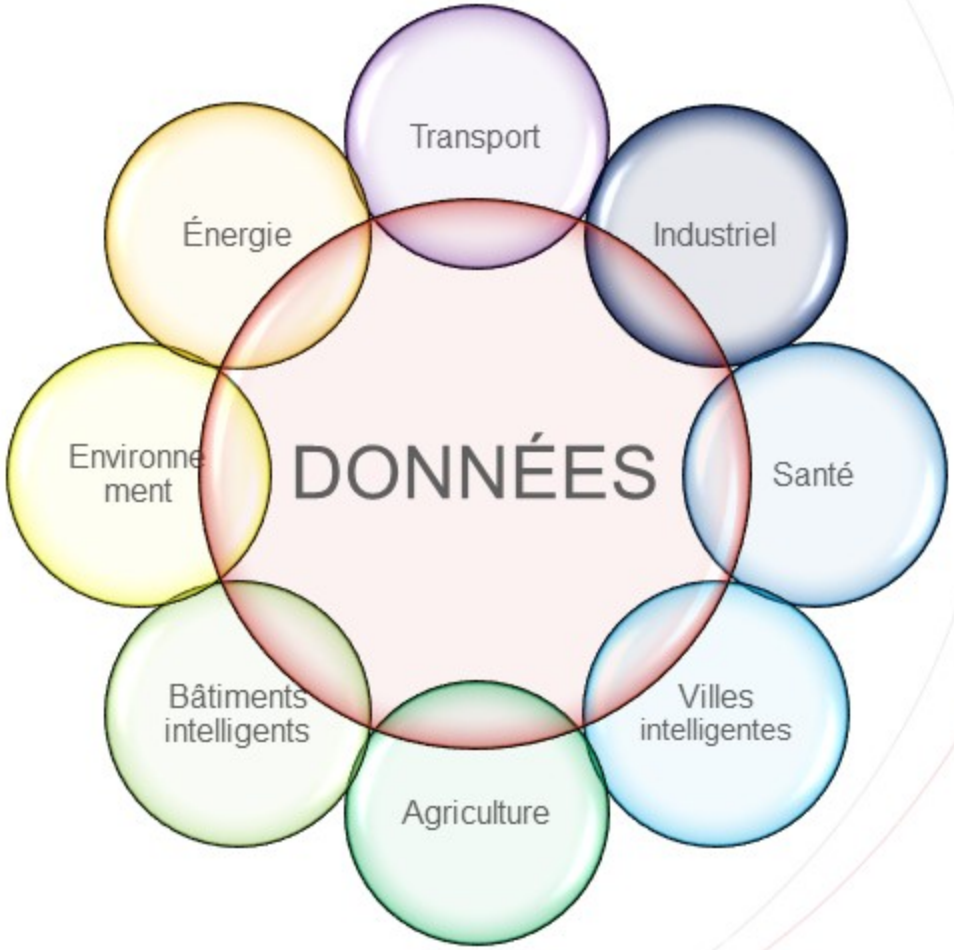
Contexte d'affaires



Contexte technologique

Contexte légal

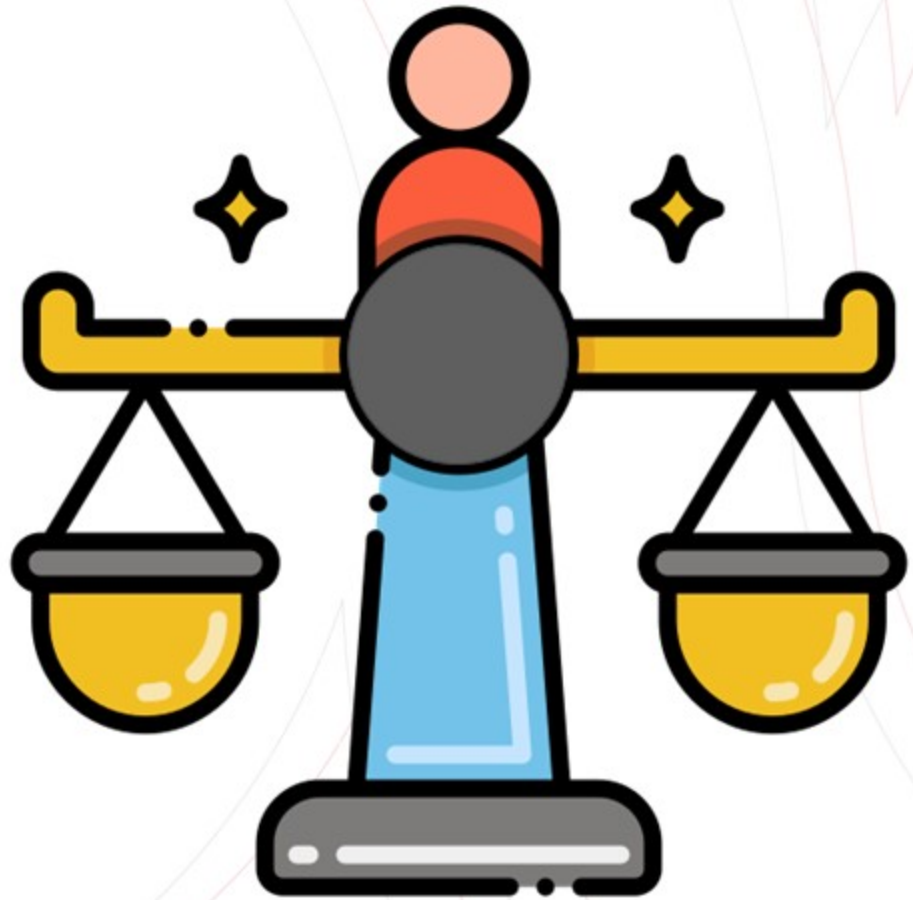
La gouvernance



- Affaires :
  - Choisir le bon IoT
  - Gestion des accès aux IoT
- Technologique:
  - Suivre la sécurité à la conception
  - Prioriser la sécurité
- Légal:
  - Respect les lois sur les données personnelles

Dans un monde « *HighTech* »

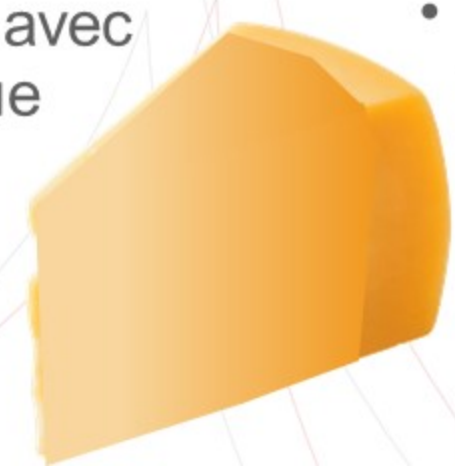
Les technologies



Les fonctions d'affaires

Le projet de loi 64

- Origines : RGPD
  Règlement général sur la protection des données
  - Europe
  - Adopté en 2016
  - Entrée en vigueur 2018
  - Adapter le cadre législatif avec le nouvel ère technologique



- Projet de loi 64
  Concernant la protection des données personnelles
  - Québec
  - Renforcer les droits des personnes
  - Responsabiliser les acteurs traitant des données

Exemples 1/3

Home › Malware

AP German Hospital Hacked, Patient Taken to Another City Dies

By Associated Press on September 17, 2020

German authorities said Thursday that what appears to have been a misdirected hacker attack caused the failure of IT systems at a major hospital in Duesseldorf, and a woman who needed urgent admission died after she had to be taken to another city for treatment.

The Duesseldorf University Clinic's systems have been disrupted since last Thursday. The hospital said investigators have found that the source of the problem was a hacker attack on a weak spot in "widely used commercial add-on software," which it didn't identify.

As a consequence, systems gradually crashed and the hospital wasn't able to access data; emergency patients were taken elsewhere and operations postponed.

https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies

Le premier homicide attribuable à une cyber-attaque de type ransomware

Exemples 2/3

https://www.youtube.com/watch?v=bJrlh94RSil

Une machine à café victime de rançon

Exemples 3/3

Exclusive: Popular Baby Monitor Wide Open to Hacking

Parents rely on internet-capable baby monitors to keep a close watch over their infants. However, an investigation by Bitdefender and PCMag has found that hackers can also exploit some iBaby monitors to spy on those same children.

By Neil J. Rubenking February 26, 2020

https://www.pcmag.com/news/exclusive-popular-baby-monitor-wide-open-to-hacking

SECURITY & PRIVACY

Warning! These smart plugs can be hacked and start fires

BY ANGELICA LEICHT, KOMANDO.COM • OCTOBER 3, 2020 SHARE:

https://www.komando.com/security-privacy/smart-plugs-hacked/757290/

Audit des vulnérabilités et tests d'intrusions

Audit des vulnérabilités

- Recherche d'informations sensibles
  - Liens vers API ou bases de données
  - Mots de passe
  - Clé de chiffrement
  - Librairies
  - Services
- Recherche des vulnérabilités connues (physiques, logiciels, communications, données)

Tests d'intrusions

- Extraction de système de fichiers
- Désassemblage des programmes
- Exploitation des communications
- Réingénierie des applications
- Exploitation des mécanismes d'authentification et d'autorisation
- Exploitation physique des objets connectés

Quelques outils 1/2

Quelques outils 2/2

HackRF One

Apimote

JTAGulator

Ubertooth One

RTL-SDR

Attify Badge

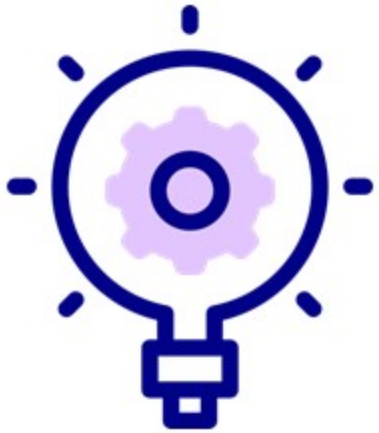
Démonstration

Outils

Govee
Smart LED Bulb

BLE dongle
Adaptateur Bluetooth

Ubertooth One



Procédure

- Vérifier la connexion de l'adaptateur BLE (hciconfig)
- Recherche des dispositifs BLE disponibles (hcitool lescan)
- Récupération de l'adresse physique de l'ampoule
- Connexion avec l'ampoule (Gatttool)
- Analyse des caractéristiques BLE
- Capture de la communication BLE (Ubertooth One)
- Analyse de la capture BLE (Wireshark)
- Réingénierie des données transmises
- Exploitation de l'ampoule avec une requête forgée (Gatttool)
- Automatisation de l'exploitation (Python)

Conclusion

Solutions maison

Acheter Intelligemment

Bien initialiser à la première utilisation

Bien configurer l'objet connecté

Apprendre à détecter les anomalies

Utiliser de façon appropriée de sorte à protéger sa vie privée

Connecter intelligemment

Protéger nos objets et nos réseaux

Maintenir une bonne configuration

Éviter les objets connectés trop vulnérables

Bitdefender Box

Lambda CYBERSÉCURITÉ

MERCI

www.lambda.ca
Infolettre:
cybersecurite@lambda.ca

Lambda CYBERSÉCURITÉ