
IBM

La sécurité des objets connectés (IoT & OT)

Croissance des attaques, criticité de l'adhésion ComEx, mise en place chez IBM

Sébastien Jardin
Directeur du Business Development
IBM Security France
Membre du CLUSIF
https://www.ibm.com/security

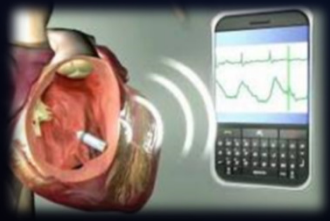
IBM Security

IBM

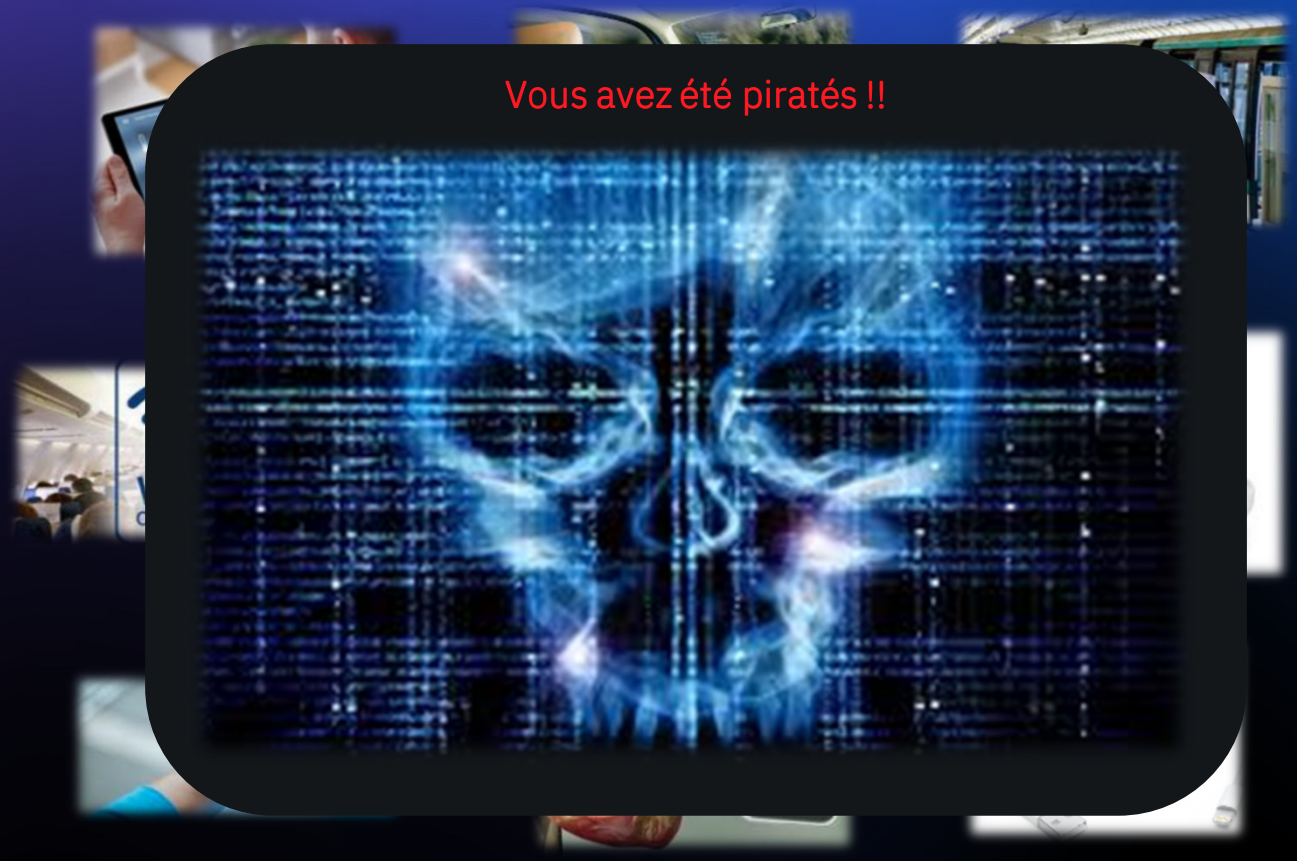
Qui est IBM Security

- Fournisseur mondial de cybersécurité d'entreprise
- 14 segments couverts en cybersécurité
- Chiffre d'affaires 2018 de $2Mds et en croissance
- 8 000+ employés en sécurité
- 10k+ brevets de sécurité

La digitalisation est une vague déferlante très utile...



… mais qui peut se retourner rapidement contre ses créateurs



Les attaques ont majoritairement une motivation financière

X-Force Threat Intelligence Index 2020

Top 10 industries targeted

Top 10 targeted industries ranked by attack volume, 2019 vs. 2018 (Source: IBM X-Force)

Sector	2019 rank	2018 rank	Change
Financial Services	1	1	–
Retail	2	4	2
Transportation	3	2	-1
Media	4	6	2
Professional services	5	3	-2
Government	6	7	1
Education	7	9	2
Manufacturing	8	5	-3
Energy	9	10	1
Healthcare	10	8	-2

Données monétisables

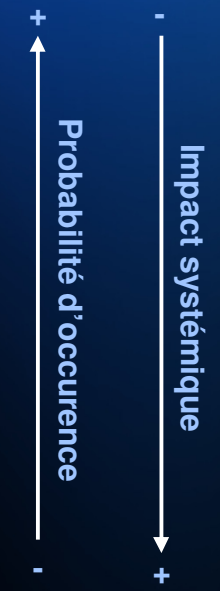
Services Financiers, Commerce de Détail, Transports, Médias, Services Professionnels, Gouvernement, Education, Fabrication, Energie, Santé

Actions monétisables

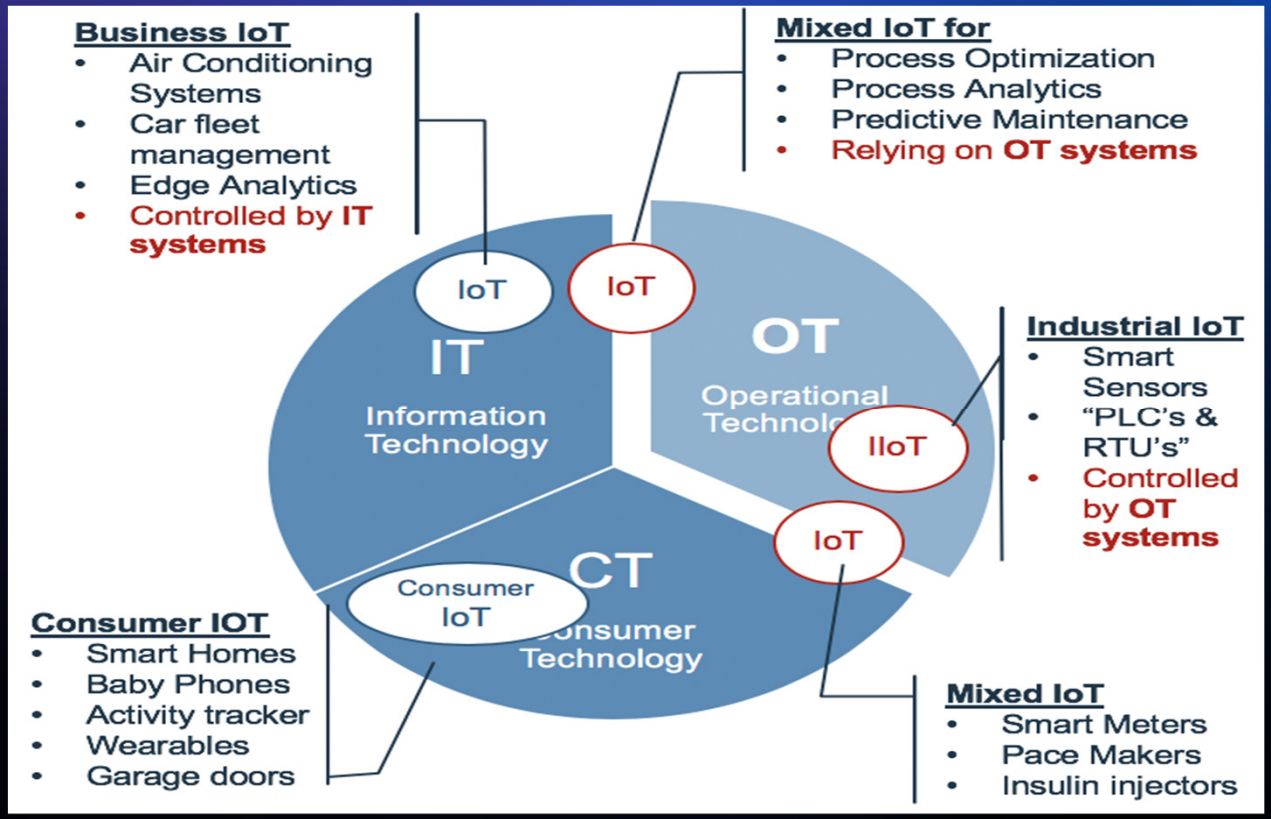
Services Financiers, Commerce de Détail, Transports, Médias, Services Professionnels, Gouvernement, Education, Fabrication, Energie, Santé

Influence & Déstabilisation

Médias, Gouvernement



IoT & OT… de quoi parle-t-on ?

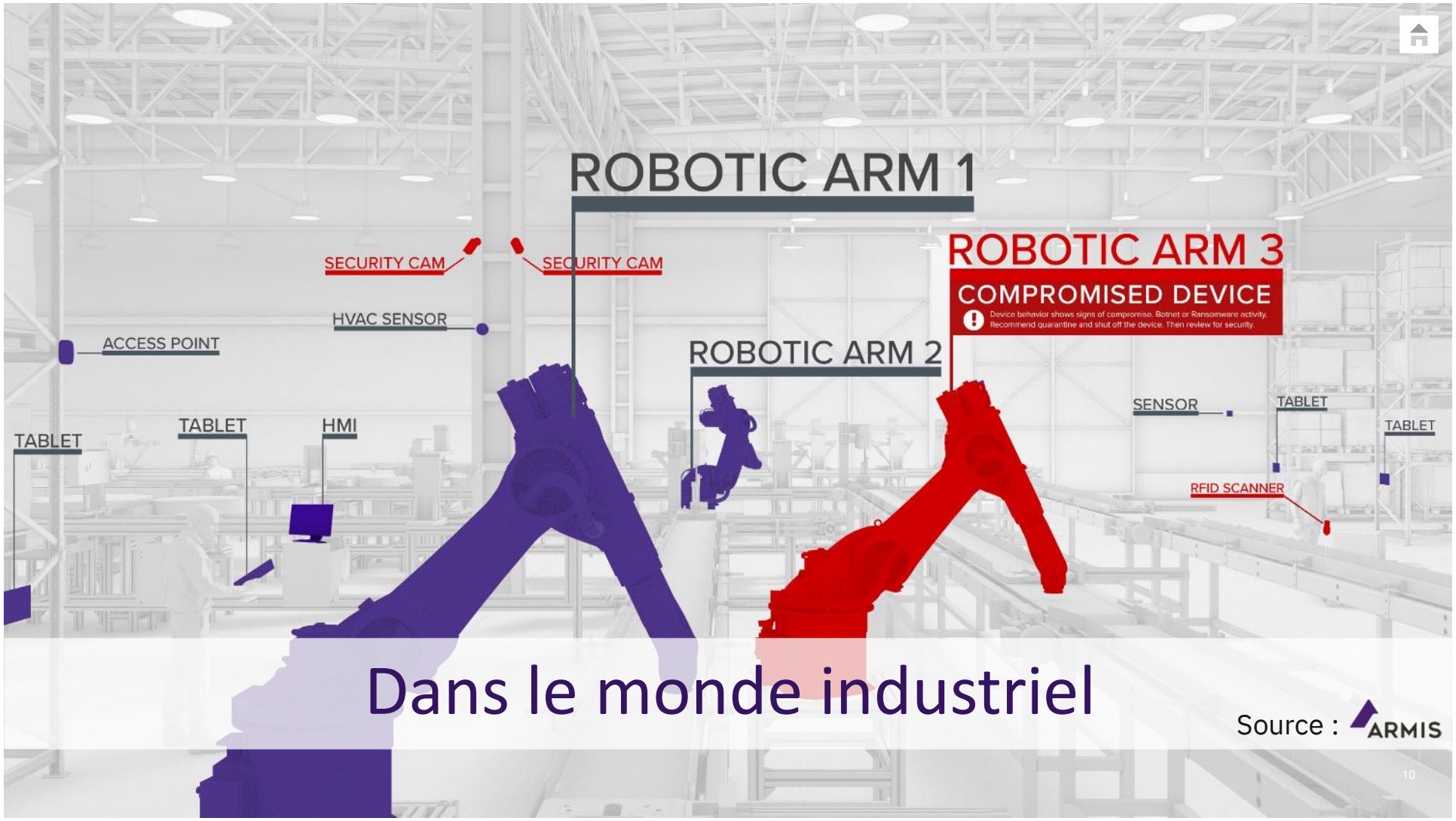


Dans toutes les entreprises

Source : ARMIS

Dans le monde médical

Source : ARMIS



Dans le monde industriel

Source : ARMIS

IoT & OT – Une nouvelle cible plébiscitée par les pirates

2000%

Hausse du nombre d'attaques entre 2018 et 2019 visant l'OT et l'IoT.

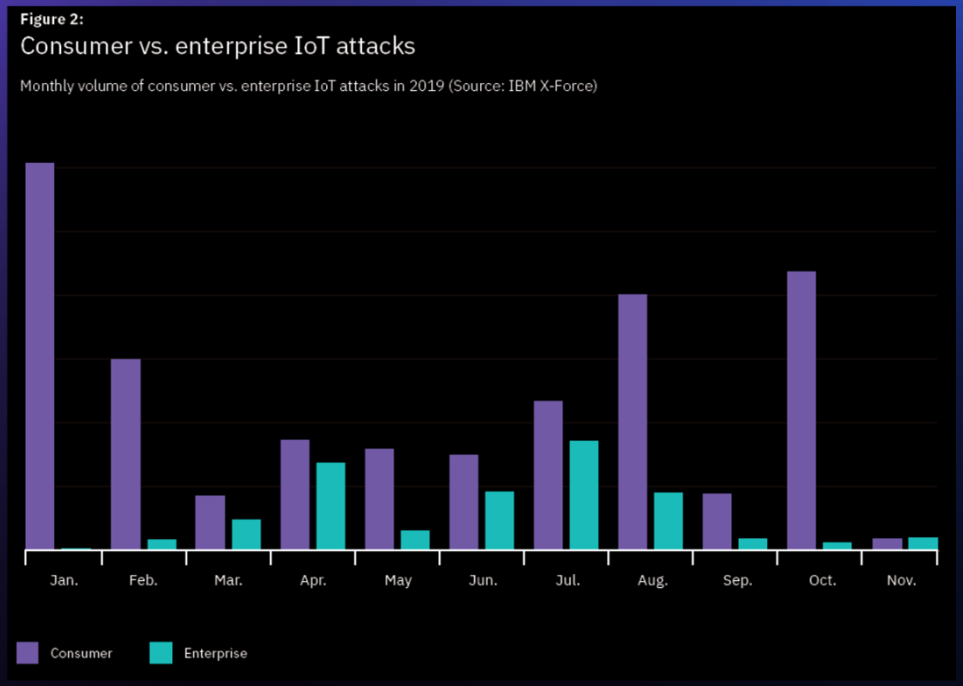
Hardware & Mots de passe

La plupart des attaques observées étaient centrées des vulnérabilités connues dans les matériels en place et utilisaient la technique de « brute force ».

Convergence IT/OT

Les pirates continuent de se tourner vers différents vecteurs d'attaque, avec un ciblage accru des appareils IoT, de la technologie opérationnelle (OT) et des systèmes industriels ou médicaux connectés.

IoT & OT – Les entreprises attaquées via les consommateurs



38 milliards

d'objets connectés en 2020, ce qui explique l'intérêt des pirates pour ce vecteur avec des rebonds de type malwares ou des scripts automatisés.

Point de bascule

2019 a connu une forte accélération des attaques sur les composants électroniques grand public vers les systèmes de l'entreprise (cf. accès réseau, BYOD…).

Identité & Accès

Les IoT & OT ont une activité souvent automatisée et opèrent en « machine to machine » ce qui rend crucial leur incorporation à l'infrastructure IAM de l'entreprise.

La sécurité de l'IoT et de l'OT est un domaine encore jeune

Sécurité IT	Sujet	Sécurité OT / IoT
Conformité Financier	Risques enjeux	Sûreté / Ecologie Vies humaines Conformité
3 à 5 ans	Cycle de vie	5 à 20 ans
Fréquents	Changements	Rares
Accepté	Interruption pour mesure de sécurité	Interdite
Fréquent	Patching	Rare et complexe (accord + tests)
IP / Zoning	Réseau	Début d'IP Spécif / analogiques
Moyennes à fortes. Maturité.	Compétences spécifiques en sécurité IT.	Pas ou peu. Sujet naissant.
Génériques et partageables.	Cas d'usage (attaques…)	Très liés aux métiers.

L’impact sur les entreprises et les humains peut être colossal…

L’USINE DIGITALE

[FIC 2017] Le patron de l’ANSSI craint des morts à cause des objets connectés *(Janvier 2017)*

3 hauts-de-france

Victime d'une cyberattaque d'ampleur mondiale, le groupe Renault a décidé de mettre plusieurs de ses sites à l'arrêt. *(Mai 2017)*

LE FIGARO tech avec le JDN

Un virus informatique paralyse un hôtel de luxe en Autriche (J*anvier 2017)*

silicon.fr

Triton: ce malware a visé un système de contrôle industriel de Schneider Electric *(Janvier 2018)*

… et parfois vous participerez à une attaque sans le savoir

LE MAGAZINE DES OBJETS CONNECTÉS ET INNOVANTS
OBJETCONNECTE.NET

Un hacker pirate un casino via le thermomètre connecté d'un aquarium *(Avril 2018)*

Oct 2016 : DDoS on Dyn impacts Twitter, Spotify and others

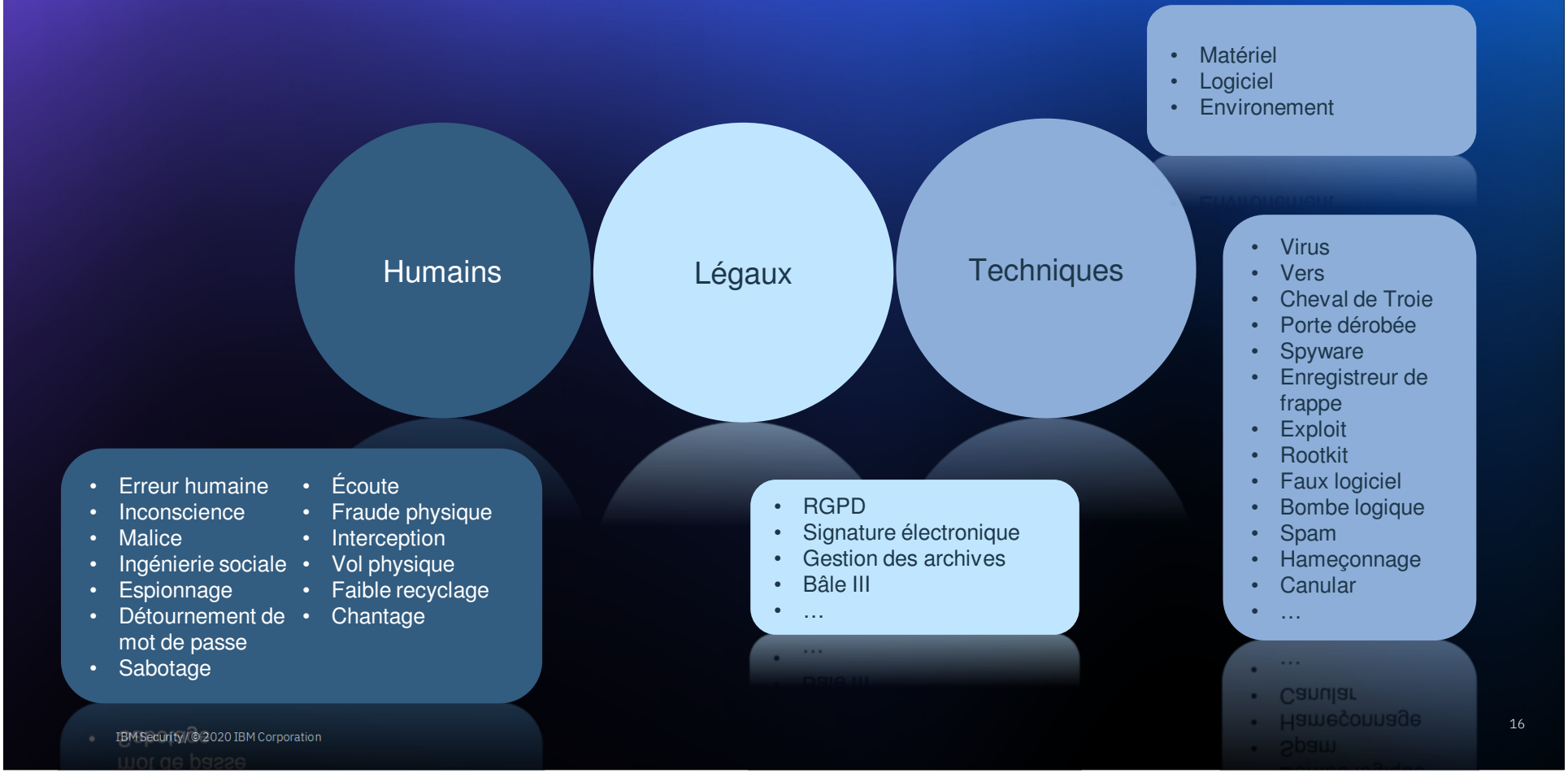
'Smart home devices used as weapons in website attack'

BBC NEWS

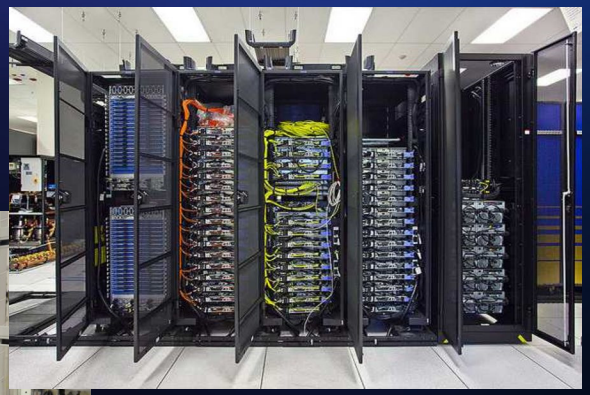
Siecle Digital

Une fois piratée, une montre connectée pour seniors pouvait mener à la surdose médicamenteuse *(Juillet 2020)*

Commencez par les sujets non négociables et leurs risques



Chez IBM, la sécurité IoT & OT est suivie au niveau ComEx



Pentesters IBM

« Cassez tout ce que vous pouvez, volez tout ce que vous pouvez. Il vaut mieux identifier les failles en amont que les découvrir suite à une attaque.

Cette façon de faire est discutée et approuvée par le top management. »

Former IBM Global CISO

Faire de la sécurité un réflexe métier est un travail quotidien

Parler le langage du ComEx

La mission du RSSI est de protéger l'entreprise et ses clients des menaces digitales. Parler le langage des métiers permet de se positionner en partenaire facilitateur et pas en contrainte.

1

Avoir une approche holistique du risque

Votre temps, équipe et budget ne seront jamais suffisants pour adresser tous les sujets, et éviter de créer des silos métiers vous permettra d'optimiser l'usage de vos ressources au global.

2

Répandre la culture sécurité

Vous ne pourrez jamais réaliser la protection digital seuls, vous avez besoin d'être expert en technologies mais aussi capable de faire des métiers la première ligne de cyberdéfense.

3

IBM France, Telecom Valley et Security by Design

- La R&D d'IBM pense & développe en mode « Security by Design », **IBM France Lab implanté depuis des années à Sophia-Antipolis**

- Participation de **Patrick Merlin** au 3e Sophia Security Camp « *Mise en place du Process SPbD dans les différentes équipes de developpement au Lab R&D d'IBM (Paris , Sophia ...) SPbD -Threat Model -Code Scan (SAST, DAST, IAST, Other) -Security Tests -Pen Test (internal vs external) -Vulnerability management SPbY on legacy code VS new software* » (8 Octobre 2019)

- Participation active des collaborateurs IBM dans les **communautés de Telecom Valley**

IBM **Security**

Merci

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- ibm.com/security/community
- www.securitylearningacademy.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions