Objets connectés Vs sécurité des biens et des personnes

fin 2018, où en sommes-nous ?

Pas grand-chose n’a changé …

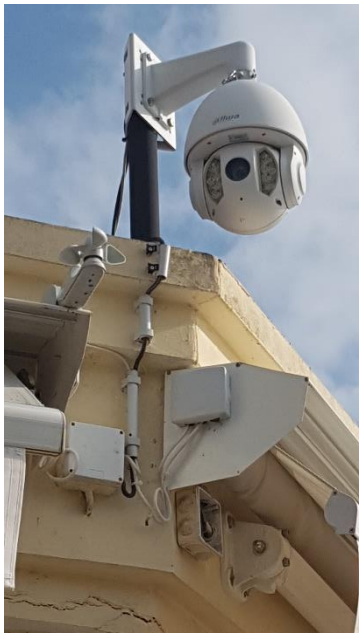
(le mois de la cybersécurité est passé. On est tranquille pour 1 an)

Au niveau des clients finaux et décideurs

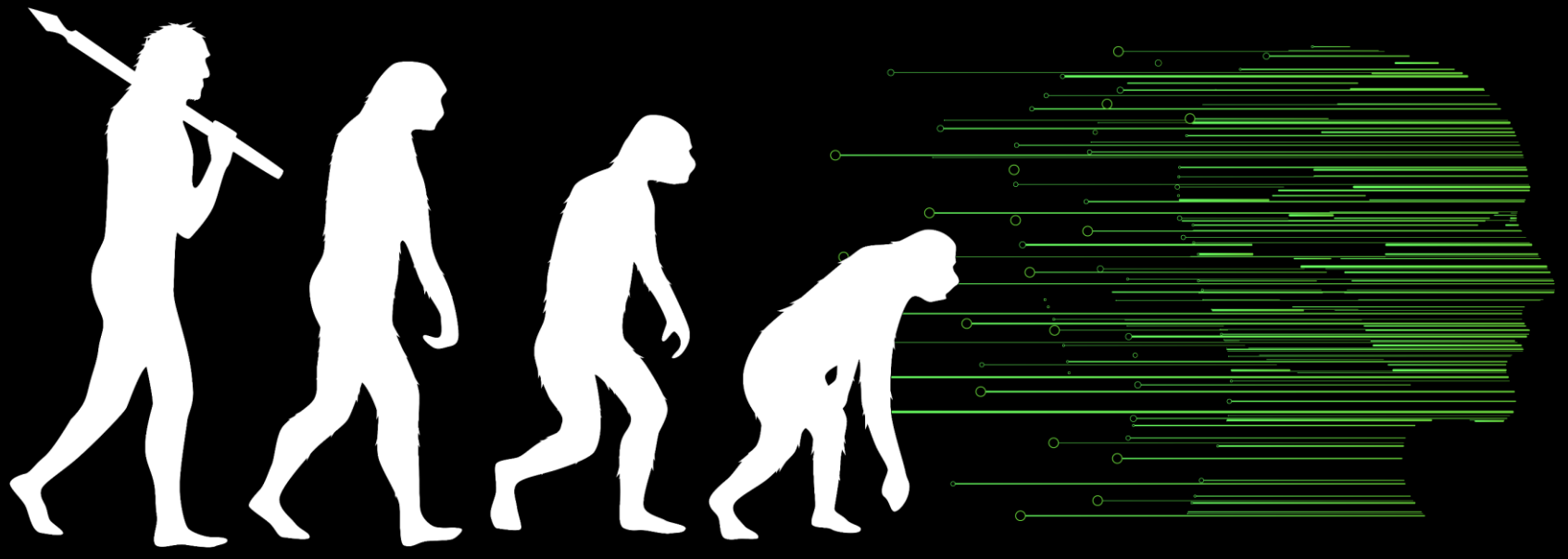
- Toujours beaucoup de bonne volonté
- Toujours de moins en moins de budget pour la sécurité sauf si ….
- Toujours un énorme fossé entre la Théorie et la Pratique.

Au niveau des industriels, éditeurs de logiciel, grossistes & intégrateurs finaux

- Toujours la course à l’armement
- Toujours de beaux effets d’annonce
- Toujours autant de failles de sécurité
- Toujours autant de manque de formation



L'IA EST UNE REVOLUTION POUR LA CYBERSECURITE ?



Objets connectés constituent une cible de choix pour les intrus indésirables et les cyberattaques.

Les systèmes de vidéoprotection constituent une cible de choix pour les intrus indésirables et les cyberattaques.

2017 et 2018 sont deux années mettant en lumière **les maillons faibles de la sécurité électronique** dans le domaine de la **vidéoprotection** et du **contrôle d'accès**.

Le RGPD **impose aux entreprises de sécurité mais aussi aux directeurs et responsables de sécurité électronique** de revoir leur gestion des données personnelles. Les enregistreurs associés notamment aux dispositifs de vidéosurveillance, la deuxième cible des attaques informatiques; après les routeurs !

Et toujours autant de questions pour les DSI, RSSI et décideurs ?

Protection contre la Cyber-Malveillance - Tous concernés ? Ou pas ?

En 2017, l'éditeur américain a recensé **50 000 attaques** sur des objets connectés*,
contre 6 000 l'année précédente.
Les routeurs restent des cibles privilégiées, impliquées en l'occurrence dans 33,6 % des assauts. Suivent les enregistreurs (23,2 %) associés notamment aux dispositifs de vidéosurveillance, les récepteurs satellite (7,3 %), les modems ADSL/câble (7 %), les NAS (3,6 %), les caméras (3,5 %) et les systèmes d'alarme (1,9 %).

Top device type performing attacks against IoT honeypot

This table identifies the types of devices involved in the IoT attacks against the Symantec honeypot in 2017, with routers being the most frequently exploited type of device.

Rank	Device Type	Percent
1	Router	33.6
2	DVR (Digital Video Recorder)	23.2
3	Network	9.3
4	Satellite Dish	7.3
5	DSL/Cable Modem	7
6	SOHO Router	4.7
7	NAS (Network Attached Storage)	3.6
8	Camera	3.5
9	PLC (Programmable Logic Controller)	3.4
10	Alarm System	1.9

Et toujours autant de questions pour les DSI, RSSI et décideurs ?

Intégration du Wi-Fi

Gérer la puissance

Contrôle de la puissance d'émission du Wi-Fi par les bornes

Segmenter le Wi-Fi

Créer de multiples SSID avec VLAN associés et séparer les visiteurs

Programmer

Diffuser le signal Wi-Fi sur plage horaire et/ou activer le PoE sur plage horaire

PoE

Contrôler

Contrôler et faire la journalisation des accès utilisateurs

Ajouter le filtrage par adresses Mac

Gérer les logs

Obligation légale de conservation des activités de navigation sur Internet

Et toujours autant de questions pour les DSI, RSSI et décideurs ?

Intégration d'un système de vidéosurveillance

- Contrôle des accès physiques au site (Portes, fenêtres, parking…)
- Contrôle des équipements et locaux sensibles (Salle serveurs, stock, laboratoire…)
- Enregistrement sur plage horaire, sur détection de mouvements
- Activation du PoE sur plage horaire ?
- VLAN dédié vidéo
- Contrôle des adresses IP des caméras.

Et toujours autant de questions pour les DSI, RSSI et décideurs ?

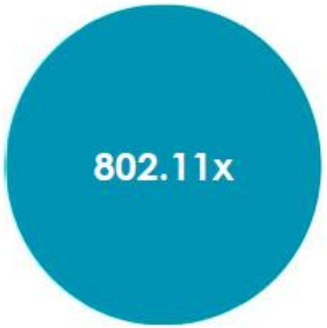
Gestion des accès utilisateurs

Sécurité physique

Limiter l'accès physique aux commutateurs et prises réseau aux seules personnes habilitées

Désactiver

Désactiver toutes les prises du réseau non utilisées



Renforcer l'accès

Renforcer les accès au réseau par mot de passe clients en authentifiant les utilisateurs au préalable

Renforcer les contrôles

Ajouter le contrôles des adresses MAC et IP des équipements connectées par la fonction IMPB

Et toujours autant de questions pour les DSI, RSSI et décideurs ?

Fonctions de sécurité	Caméras IP standards	
HTTPS (SSL/TLS) et certificats	☒	☒
Authentification « Digest » pour HTTP	☒	☒
Liste de contrôle d'accès	☒	☒
Personnalisation des droits (groupes et utilisateurs)	△	☒
Détection d'intrusion	△	☒
Protection contre les bots (web crawling)	⑥	☒
Enregistrements chiffrés	⑥	☒
Vidéos et messages chiffrés	⑥	☒
Client VPN	⑥	☒
Tests externes de cybersécurité	△	☒
Développement logiciel sécurisé	△	☒
Connexion sécurisée optionnelle (MxBus)	⑥	☒

Installation
Matériel Serveur
Stockage
Caméras
Mur d'images
Maintenance

☒ = mis en œuvre

⑥ = non mis en œuvre

△ = seulement partiellement mis en œuvre

La **caméra**,
la **communication**,
l'**enregistrement**,
l'**accès**,
le **VMS***,
les **logiciels**, **le matériel** et la **R&D** sont

FIABLES

Trois Niveaux de Sécurité

Accès à l'interface de Configuration

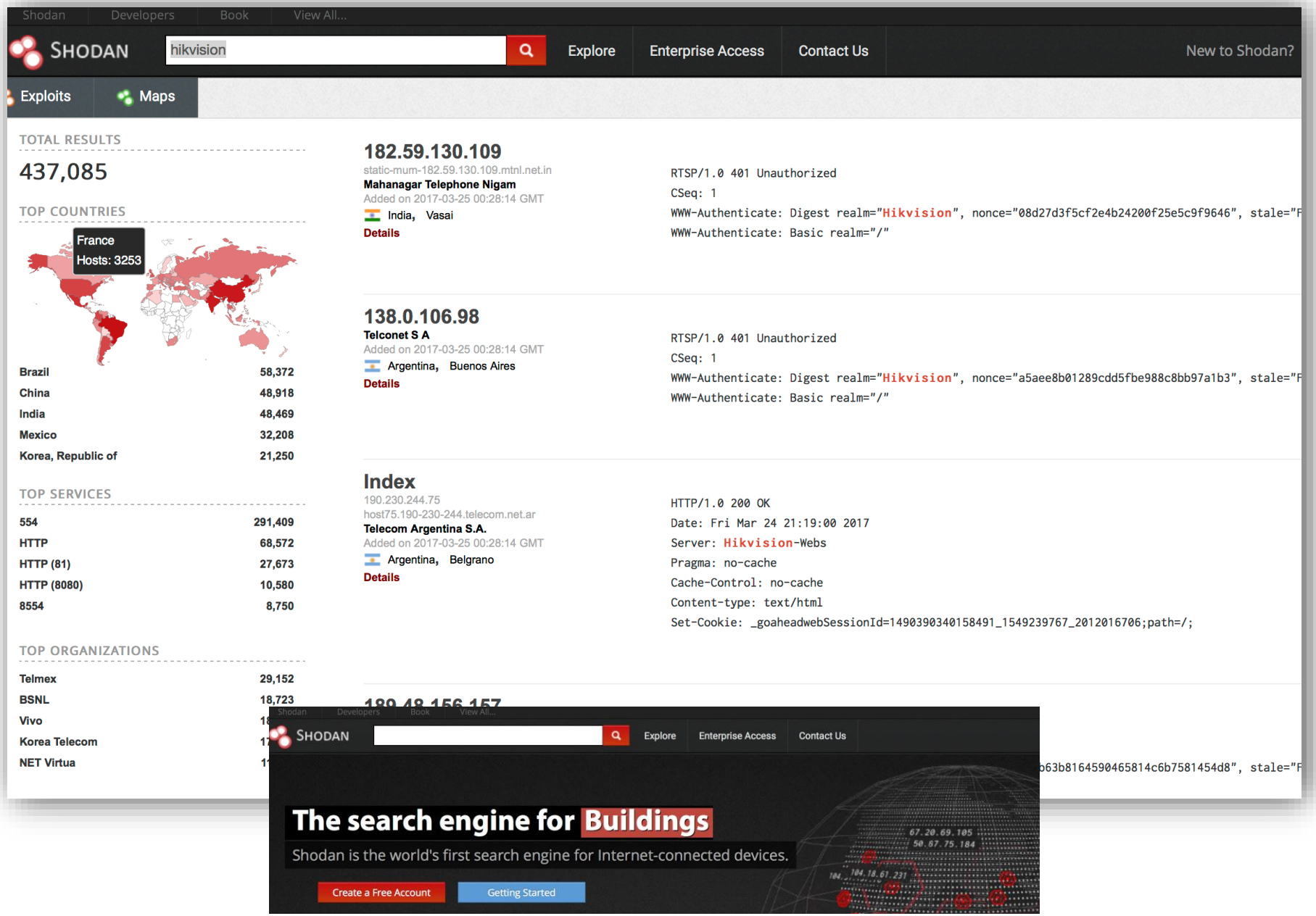
L'accès à l'interface de configuration de la caméra doit être réservé uniquement aux utilisateurs autorisés. De plus, il doit être possible d'ajuster les droits en fonction des groupes d'utilisateurs.

Protocoles de Communication

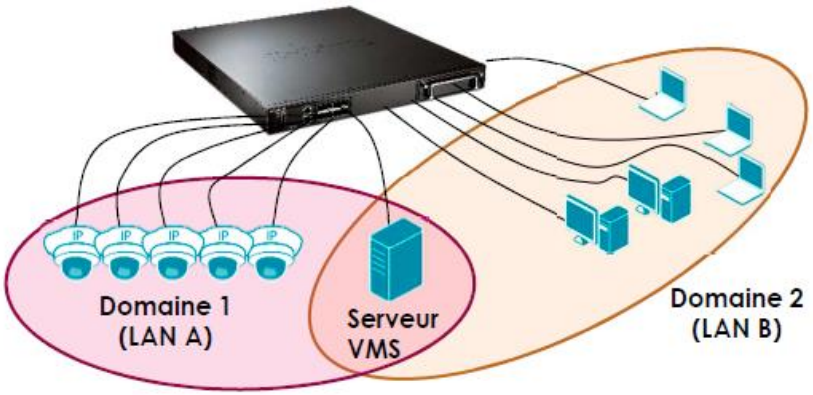
Toutes les données échangées entre la caméra et d'autres clients sur le réseau doivent être cryptés pour assurer leur confidentialité et leur intégrité.

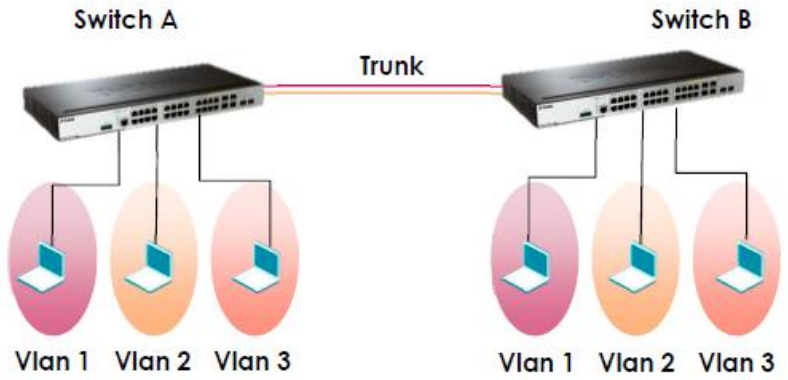
Données Stockées (Enregistrements)

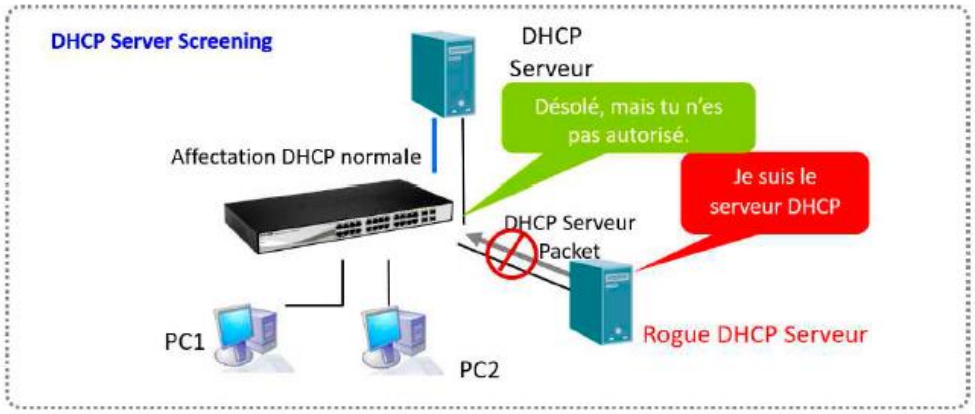
Tous les enregistrements générés par la caméra doivent être cryptés de façon à ce que seuls les utilisateurs autorisés puissent les relire.

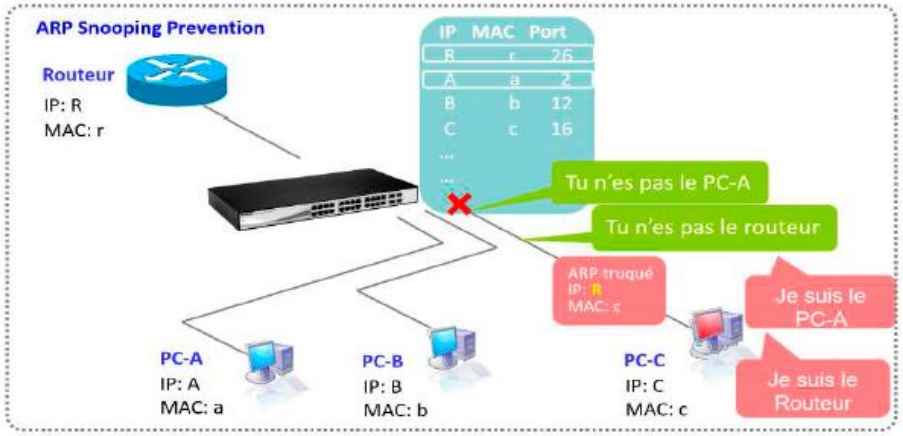

Shodan
Developers
Book
View All...
SHODAN
hikvision
Explore
Enterprise Access
Contact Us
New to Shodan?
Exploits
Maps
TOTAL RESULTS
437,085
TOP COUNTRIES
France
Hosts: 3253
Brazil 58,372
China 48,918
India 48,469
Mexico 32,208
Korea, Republic of 21,250
TOP SERVICES
554 291,409
HTTP 68,572
HTTP (81) 27,673
HTTP (8080) 10,580
8554 8,750
TOP ORGANIZATIONS
Telmex 29,152
BSNL 18,723
Vivo
Korea Telecom
NET Virtua
182.59.130.109
static-mum-182.59.130.109.mtnl.net.in
Mahanagar Telephone Nigam
Added on 2017-03-25 00:28:14 GMT
India, Vasai
Details
RTSP/1.0 401 Unauthorized
CSeq: 1
WWW-Authenticate: Digest realm="Hikvision", nonce="08d27d3f5cf2e4b24200f25e5c9f9646", stale="F
WWW-Authenticate: Basic realm="/"
138.0.106.98
Telconet S A
Added on 2017-03-25 00:28:14 GMT
Argentina, Buenos Aires
Details
RTSP/1.0 401 Unauthorized
CSeq: 1
WWW-Authenticate: Digest realm="Hikvision", nonce="a5aee8b01289cdd5fbe988c8bb97a1b3", stale="F
WWW-Authenticate: Basic realm="/"
Index
190.230.244.75
host75.190-230-244.telecom.net.ar
Telecom Argentina S.A.
Added on 2017-03-25 00:28:14 GMT
Argentina, Belgrano
Details
HTTP/1.0 200 OK
Date: Fri Mar 24 21:19:00 2017
Server: Hikvision-Webs
Pragma: no-cache
Cache-Control: no-cache
Content-type: text/html
Set-Cookie: _goaheadwebSessionId=1490390340158491_1549239767_2012016706;path=/;
Shodan
Developers
Book
View All...
SHODAN
Explore
Enterprise Access
Contact Us
The search engine for Buildings
Shodan is the world's first search engine for Internet-connected devices.
Create a Free Account
Getting Started
67.20.69.105
50.87.75.184
104.18.61.231

Gestion des accès utilisateurs









En 2050 et d'ici là ?

3 enjeux majeurs…. Parmi beaucoup d'autres

Bâtiment durable et valorisé

- 50% des bâtiments existants seront encore utilisés en 2050.
- 90% des bâtiments européens ont besoin d'être rénovés.
- Le nombre de produits connectés est en forte croissance.
- Un bâtiment évolutif aux tendances du marché.

Productivité et Expérience des usagers

- 22% des salariés ont peur d'être dépassés par les nouveaux outils et les changements technologiques.
- 77% pensent avoir une bonne maîtrise des outils informatiques et des logiciels qu'ils utilisent dans leur travail (-3 points vs 2015).
- 55% des salariés ont le sentiment d'être ou de pouvoir être contrôlés à tout moment (+4 points vs 2010).

Efficacité Opérationnelle

- Les échanges d'information et de données sont en croissance exponentielle.
- Adaptabilité à la mobilité des utilisateurs .
- 40% des effectifs de services en moins d'ici 2025 du fait de la Digitalisation.

Vos priorités ? Votre budget ?

Besoins clients

- Un bâtiment conforme aux exigences de performances actuelles & futures
- Disposer d'une infrastructure capable de supporter plusieurs générations d'actifs.
- Perfomance, évolutivité, interopérabilité

Besoins clients

- Assurer une continuité de service en limitant les temps d'arrêt et les inefficiences opérationnelles
- Minimiser les erreurs, optimiser l'exploitation et la maintenance de l'infrastructure
- Assurer la sécurité et la disponibilité

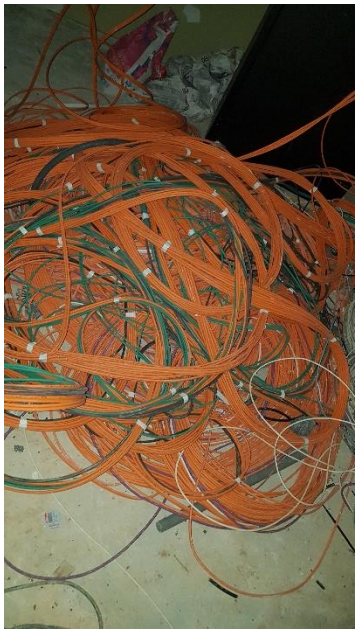
Besoins clients

- Maintenir & améliorer la productivité
- Proposer de bonnes conditions de travail par une connectivité garantie
- Assurer la satisfaction des usagers

NE pas confondre politique et informatique ?
Diversité des législations selon les pays
Remise en question ? Accompagnement ?

Et un peu de sécurité ?
Et un peu de tranquillité d'esprit ?
Et éventuellement se concentrer sur son business ?

Les Infrastructures Fibre Optique comment ont-elles évoluées ? Depuis 2006 ? Depuis 2010 ?



Les exigences de bande passante ont elles évoluées ?

Avez-vous plus de liens à certifier ? À dépanner ?

Rencontrez-vous plus d'erreurs lors de la certification ?

D'où viennent ces erreurs ?

Les dépannages sont ils plus compliqués ? Plus longs ?

Avez-vous plus de temps pour certifier ?

Avez vous plus de ressources ?

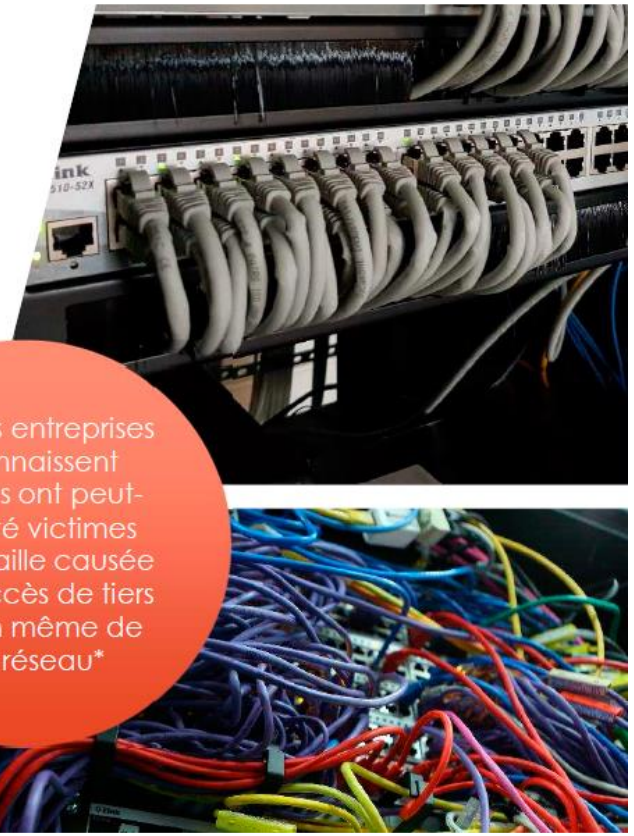
Ces Infrastructures sont elles documentées ?

Des Infrastructures Fibre Optique performantes :

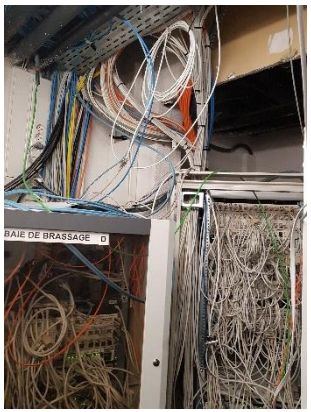
- Une bonne connaissance des Normes, Méthodologies et Meilleures pratiques
- Des solutions de gestion de projet, de certification et de dépannages adaptés

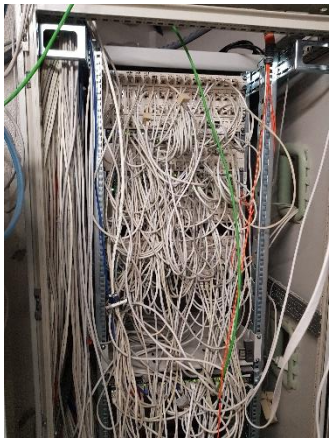
Le réseau dans une entreprise aujourd'hui et les risques encourus

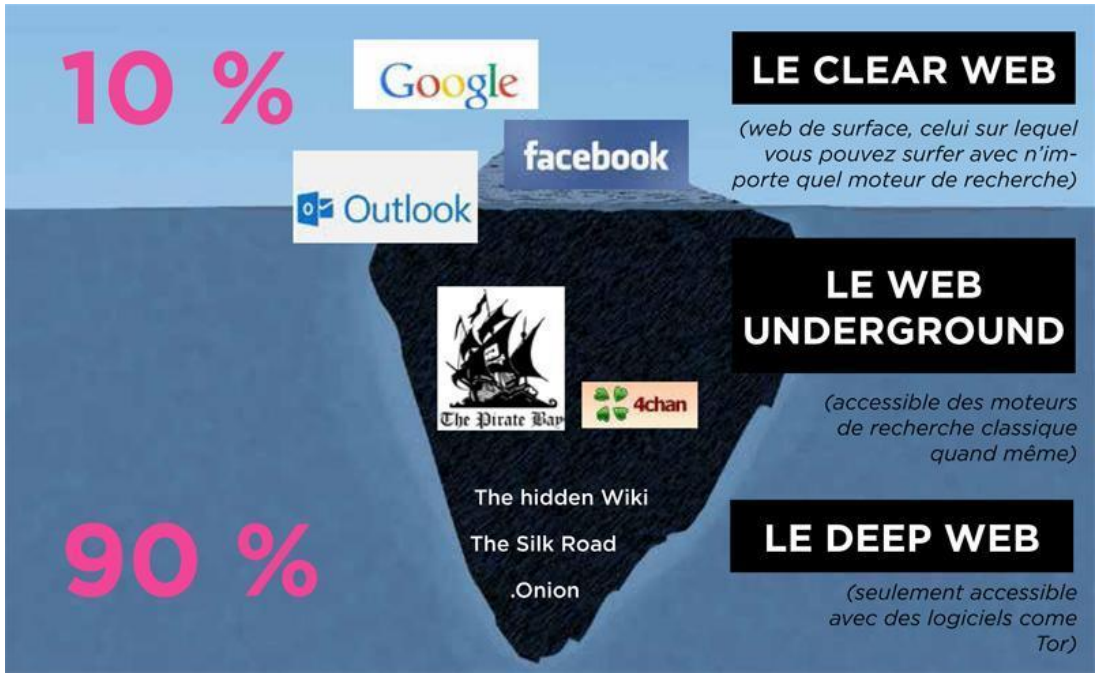
- **Menace** : Intrusion physique dans les locaux et/ou incendie
  - *Vol du matériel informatique, destruction, perte d'activité*
- **Menace** : Panne disque dur
  - *Perte définitive de données (Absence de sauvegarde externe)*
- **Menace** : Panne partielle ou générale du système informatique
  - *Impossibilité de poursuite rapide d'activité*
- **Menace** : Réseau ouvert, sans sécurité
  - *Fuite de données confidentielles et/ou mise hors service du système*
- **Menace** : Attaque cybercriminelle
  - *Fuite de données confidentielles et/ou mise hors service du système*
- **Menace** : Mauvaises pratiques utilisateurs
  - *Fuite de données confidentielles et/ou mise hors service du système*

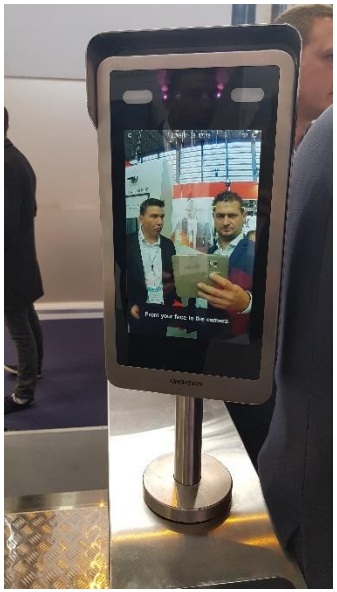


66% des entreprises reconnaissent qu'elles ont peut-être été victimes d'une faille causée par l'accès de tiers au sein même de leur réseau*



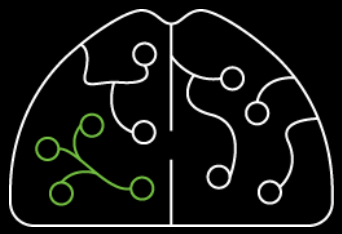






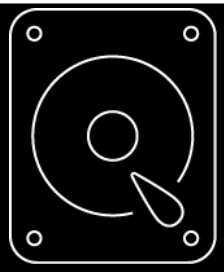
Compétition mondiale
Enjeux économiques
Rachat / GAFA ….

La taille ne compte pas ?



EFFICACITE

SIMPLICITE



PERFORMANCE

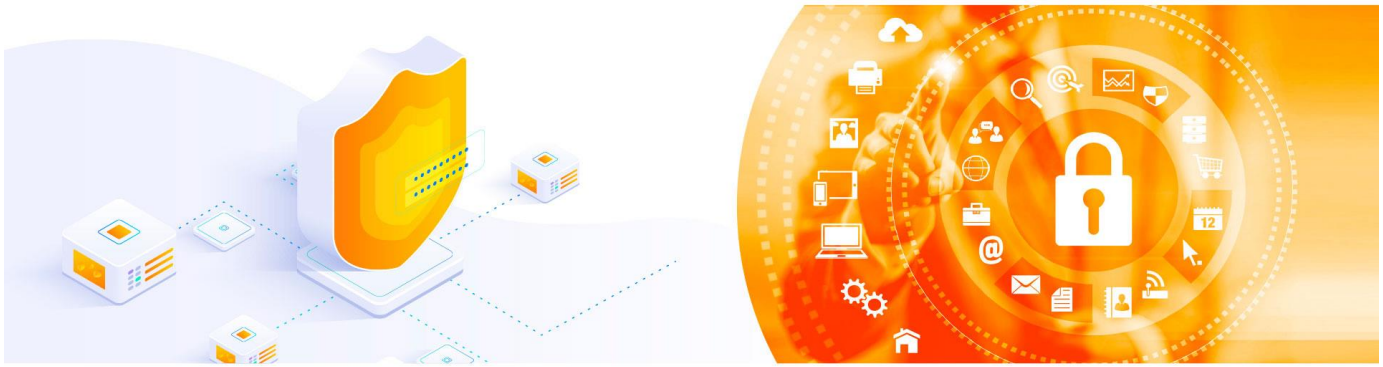
Merci pour votre écoute ! Des questions ?

06 20 36 16 59

ivan@tanco.fr

AFTERWORK CYBERSÉCURITÉ #03

organisé par le MCABH et Tanco & Co



ÉTAT DES LIEUX DES MENACES FIN 2018

Face à des cyber-attaques incessantes, comment se protéger ?

JEUDI 6 DÉCEMBRE 2018

À partir de 17h30

Ateliers, conférences & cocktail dinatoire

Golden Tulip Sophia Antipolis

120, route des Macarons - 06560 Valbonne

inscription : koolcrm@tanco.fr