# Sécurisation des SI
# Plans de continuité
# DataCenter et Cloudcomputing
# RGPD

IT-OPSLINK

IT-OPSLINK

- Expert en télécommunications, systèmes d'information et cyber sécurité
- Conception et déploiement de multiples systèmes d'information et de communication civils et militaires (SICA,SITRANS, SDIS, Bi-SC AIS, automatisation de ligne de métro, impots.gouv.fr)
- Président au sein d'EOS d'un groupe d'experts pour fournir des recommandations en cyber sécurité au profit de la Commission Européenne
- Conduite de projets de recherche cyber sécurité FP7 , H2020 : GLOBE, CRISYS, EURACOM
- Fondateur de IT-OPSLINK en 2014 : PME spécialisée en formation sur mesure et déploiement de solutions cyber sécurité pour les TPE et PME
- AMOA pour le projet de recherche : Méthodologie de gestion de crise au centre commun de gestion de crise cybernétique de l'Université de Bretagne Sud

Jp.perin@it-opslink.com
www.it-opslink.com

Support de cours @ http://

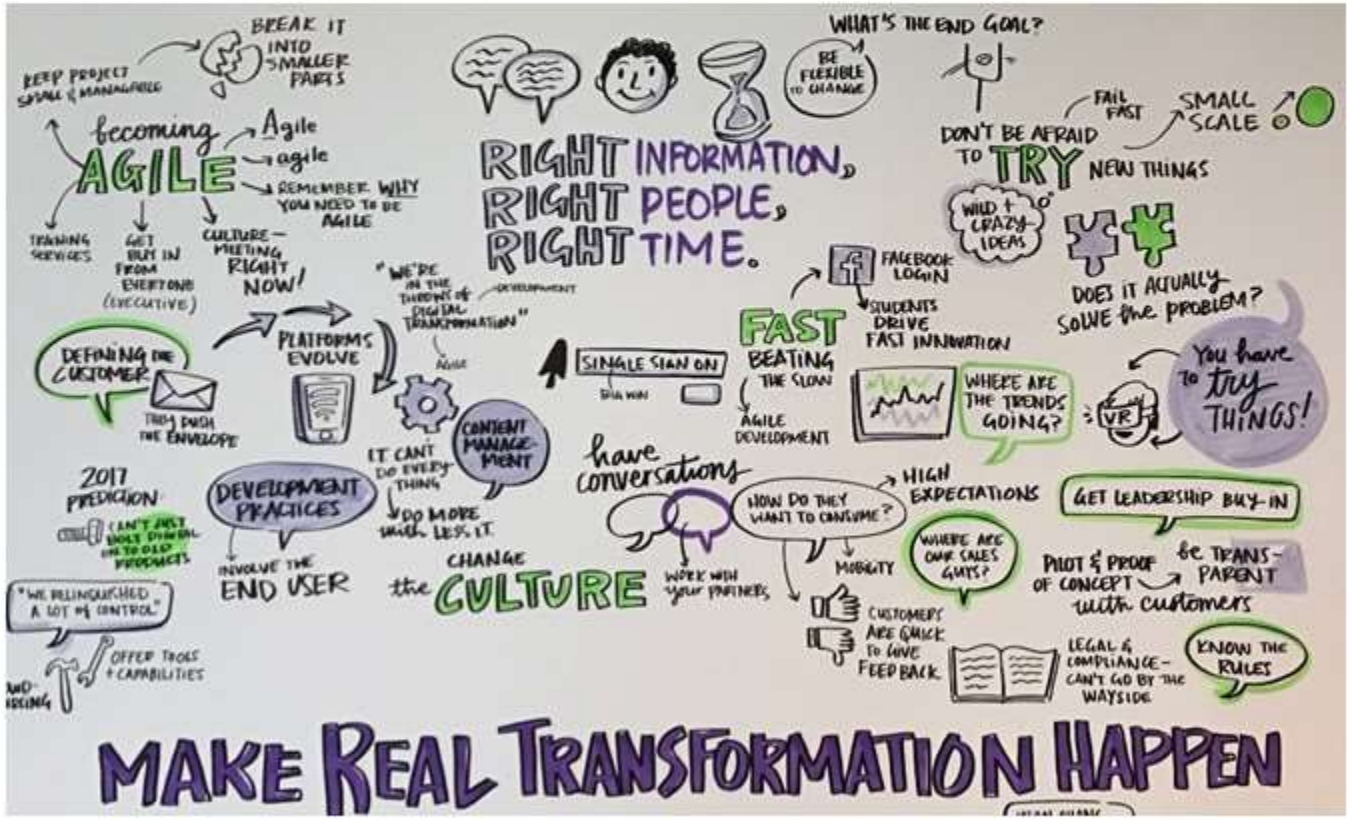

Risques numériques
MRT de sécurisation
Sécurisation des architectures SI et ICS
Datacenter et Cloud Computing
RGPD

les défis des nouvelles technologies sur les usages et le traitement e l'information

# La sécurite d'entreprise dans un monde en perpétuelle évolution

**« La plus grande difficulté de la transformation numérique, c'est de changer la roue de la voiture sans l'arrêter. »**

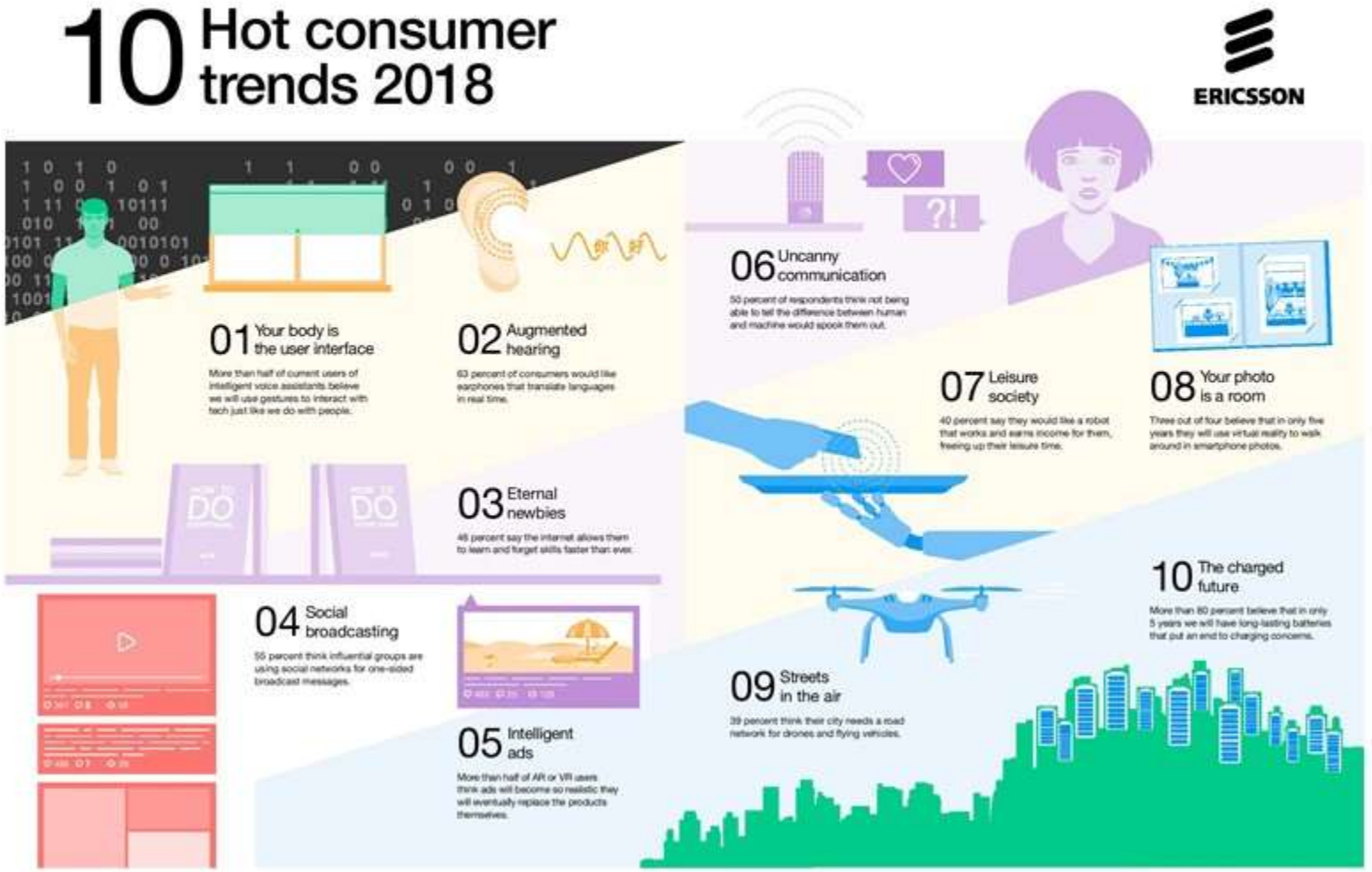
– **Éric Blot**, Président, Awak'IT (Forum CXP, juin 2016).




Idées maîtresses ?

# Les nouvelles incitations impactent la sécurité des données

**L'expérience du client prime. Dans les magasins, les consommateurs vont choisir avec leurs pieds, en ligne avec leurs doigts : ce sont les services les plus pratiques qui s'imposeront. »**



# Top 5 Communication Technology Trends That Will Shape 2020




# Les cyber risques (rappel)

# Rappel - L'environnement numérique et ses acteurs

**Tout le monde est connecté et donc devient une cible potentielle**

- Entreprises
- Employés
- Partenaires
- Clients

# La réalité de notre monde connecté – Rien de paisible

# Professionnalisation des cyber attaquants **Crime as a Service**

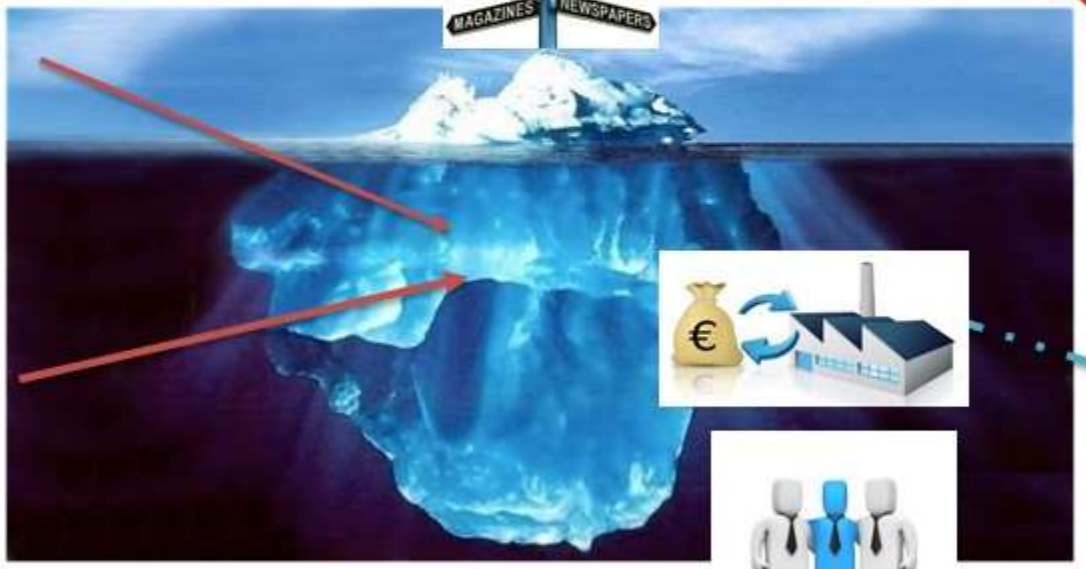
**Cyber attaquants :**

- **Objectifs** : gagner de l'argent facilement ou déstabiliser un gouvernement

- **Moyens** :
  - outils développés par des spécialistes et mis à disposition sous forme de service (CaaS : Crime as a Service)
  - Investissement dans le développement de nouvelles techniques d'attaque

- **Top des outils** :
  - Le rançongiciel (ransomware)
  - Le déni de service distribué (DDOS)
  - Le piratage des téléphones mobiles : applications piégées sur Apple Store, Google Play
  - Le détournement des aides vocales : Sir, Cortina
  - Les virus permettant l'observation silencieuse de vos activités (analyseur de frappe : keylogger)

# Les outils de cyber attaquent ciblent les entreprises vulnérables









WannaCry Ransomware Attack

Merck

Maersk

NHS Hospital (UK)

???

Publié le 19 septembre 2017 à 10h22 | Mis à jour le 19 septembre 2017 à 19h54

# Cent mille Canadiens touchés par le piratage d'Equifax


Equifax a été victime d'une cyberattaque massive.
PHOTOTHÈQUE LE SOLEIL

# Equifax a redirigé des clients vers un site d'hameçonnage

PUBLIÉ LE JEUDI 21 SEPTEMBRE 2017 À 22 H 18


La faille de sécurité informatique touche environ 143 millions de consommateurs aux États-Unis. Photo : Reuters/Dado Ruvic

**L'agence d'évaluation du crédit Equifax a dirigé ses clients inquiets, dont les informations personnelles ont été compromises dans une attaque informatique, vers un site d'hameçonnage à au moins quatre reprises, ont appris des médias américains.**

Radio-Canada avec The New York Times et The Verge

Les jours se suivent et se ressemblent pour Equifax. Après s'être fait voler les renseignements personnels de 143 millions de ses clients nord-américains, dont 100 000 Canadiens, et que la filiale argentine de l'entreprise a été surprise à utiliser le mot de passe « admin », voilà qu'Equifax a une fois de plus été prise en flagrant délit de négligence.

# Négligences EQUIFAX=> conséquences à assumer

**Perte de confiance** des clients ou des partenaires (chute immédiate des actions en bourse de plus de 14%)

**Pertes financières**

- Perte de clientèle (crédits)
- Indemnités ou coûts de suivi pour les dizaines de millions de données confidentielles volées dont numéro de sécurité sociale (usurpation d'identité)
- Coût des audits …
- Coût de restauration des systèmes
- Coût des sanctions pénales ?

**Responsabilités civiles et pénales engagées (Direction)**

- Sécurité nationale engagée (employés fédéraux)
- Gestion du risque et mesures préventives insuffisantes
- Gestion des incidents : interrogation sur les délais pour informer les clients un mois après la découverte de la brèche
- Plaintes en nom collectif

# Evolution cyber attaques 2018

- **Ransomware** tels que Wannacry et NotPetya en augmentation : un milliard de profit en 2017

- **Explosion du crypto-jacking** utilisation de JavaScript sur une page pour miner des cryptocurrencies lors d`une visite sur un site web visite sans installation

*Cryptojacker* consiste à utiliser l'ordinateur de quelqu'un à son insu, pendant quelques secondes, pour générer de la cryptomonnaie

*Microsoft estime désormais que plus de 600.000 PC sont exposés à des logiciels malveillants de cryptomining chaque mois. Et des salariés pourraient être tentés d'installer des outils d'extraction de monnaie virtuelle sur le parc de l'entreprise pour gagner de l'argent*

- **Les attaques basées sur PowerShell seront amenées à augmenter**

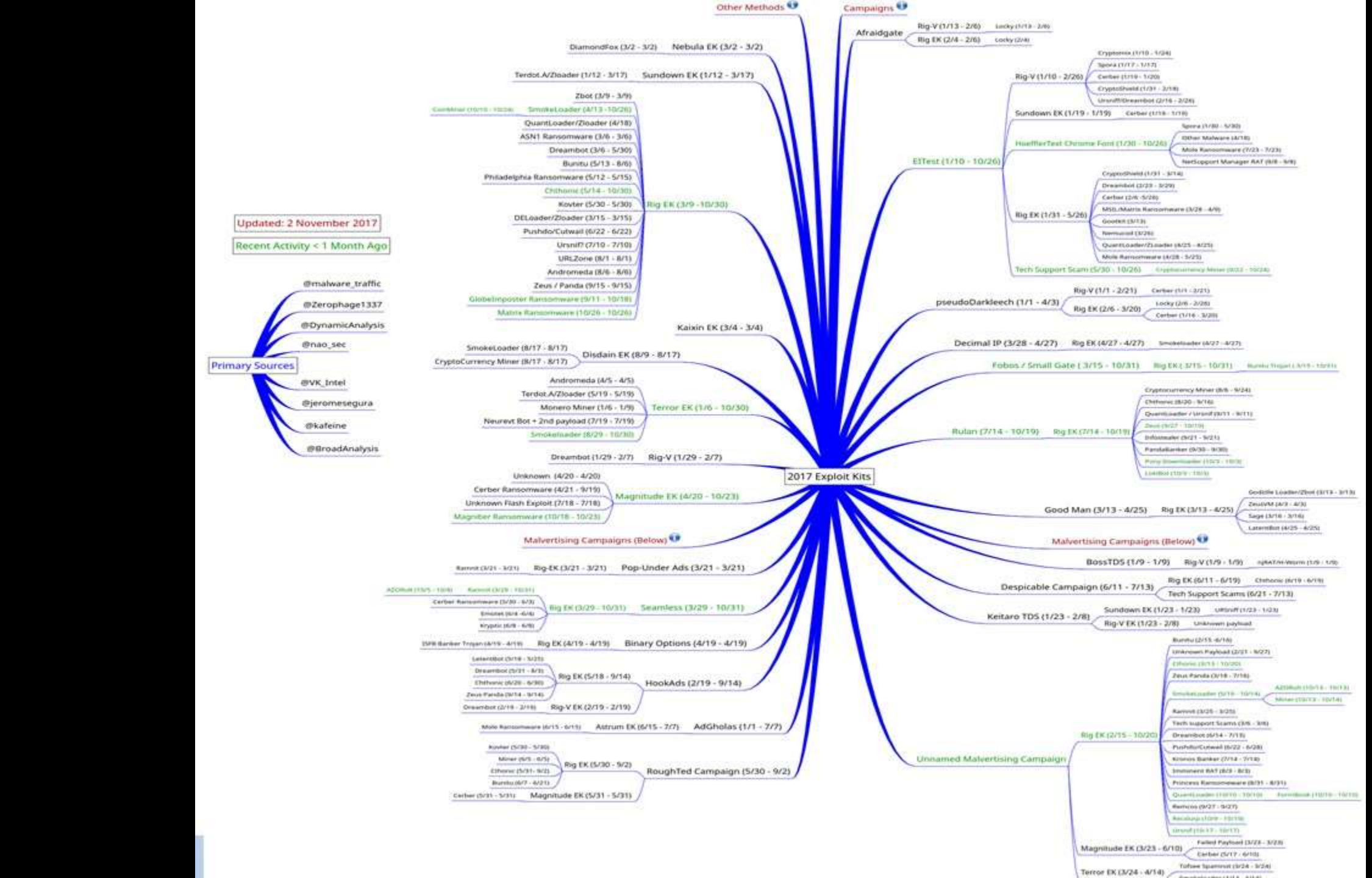
*Il y a quelque mois, des membres du gouvernement saoudien ont été attaquées via une macro du logiciel Word qui a infecté les ordinateurs avec des chevaux de Troie voleurs d'informations. Plutôt que de récupérer une charge utile binaire, l'attaque s'est appuyée sur des scripts malveillants pour communiquer avec des sites Web compromis. Ces attaques basées sur des scripts, et en particulier celles basées sur PowerShell, sont extrêmement difficiles à identifier et peuvent facilement échapper aux antivirus.*

- **Les logiciels de sécurité auront une cible attachée dans le dos**

*En 2018, les cybercriminels cibleront et exploiteront davantage les logiciels de sécurité. En ciblant ces programmes de confiance et la chaîne d'approvisionnement logicielle et matérielle, les attaquants peuvent contrôler les dispositifs et manipuler sans réserve les utilisateurs. Les pirates informatiques tireront parti des produits de sécurité et les exploiteront, soit par une corruption directe de l'agent installé sur le poste de travail, soit en interceptant et en redirigeant le trafic du cloud pour atteindre leurs objectifs. Au fur et à mesure que ces pratiques seront plus connues du public, la perception des logiciels de sécurité, en particulier celle des antivirus traditionnels se détériorera encore davantage.*

- **L'IoT va créer de nouveaux défis dans le domaine de la santé**

*La possibilité pour les dispositifs médicaux de se connecter au Web, rendue possible par l'Internet des objets (IoT) offre de nombreux avantages. Une plus grande connectivité signifie de meilleures données, une meilleure analyse et de meilleurs soins offerts aux patients. Mais elle ouvre aussi la porte à de nouvelles menaces comme la perte de données particulièrementsensibles puisqu'elles concernent la santé et à l'accès non autorisé aux appareils.*


Updated: 2 November 2017
Recent Activity < 1 Month Ago
Primary Sources
@malware_traffic
@Zerophage1337
@DynamicAnalysis
@nao_sec
@VK_Intel
@jeromesegura
@kafeine
@BroadAnalysis
2017 Exploit Kits
Other Methods
Campaigns
Afraidgate
Rig-V (1/13 - 2/6)
Rig EK (2/4 - 2/6)
EITest (1/10 - 10/26)
Rig-V (1/10 - 2/26)
Sundown EK (1/19 - 1/19)
HoefflerText Chrome Font (1/30 - 10/26)
Rig EK (1/31 - 5/26)
Tech Support Scam (5/30 - 10/26)
pseudoDarkleech (1/1 - 4/3)
Rig-V (1/1 - 2/21)
Rig EK (2/6 - 3/20)
Decimal IP (3/28 - 4/27)
Rig EK (4/27 - 4/27)
Fobos / Small Gate ( 3/15 - 10/31)
Rig EK ( 3/15 - 10/31)
Rulan (7/14 - 10/19)
Rig EK (7/14 - 10/19)
Good Man (3/13 - 4/25)
Rig EK (3/13 - 4/25)
Malvertising Campaigns (Below)
BossTDS (1/9 - 1/9)
Rig-V (1/9 - 1/9)
Despicable Campaign (6/11 - 7/13)
Rig EK (6/11 - 6/19)
Tech Support Scams (6/21 - 7/13)
Keitaro TDS (1/23 - 2/8)
Sundown EK (1/23 - 1/23)
Rig-V EK (1/23 - 2/8)
Unnamed Malvertising Campaign
Rig EK (2/15 - 10/20)
Magnitude EK (3/23 - 6/10)
Terror EK (3/24 - 4/14)
Nebula EK (3/2 - 3/2)
DiamondFox (3/2 - 3/2)
Sundown EK (1/12 - 3/17)
Terdot.A/Zloader (1/12 - 3/17)
Rig EK (3/9 - 10/30)
Zbot (3/9 - 3/9)
SmokeLoader (4/13 - 10/26)
QuantLoader/Zloader (4/18)
ASN1 Ransomware (3/6 - 3/6)
Dreambot (3/6 - 5/30)
Bunitu (5/13 - 8/6)
Philadelphia Ransomware (5/12 - 5/15)
Chthonic (5/14 - 10/30)
Kovter (5/30 - 5/30)
DELoader/Zloader (3/15 - 3/15)
Pushdo/Cutwail (6/22 - 6/22)
Ursnif (7/10 - 7/10)
URLZone (8/1 - 8/1)
Andromeda (8/6 - 8/6)
Zeus / Panda (9/15 - 9/15)
GlobeImposter Ransomware (9/11 - 10/18)
Matrix Ransomware (10/26 - 10/26)
Kaixin EK (3/4 - 3/4)
Disdain EK (8/9 - 8/17)
SmokeLoader (8/17 - 8/17)
CryptoCurrency Miner (8/17 - 8/17)
Terror EK (1/6 - 10/30)
Andromeda (4/5 - 4/5)
Terdot.A/Zloader (5/19 - 5/19)
Monero Miner (1/6 - 1/9)
Neurevt Bot + 2nd payload (7/19 - 7/19)
Smokeloader (8/29 - 10/30)
Rig-V (1/29 - 2/7)
Dreambot (1/29 - 2/7)
Magnitude EK (4/20 - 10/23)
Unknown (4/20 - 4/20)
Cerber Ransomware (4/21 - 9/19)
Unknown Flash Exploit (7/18 - 7/18)
Magniber Ransomware (10/18 - 10/23)
Malvertising Campaigns (Below)
Pop-Under Ads (3/21 - 3/21)
Rig-EK (3/21 - 3/21)
Seamless (3/29 - 10/31)
Rig EK (3/29 - 10/31)
Cerber Ransomware (5/30 - 6/3)
Binary Options (4/19 - 4/19)
Rig EK (4/19 - 4/19)
HookAds (2/19 - 9/14)
Rig EK (5/18 - 9/14)
Dreambot (5/31 - 8/3)
Chthonic (6/20 - 6/30)
Rig-V EK (2/19 - 2/19)
AdGholas (1/1 - 7/7)
Astrum EK (6/15 - 7/7)
RoughTed Campaign (5/30 - 9/2)
Rig EK (5/30 - 9/2)
Kovter (5/30 - 5/30)
Miner (6/5 - 6/5)
Chthonic (5/31- 9/2)
Bunitu (6/7 - 6/21)
Magnitude EK (5/31 - 5/31)

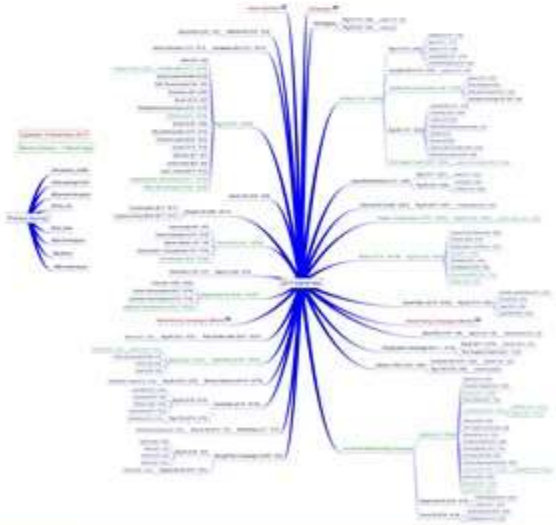
# Les nouveaux enjeux sécuritaires

## Surface d'attaque grandissante

Nouveaux usages, système d'information étendu, objets connectés, nuage informatique

## Un équilibre à trouver


## Évolution des menaces et outils



## De multiples impacts

**Perte de confiance** des clients ou des partenaires (image de l'entreprise)

**Pertes financières** (stabilité financière de l 'entreprise menacée)

- Non production
- Vol ou modification de données confidentielles
- Menaces environnementaux dans le cas des entreprises sensibles

**Responsabilités civiles et pénales engagées** (inéligibilité et indemnités)

# La cyber sécurité

# Surface d'attaque grandissante des entreprises / collectivités

**L'entreprise est connectée** et est visible sur internet

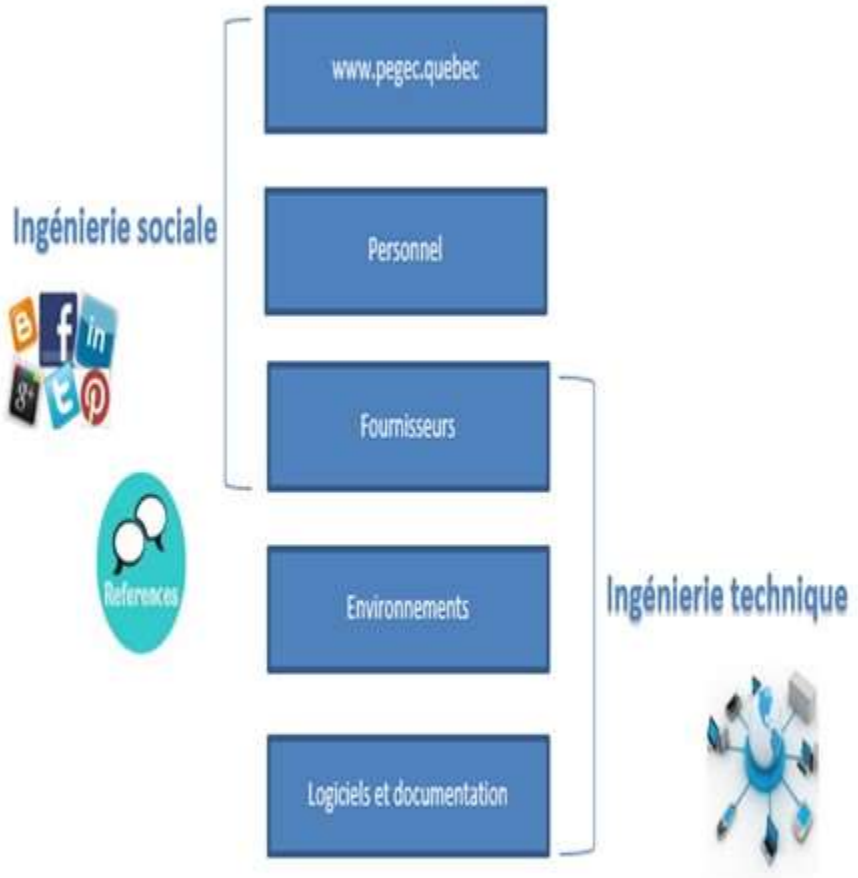
- Portail de services
- Commerce en ligne
- Utilisation des réseaux sociaux

**Son information est devenue dispersée et consultable à distance**

- Utilisation des téléphones intelligents pour consulter sa messagerie
- Stockage des données dans l'info nuage (cloud)

**Besoins de s'afficher pour être reconnu**

**Le matériel et les applications (logiciels) sont disparates** et difficiles à gérer



# Nouveaux usages – nouveaux risques – pas de formation dédiée

## Plus de 90% des attaques se font via les utilisateurs

Collaboration dans les nuages sans confidentialité

C

Services et données accessibles tout le temps et n'importe où : téléphones intelligents, tablettes non protégés


M

Employé(e)s et client(e)s multi-réseaux sociaux

S

T

Produits / service attractifs mais non sécurisés

A

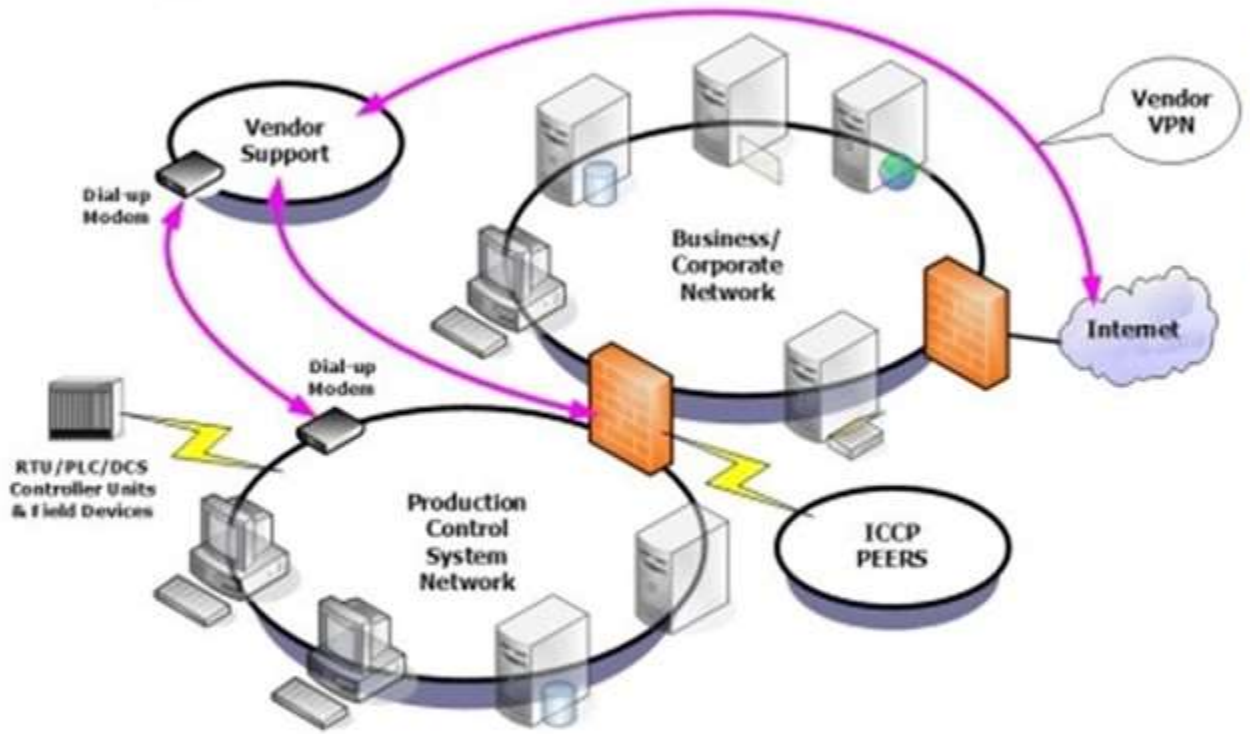
Analyse , récolte des données comportementales –> bataille commerciale

H

Télétravail, nomadisation

# Niveau technique - Des réseaux difficiles à protéger

**Vendor Support**



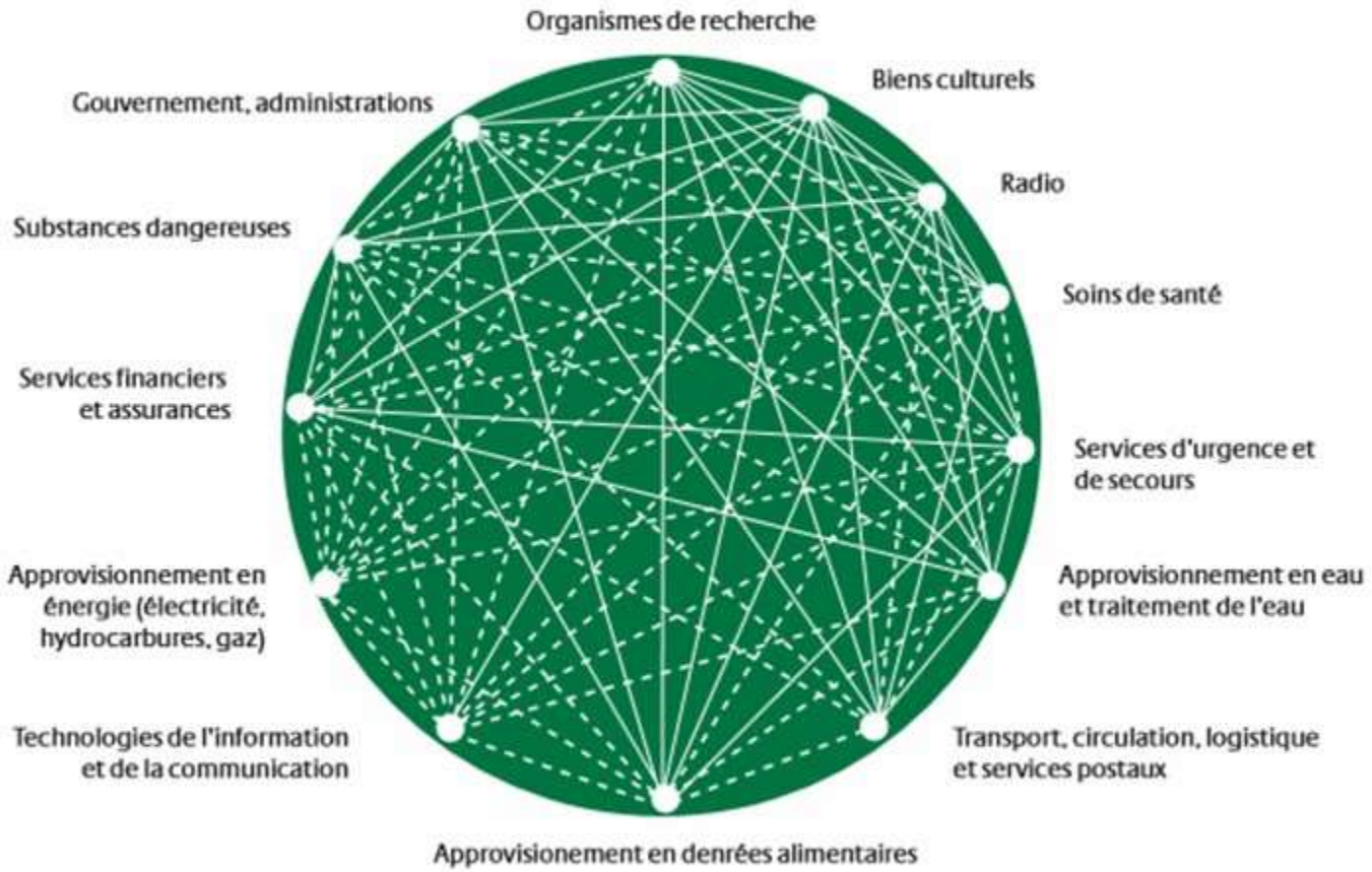

large version

**Figure 8: Vendor support**

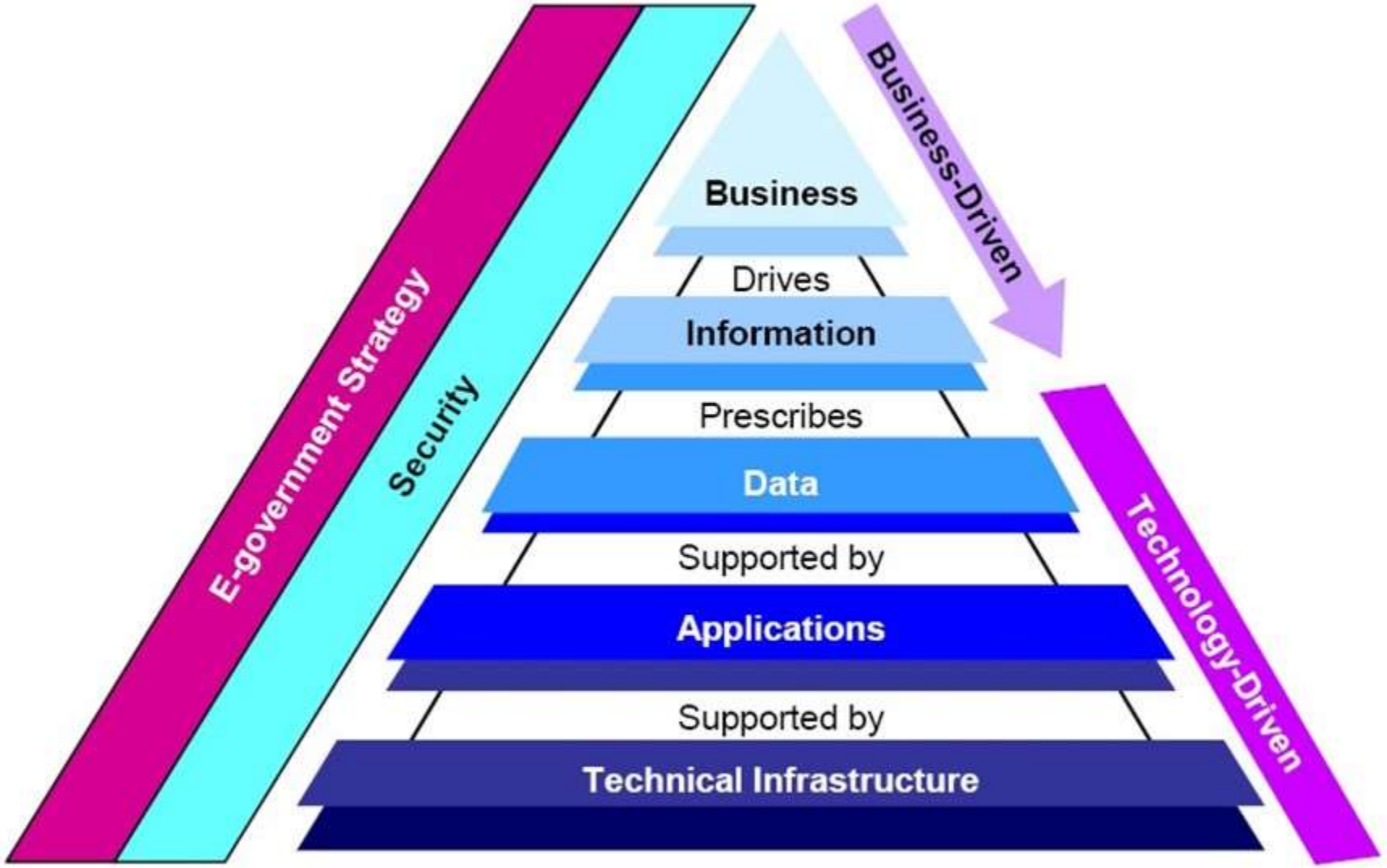
- Accès à distance multiples
- Protocoles multiples
- Acteurs multiples

# Interdépendance des infrastructures – OIV

**Illustration 1 : Interdépendances entre certaines infrastructures critiques**



# Tout est lié - la sécurité est l'affaire de tous



# La sécurité numérique est un problème culturel


**Simple**

- ✓ Apprentissage obligatoire
- ✓ Respect des contrôles techniques (visites obligatoires du véhicule)
- ✓ Prise de conscience : Responsable tout le temps


**Complexe**

- ➢ Pas d 'apprentissage obligatoire (cyber-hygiène)
- ➢ Méconnaissance des exigences de sécurité (obligations légales)
- ➢ Pas de prise de conscience des dangers numériques

SÉCURITÉ NUMÉRIQUE

TOUS RESPONSABLES

Direction

Utilisateurs

Informatique

# L’entreprise / la collectivité face à ces enjeux

# Enjeux de la sécurité des systèmes d'information (SI)

**4 enjeux pour l'entreprise**

- **Protéger ses atouts informationnels** : données sensibles, propriété intellectuelle
- **Obligation de conformité** par apport aux règlements gouvernementaux et internationaux (RGPD : règlement général pour la protection des données concernant l'ensemble des citoyens européens)
- **Assurer la continuité de ses services :=> résilience**
- **Savoir gérer les incidents et les crises lors de cyber incidents**

# Les ingrédients de l'insécurité

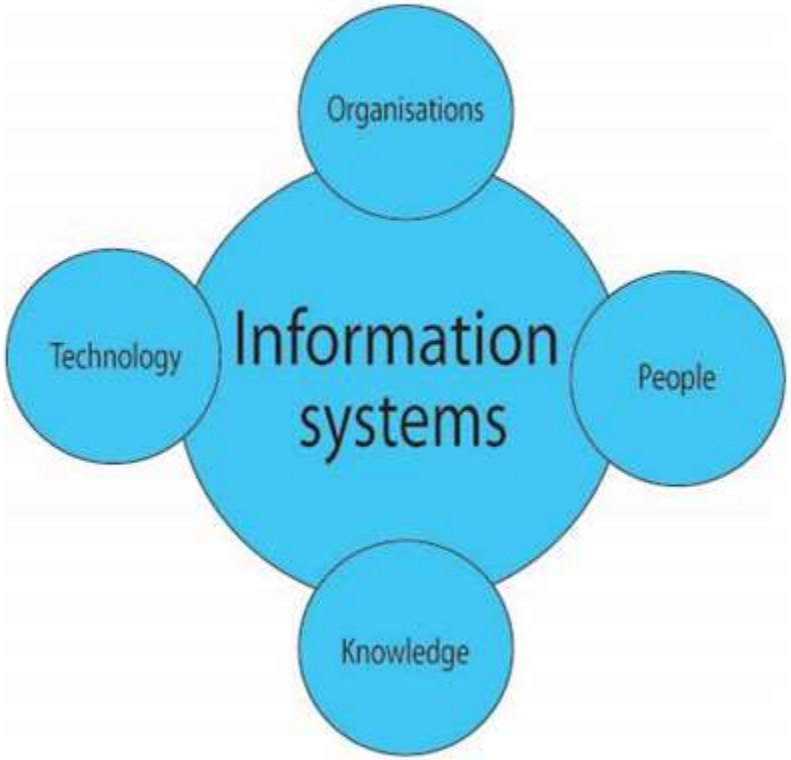
- **Les éléments qui favorisent et entretiennent un incendie sont: l'oxygène, la chaleur et les produits inflammables (essence, gaz, mazout, etc.).** L'enlèvement d'un élément de ce triangle a comme effet la disparition de l'incendie.

- **En matière de sécurité informatique, on joue aussi avec trois éléments:**
  - ceux qui attaquent (par exemple les hackers),
  - les vulnérabilités des systèmes et des logiciels,
  - les ressources et/ou les informations ciblées.

On peut en déduire que sans ceux qui attaquent, les protections n'ont plus de sens. Il en va de même pour les vulnérabilités des systèmes et des logiciels

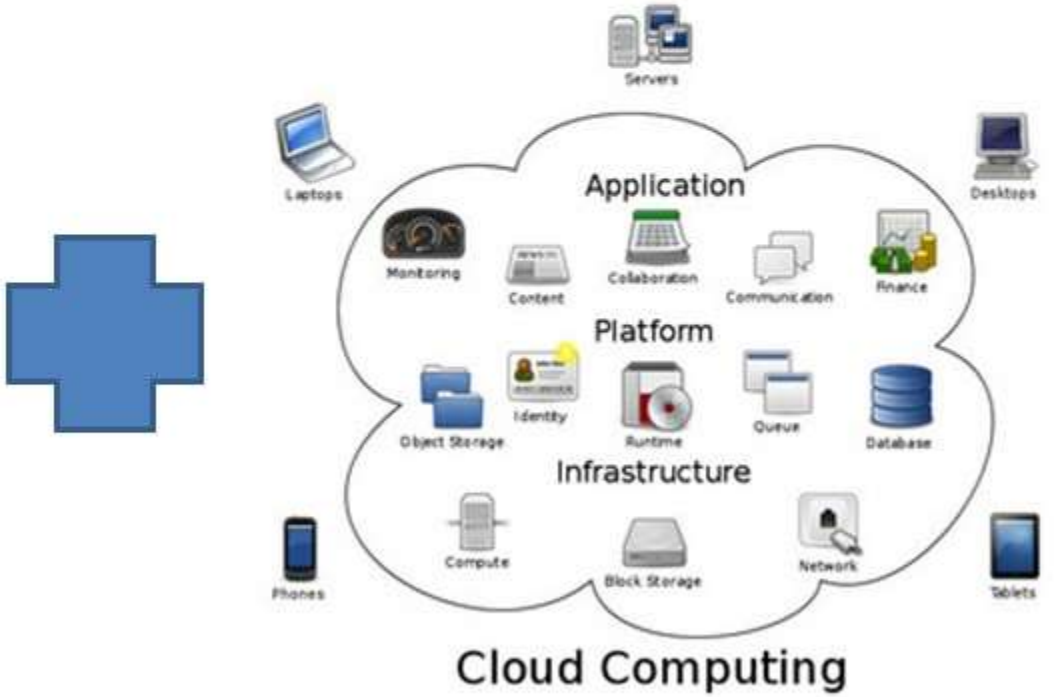
# Le système d'information

**Un Système d'Information est défini comme un ensemble de ressources** (personnel, logiciels, processus, données, matériels, équipements informatique et de télécommunication…) permettant la collecte, le stockage, la structuration, la modélisation, la gestion, la manipulation, l'analyse, le transport, l'échange et la diffusion des informations (textes, images, sons, vidéo…) au sein d'une organisation.



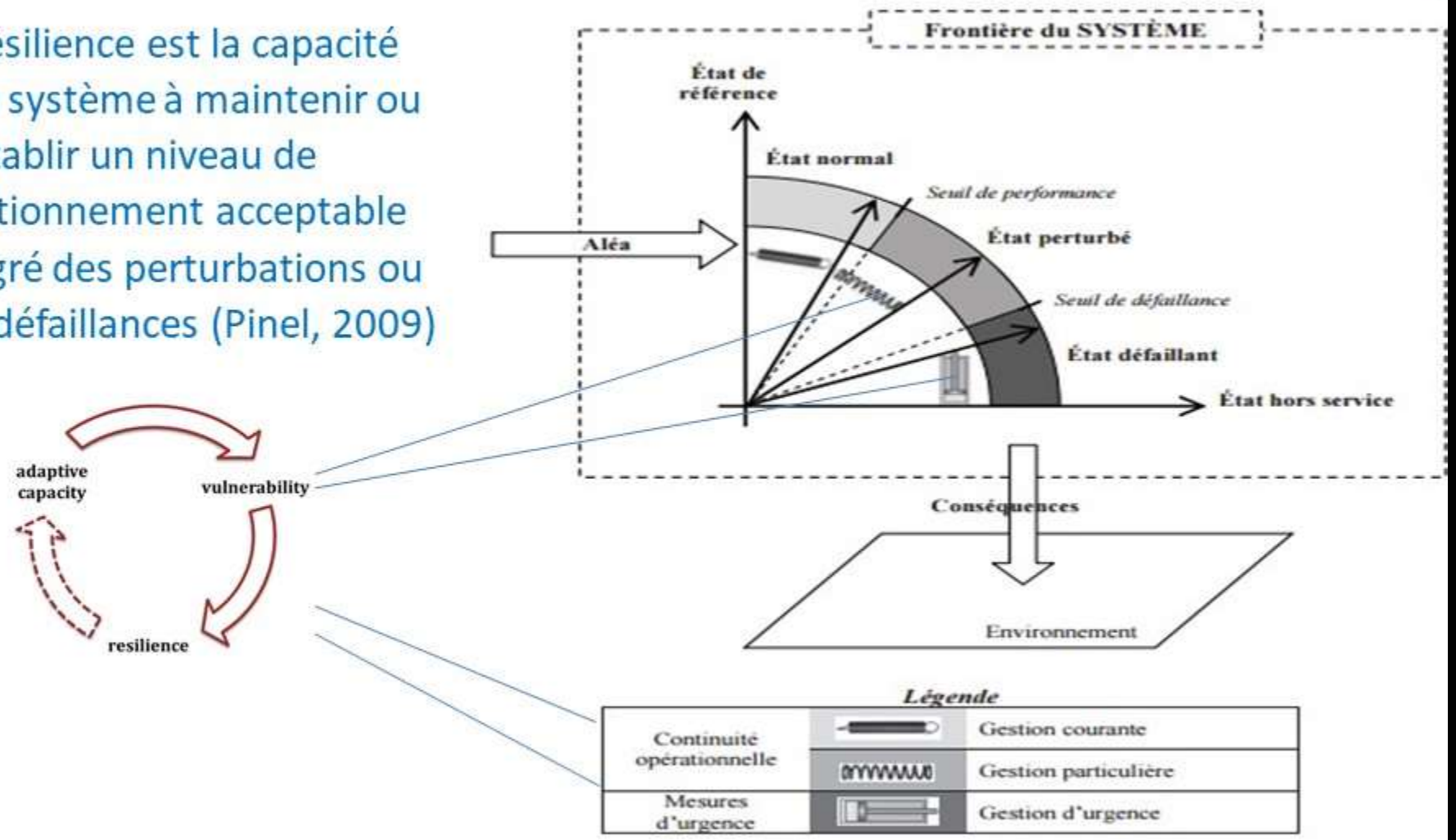
# Cybersécurité

Cybersécurité concerne la protection de toute l'information stockée numériquement ainsi que les moyens électroniques associés pour assurer la disponibilité, l'intégrité, la confidentialité

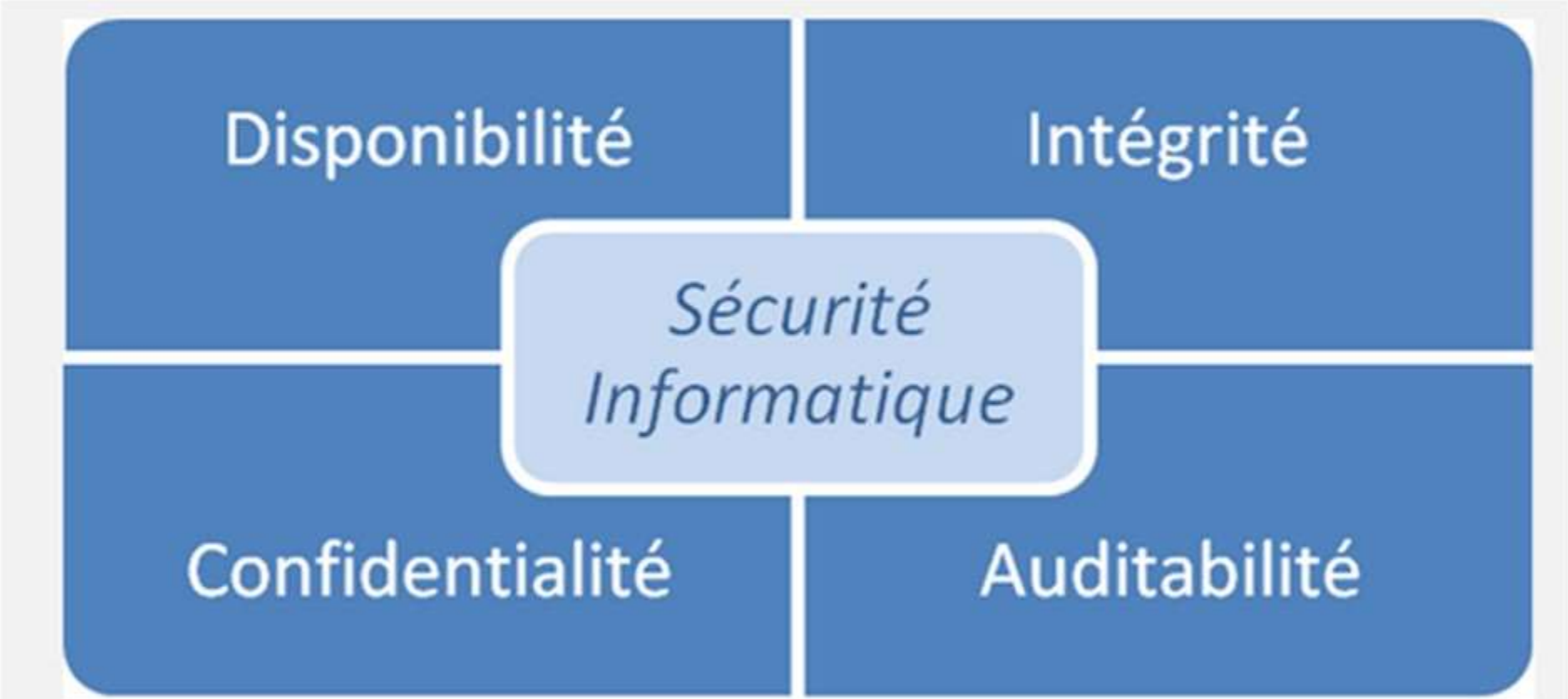



# La résilience – Objectifs continuité & réactivité aux incidents

La résilience est la capacité d'un système à maintenir ou à rétablir un niveau de fonctionnement acceptable malgré des perturbations ou des défaillances (Pinel, 2009)



# Quelques définitions



# Disponibilité

- **Garantir l'accès aux ressources au moment voulu aux personnes habilitées à accéder à ces ressources**

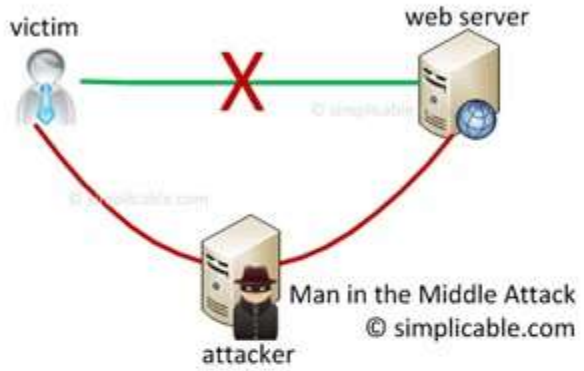
- **Menaces actuelles** :
  - Déni de service distribué
  - Rançongiciel


- **Prévention et réaction**
  - Opérationnel :
    - Définir les besoins en continuité et les moyens pour l'assurer
    - Mettre en place les procédures et entrainer le personnel
    - Gérer les incidents et la crise
  - Technique
    - Outils de détection
    - Segmentation des réseaux
    - Sauvegardes éprouvées sur au moins 3 supports différents
    - Gérer la restauration en fonction des objectifs de continuité de services

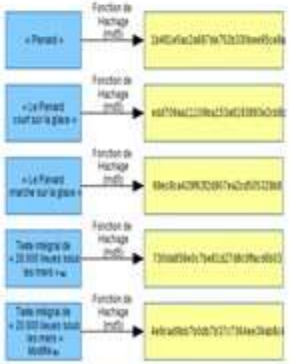
# Intégrité

- **Garantir que les données échangées ou stockées sont exactes et correctes**

- **Menaces actuelles**
  - Modification des données par attaque malicielle
  - Détournement des flux d'information (Man in the Middle)




- **Prévention et réaction**
  - Opérationnel : procédures de vérification pour assurer une traçabilité complète des données : gestion des accès, droits de lecture, d'écriture, de modification, diffusion sécurisée, stockage résilient
  - Technique :
    - Signature lors de la transmission de données
    - Chiffremnt des liaisons et des données
    - Vérification des données par des techniques d'empreinte des fichiers (hachage)



# Confidentialité

- Assurer la gestion des différents accès à l'information en fonction des besoins à en connaître (classification : publique, diffusion restreinte, confidentiel, secret)

- **Menaces actuelles :**
  - Accès aux données (messagerie, stockage , accès non autorisé du personnel) après attaque de hameçonnage ou infection virale du système d'information
  - Piratage des moyens de communication (wifi libre)


- **Prévention et réaction**
  - Opérationnel : Classification de l'information et Plan de gestion opérationnelle des accès (personnel, sous-traitant, stagiaires)
  - Technique :
    - Gestion des identités et des accès
    - Contrôle quotidien des logs

# Cyber continuité / Cyber hygiène / Cyber protection

- Vision de la sécurité est différente en fonction de son niveau décisionnel
  - **Stratégique** : CxO culture métier – rentabilité – services - coûts -bénéfices – risques
  - **Opérationnel** : mise en œuvre ( services applications automatisation)
  - **Utilisateurs** : utilisation travail / privé
  - **Technique** – Sécurisation du SI

Vers une résilience de l'entreprise – un projet collectif


Risques numériques
MRT de sécurisation
Sécurisation des architectures SI et ICS
Datacenter et Cloud Computing
RGPD

# La MRT : la sécurité de bout-en-bout

# ISO 27002 – Evaluation de la maturité de l'entreprise face aux risques

| Contrôles Applicables | Non applic. | ISO 27002 11 domaines, 39 objectifs, 133 contrôles | Cote | % | Notes ciblées | % | Cote ISO 27002 | Note ciblée ISO 27002 |
|---|---|---|---|---|---|---|---|---|
| 2 | 0 | 5.Politique de sécurité | 0.0 | 0.00% | | 0.00% | | |
| 11 | 0 | 6.Organisation de la sécurité | 0.0 | 0.00% | | 0.00% | | |
| 5 | 0 | 7.Gestion des biens | 0.0 | 0.00% | | 0.00% | | |
| 9 | 0 | 8.Sécurité liée aux RH | 0.0 | 0.00% | | 0.00% | | |
| 13 | 0 | 9.Sécurité physique et environnementale | 0.0 | 0.00% | | 0.00% | | |
| 32 | 0 | 10.Gestion de l'exploitation et des télécommunications | 0.0 | 0.00% | | 0.00% | | |
| 25 | 0 | 11.Contrôle d'accès | 0.0 | 0.00% | | 0.00% | | |
| 16 | 0 | 12.Acquisition, dévelop. et maintenance des systèmes | 0.0 | 0.00% | | 0.00% | | |
| 5 | 0 | 13.Gestion des incidents | 0.0 | 0.00% | | 0.00% | | |
| 5 | 0 | 14.Gestion du plan de continuité de l'activité | 0.0 | 0.00% | | 0.00% | | |
| 10 | 0 | 15.Conformité | 0.0 | 0.00% | | 0.00% | | |
| 133 | 0 | | | | | | 0.00% | 0.00% |

**Sécurité conforme aux meilleures pratiques (entre 2.0 et 4.0)**

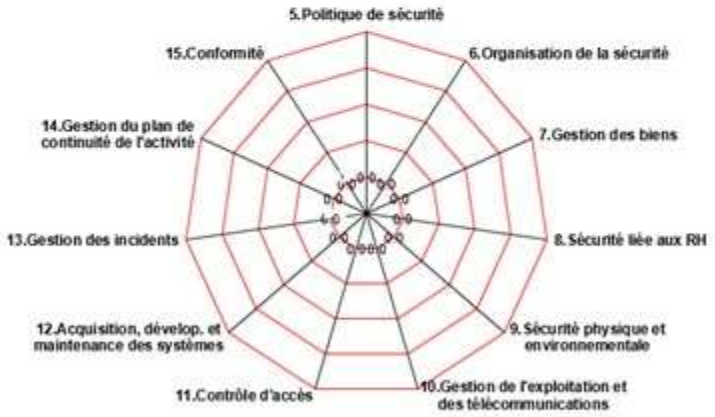
**ÉTAT DE LA SÉCURITÉ**

Audit de conformité réalisé par : _____

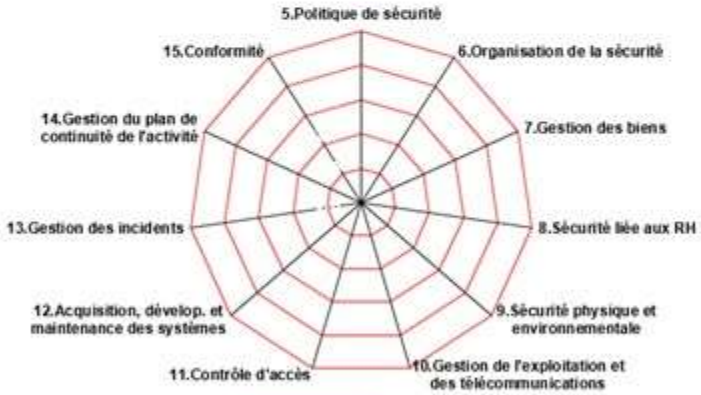
Date: _____

Note:

Portrait actuel




Portrait cible




L'actuel
Cible

Domaine 1 (Global) | Domaine 5 | Domaine 6 | Domaine 7 | Domaine 8 | Domaine 9 | Domaine 10 | Domaine 11 | Domaine 12 | Domaine 13 | Domaine 14 | Domaine 15

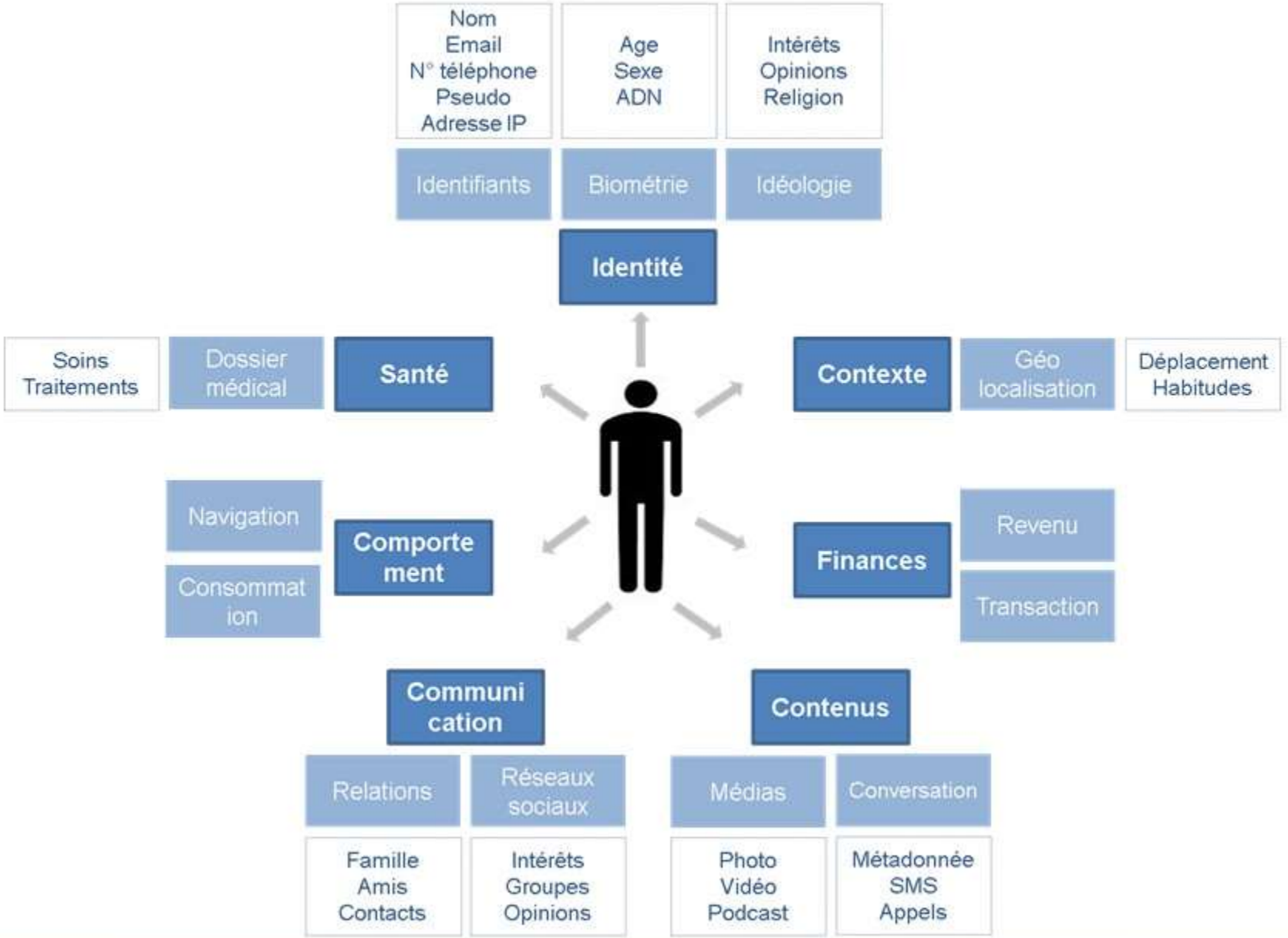
# Vision opérationnelle : MRT (Méthode de Raisonnement Tactique)

# Les biens essentiels

# Données et processus sensibles dans une entreprises


- **Production :** Données / processus relatifs aux secrets industriels, aux données de commande , aux données logistiques, aux services en ligne
- **Finance** : Données / processus relatifs aux investissements, à la facturation, au paiement
- **Ressources Humaines** : Données / processus relatifs à la gestion des données personnelles des employés
- **Vente – Marketing – Communication** : Données / processus relatifs aux clients, aux contrats, à la grille des prix

# Les données à caractère personnel –RGPD



# Cycle de gestion des données – INDISPENSABLE


- **Production de données**
  - ✓ Multiples formats
  - ✓ Différentes obligations légales de conservation
  - ✓ Différents niveaux de confidentialités

- **Exploitation**
  - ✓ Différents droits à en connaître
  - ✓ Différentes obligations légales

# Archivage – Durée de conservation légale

| Type de document | Conservation |
|---|---|
| Contrat papier | 5 ans |
| Contrat par voie électronique | 10 ans |
| Document bancaire | 5 ans |
| Livre & registre comptable | 5 ans |
| Bons de commande, livraison, factures | 10 ans |
| Impôts sur revenu société | 6 ans |
| Contrats de travai l, salaires, primes | 5 ans |

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

mon.
Service-Public.fr
Le compte personnel des démarches en ligne

Vosdroits.service-public.fr


# Evaluer les menaces et les risques

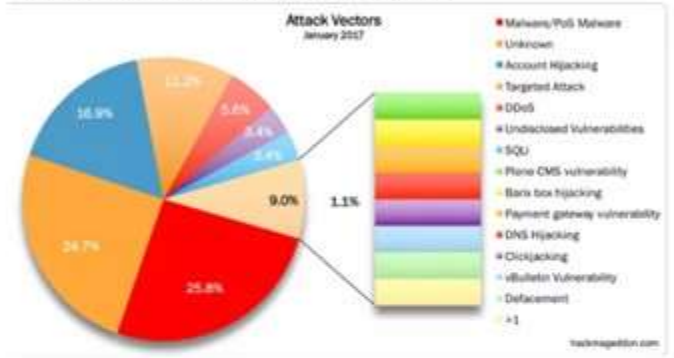
# Les menaces sur vos activités

Séisme
Grèves
Panne logicielle
Coupure informatique
Inondation
Panne matérielle
Panne électrique
Défaillance de prestataires
Incendie
...



# Prise d'empreinte de votre entreprise (menace culturelle - opérationnelle)

Evolution des cyber-menaces





**Ingénierie sociale**

References

- www.entreprises.com
- Personnel
- Fournisseurs
- Environnements
- Logiciels & Documentation

**Ingénierie technique**

# Exercice de prise d'empreinte de votre entreprise

## Ingénierie sociale

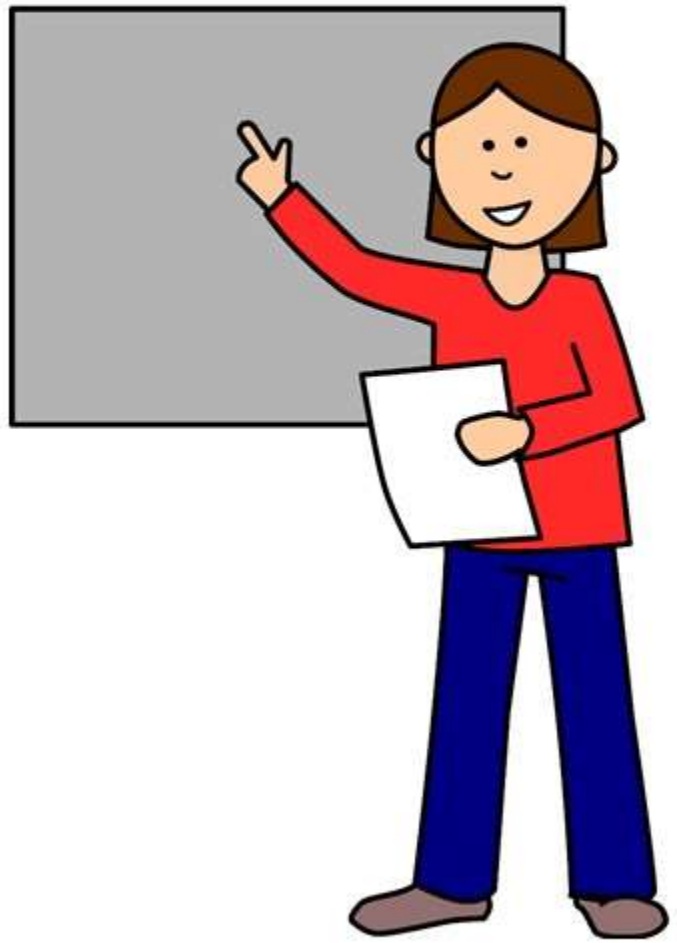

- www.entreprises.com
- Personnel
- Fournisseurs
- Environnements
- Logiciels & Documentation

## Ingénierie technique

# Outils de recherche

# Outil de synthèse: Freemind

# Restitution par groupes de travail



# Déterminer les autres menaces hormis les catastrophes naturelles

Origine des  menaces


- **D'origine internes** : employés, partenaires, sous-traitants => compromission de vos données & de vos systèmes NTIC par accident, négligences ou volontairement
- **Criminelles** : vols d'information permettant des gains financiers ou ayant pour but de paralyser votre activité par plaisir
- **Compétiteurs** : vols d'information ou sabotage pour gains financiers
- **Etatiques** : paralysie OIV

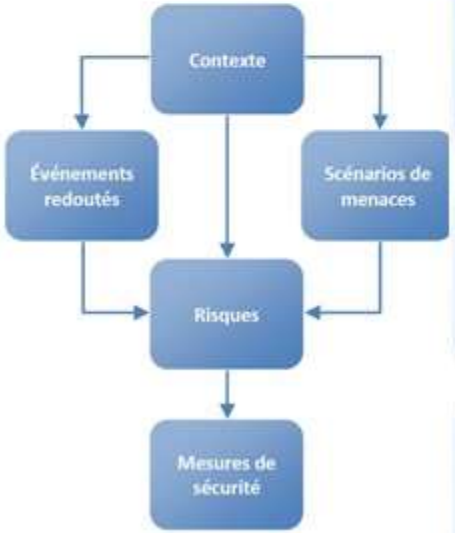
# Comment ces menaces se traduisent-elles?

## Formes de menaces


- **Vols ou accès non autorisés** : stations de travail, portables, tablettes, téléphones intelligents
- **Prise de contrôle à distance** de votre système IT ou système de production
- **Atteinte à la confidentialité, intégrité, disponibilité** de vos données via un de vos fournisseur , hébergeurs de données ou employés
- **Divulgation de vos données stratégiques ou sensibles** par recoupement des données publiées par vos employés sur les réseaux sociaux, forums, wiki etc.

# Analyse de risque – Méthode EBIOS

https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/




**Contexte**
- Pourquoi et comment va-t-on gérer les risques ?
- Quel est le sujet de l'étude ?

**Evénements redoutés**
- Quels sont tous les événements craints ?
- Quels seraient les plus graves ?

**Scénarios de menaces**
- Quels sont tous les scénarios possibles ?
- Quels sont les plus vraisemblables ?

**Risques**
- Quelle est la cartographie des risques ?
- Comment choisit-on de les traiter ?

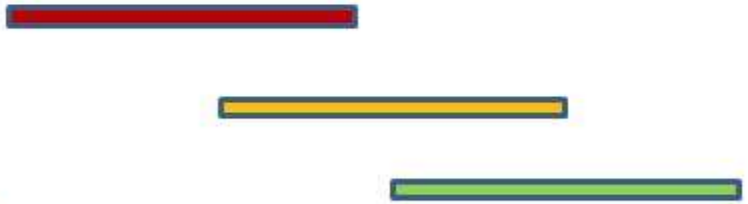
**Mesures de sécurité**
- Quelles mesures devrait-on appliquer ?
- Les risques résiduels sont-ils acceptables ?

# Déterminer les impacts (conséquences) sur mes activités

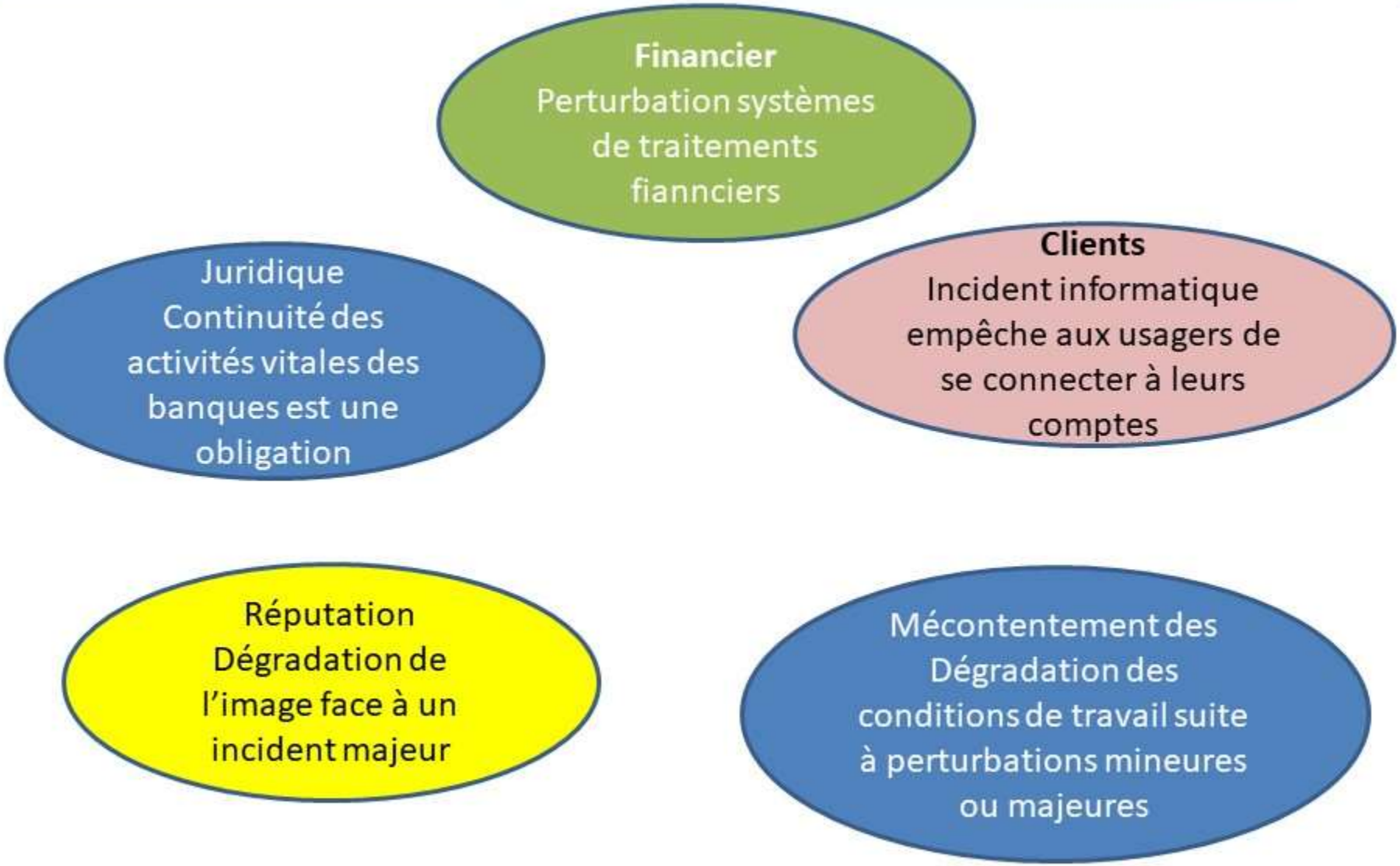
**Notion de criticité (gravité)** : si j'ai un problème dans un des domaines d'activités, **quelles** sont les conséquences pour mon entreprise?

3 niveaux de criticité

- Critique
- Important
- Négligeable



# Exemples d'impacts pour un établissement financier



# Cartographie des risques d'une entreprise

- **Risques stratégiques**
  - Liés au cyber espionnage, perte de notoriété, risques financiers
- **Risques opérationnels**
  - Risques naturels et environnementaux
  - Risques technologiques ou accidentels : indisponibilité Internet, défaillance d'un processus industriel, défaillance d'un système
  - Risques provoqués : malveillance, intrusion, actions de destruction ou de sabotage, menaces informatiques, vols d'informations sensibles ou de brevets
- **Risques de gouvernance**
  - Manque d'anticipation, absence de coordination dans la gestion d'incidents, fonction de pilotage déficiente
- **Risques de conformité**
  - Responsabilité civile et pénale, obligations de rendre compte aux autorités

# Identification des risques importants et critiques pour l'activité de l'entreprise

| Processus ou données | Composants fournissant le service (humain, IT HW ou SW, réseau, composant industriel) | Nature du risque probable (RETEX) | Durée maximale interruption acceptable DMIA | Impacts<br>• Important<br>• Critique | Priorités |
|---|---|---|---|---|---|
| Données bancaires fournisseurs | Comptable<br>Logiciel comptable | • Remplacement du comptable<br>• Changement des données fournisseurs (malversation)<br>• Logiciel comptable HS<br>• Inondation : destruction HW SW | | • Important | P1 |
| Design Processus industriel | Equipe projet<br>Plateforme collaborative<br>Emails<br>Transit données via Internet | • Remplacement membre équipe<br>• Vol ou destruction de données (piratage interne ou externe) | | Critique | P0 |

| Menaces |
| --- |
| Environnement : feu, inondation, tremblement de terre |
| Ressources : panne matérielle, arrêt approvisionnement, employés |
| Hacker – criminel – employé mécontent |

| Vulnérabilités |
| --- |
| Vulnérabilités dans les protections de sécurité : défacement site web, rançongiciel, déni de service |

| Probabilités pour avoir un cyber incident dangereux |
| --- |
| Occurrence basée sur votre historique ou statistiques |
| Opportunités pour les attaquants : capacité et intention |

| Impacts – dangers potentiels pour l'entreprise |
| --- |
| Vol ou publication d'informations sensibles ou critiques |
| Modification des données ou de vos systèmes |
| Perte d'information ou des disponibilité des systèmes |

**RISQUES**

# Travail par groupe – Analyse des risques face aux menaces et mesures de prévention

**Attaque Phishing /RANSOMWARE / DDOS / man in the middle**

| Ressources humaines | Données / processus | Applications / services | Logiciels | Infrastructure réseau |
|---|---|---|---|---|

**Impacts possibles**

| Ressources humaines | Données/processus | Applications / services | Logiciels | Infrastructure réseau |
|---|---|---|---|---|

**Analyse des risques et solutions de prévention**

?

# Quel plan de prévention face à ces scénarios ?

Direction

?

Responsable système information / divisions opérationnelles

?

Employés / Clients

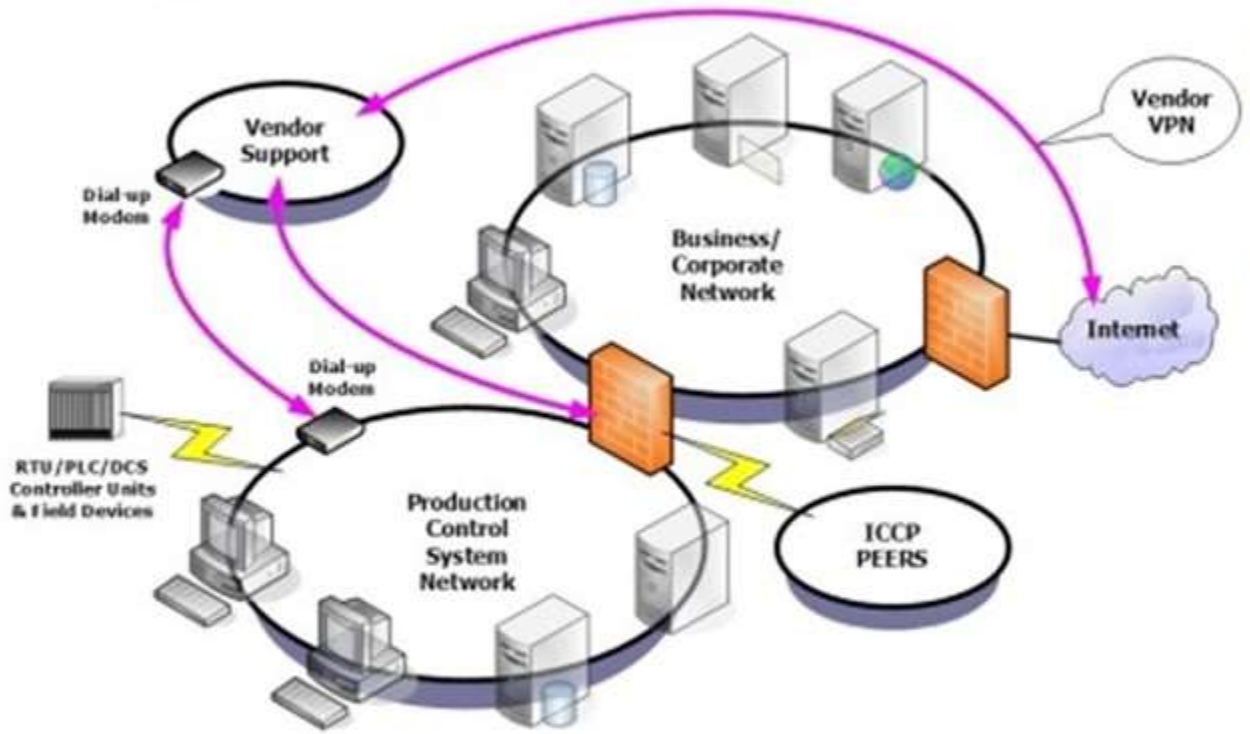
?

Infrastructure / IT

?

# Gestion des accès distants – quelles mesures de prévention ?

**Vendor Support**

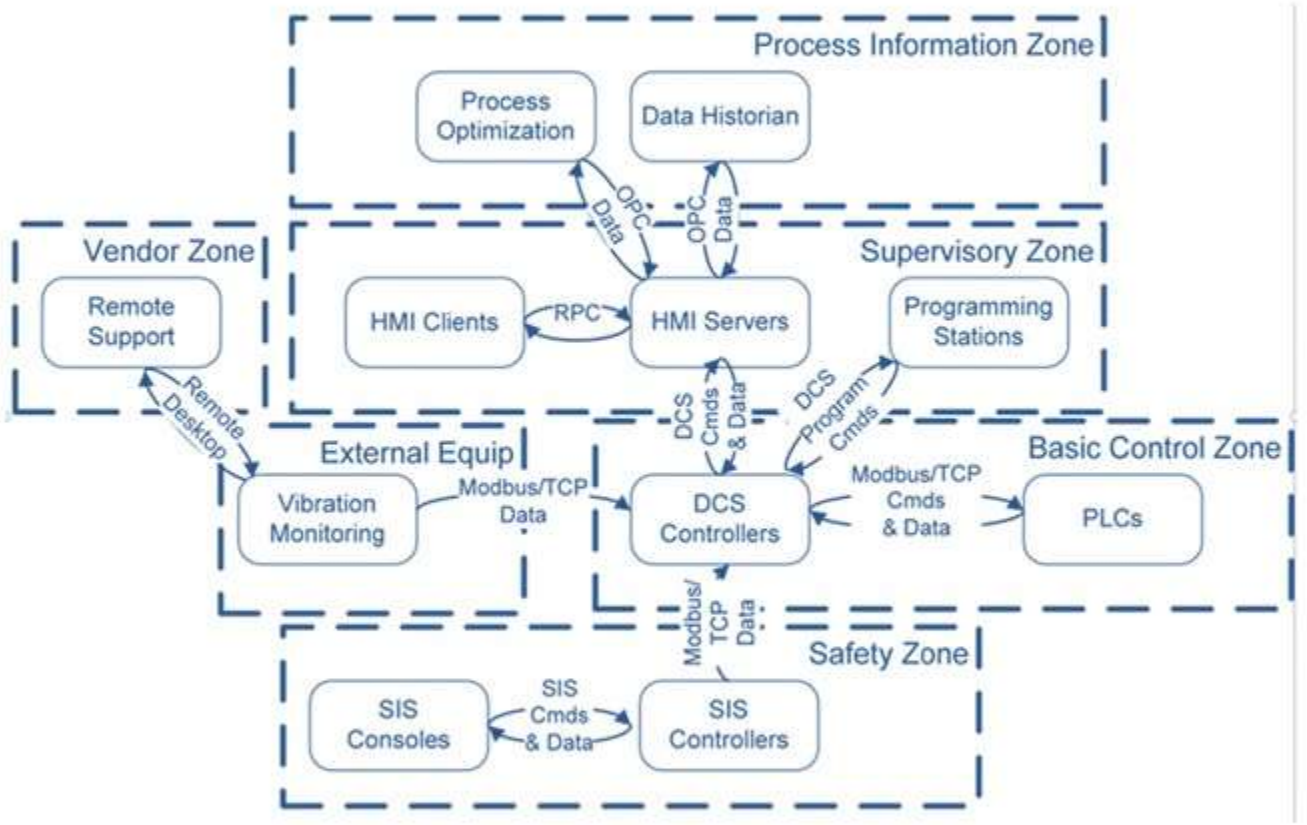



large version

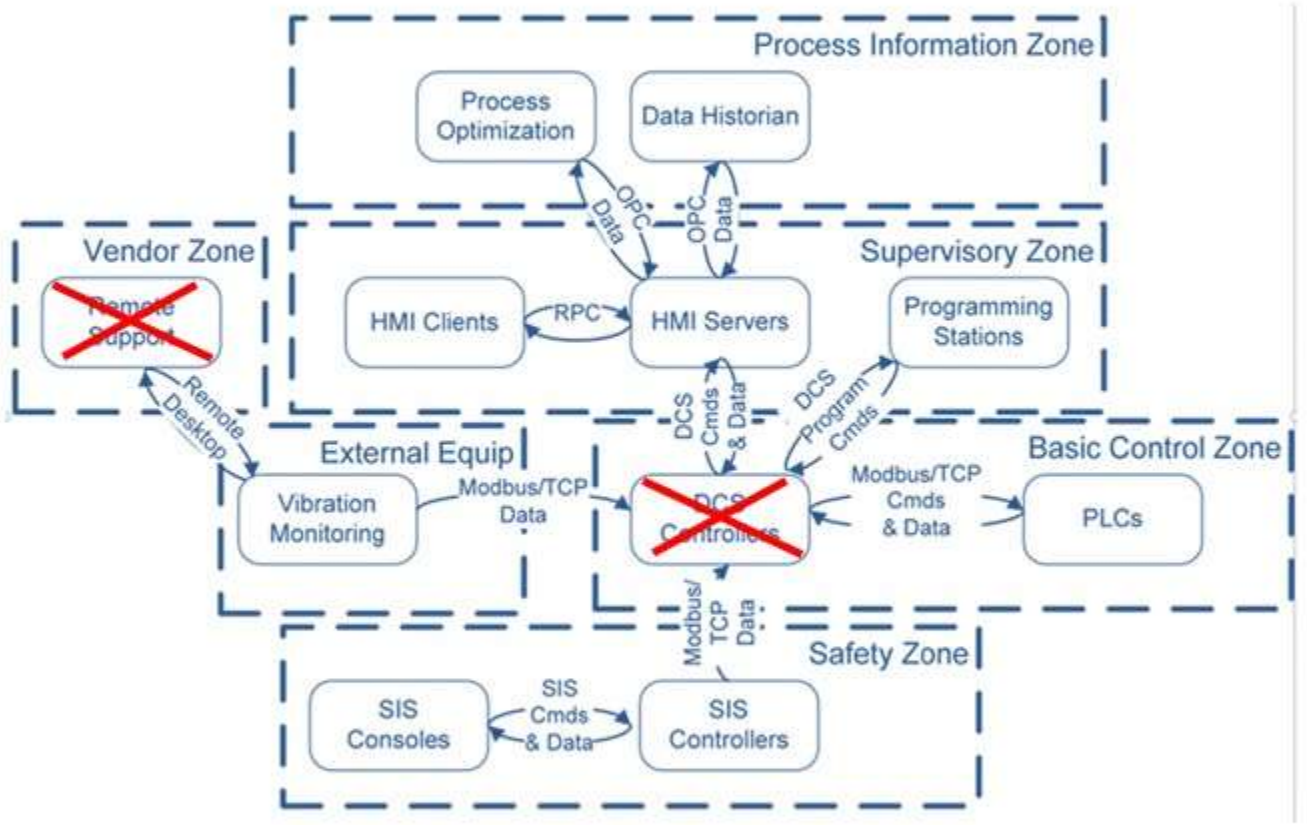
**Figure 8: Vendor support**

- Accès à distance multiples
- Protocoles multiples
- Acteurs multiples

# Diagramme des flux complet pour chaque zone



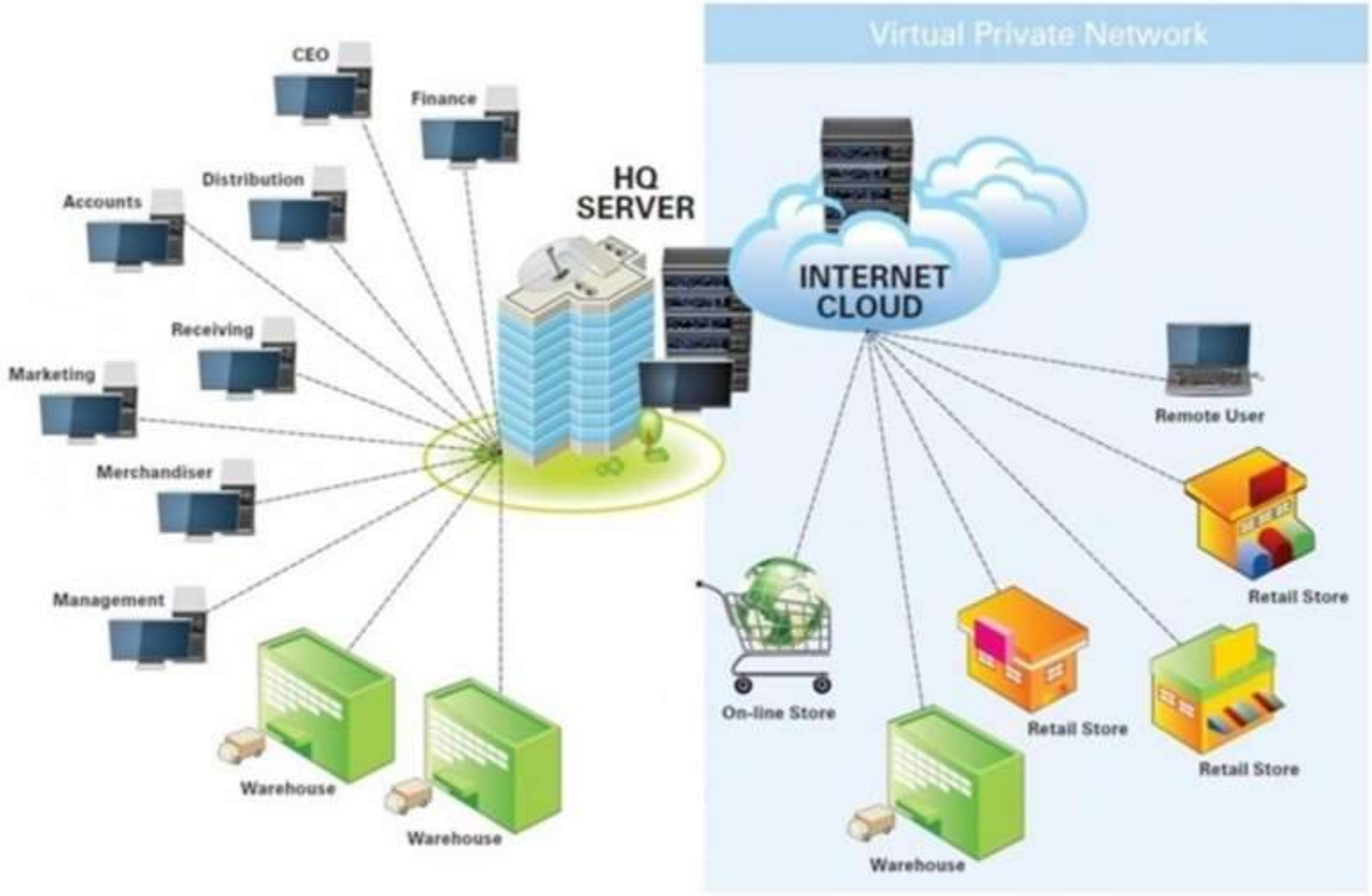
# Visualisation des risques (défaillance ou attaque cyber)



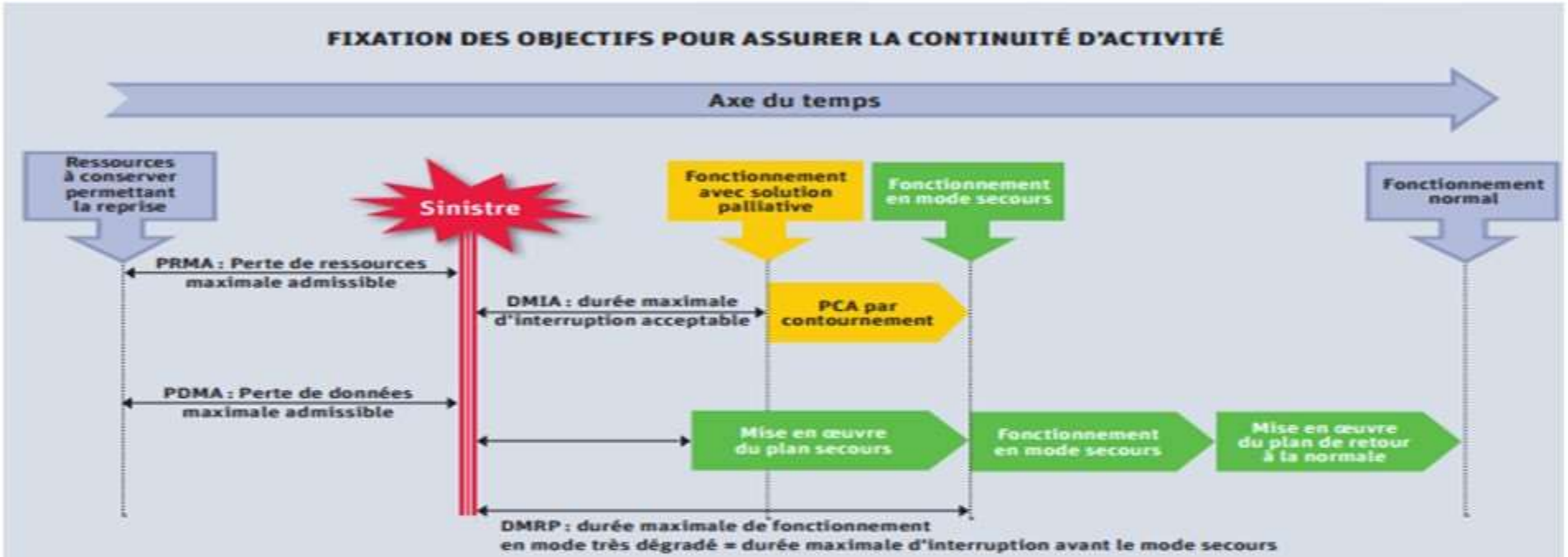

# Les mesures de protection : politique de sécurité, plan de continuité, plan de reprise d'activités, gestion d'incidents

IT-OPSLINK


INDISPONIBLE!


Virtual Private Network
CEO
Finance
Distribution
Accounts
HQ
SERVER
Receiving
Marketing
Merchandiser
Management
Warehouse
Warehouse
INTERNET
CLOUD
Remote User
Retail Store
On-line Store
Retail Store
Retail Store
Warehouse

# Besoins en continuité – pertes et durées maximales admissibles




PDMA mesure le temps maximum acceptable durant lequel les données sont perdues, car elles ne peuvent pas être reconstituées ; il est nécessaire de recourir aux dernières données sauvegardées.

DMIA mesure la durée d'interruption de fonctionnement du processus au-delà duquel les conséquences deviennent intolérables.

DMRP (délai maximum de reprise technique prévu) mesure la durée d'interruption de fonctionnement des parties techniques du processus avant la reprise en mode secours. Cela correspond à la durée maximale de fonctionnement acceptable en mode très dégradé.

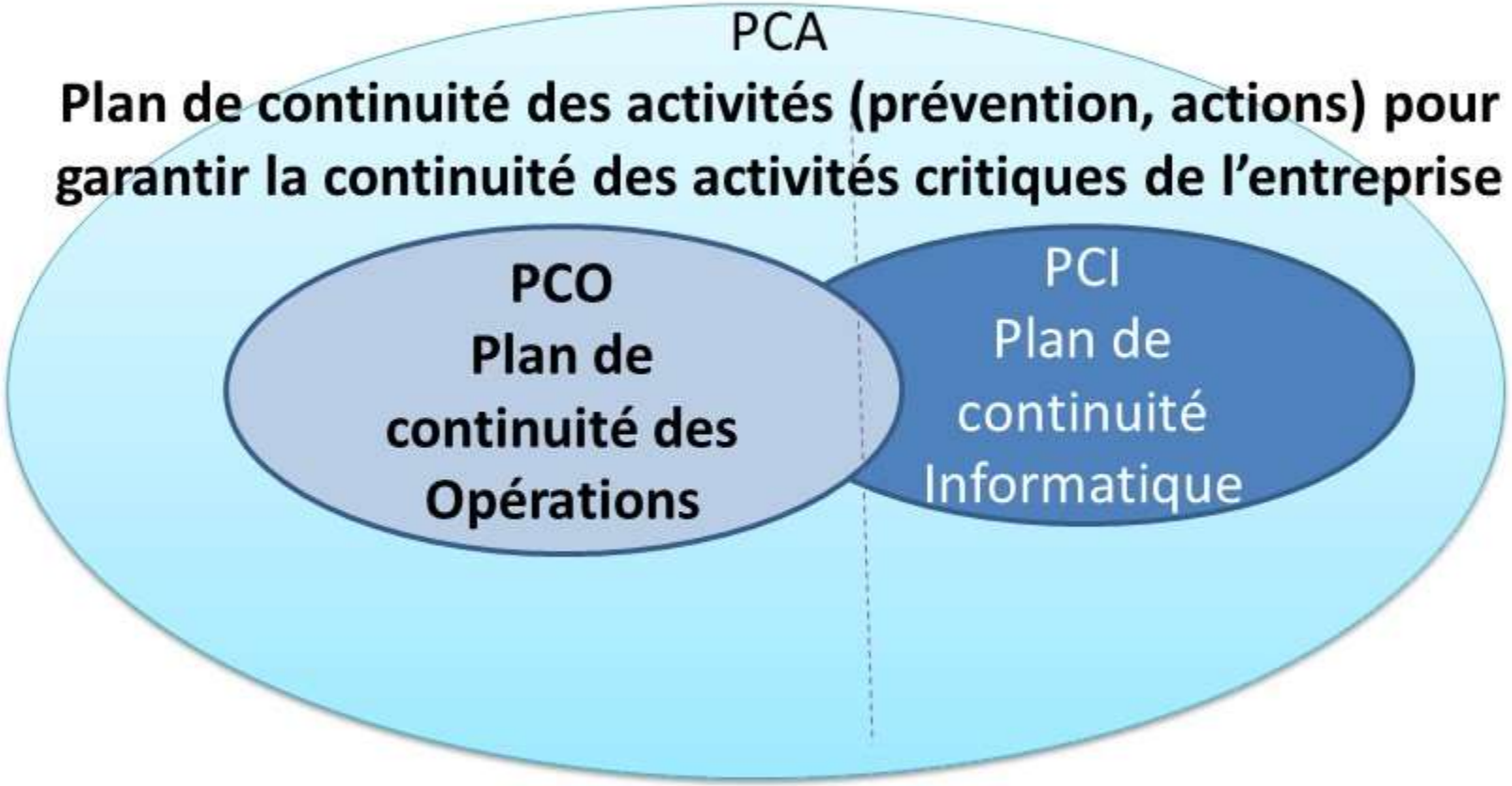
# DIMA , PDMA , DMRP : 3 critères essentiels

DMIA : Délai Maximal Admissible , durée maximale d'interruption d'une ressource que peuvent tolérer les utilisateurs de cette ressource

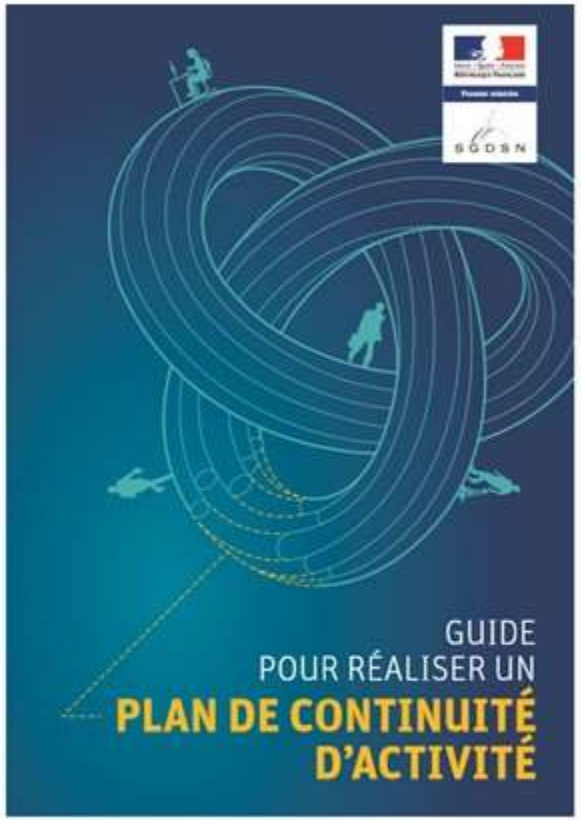
PDMA : Perte de données Maximale Admissible fonction de la politique et de la fréquence de sauvegarde des données


DMRP : Durée maximale en mode de fonctionnement très dégradé avant la mse en œuvre du plan de secours

# Définitions PCA, PCO , PCI



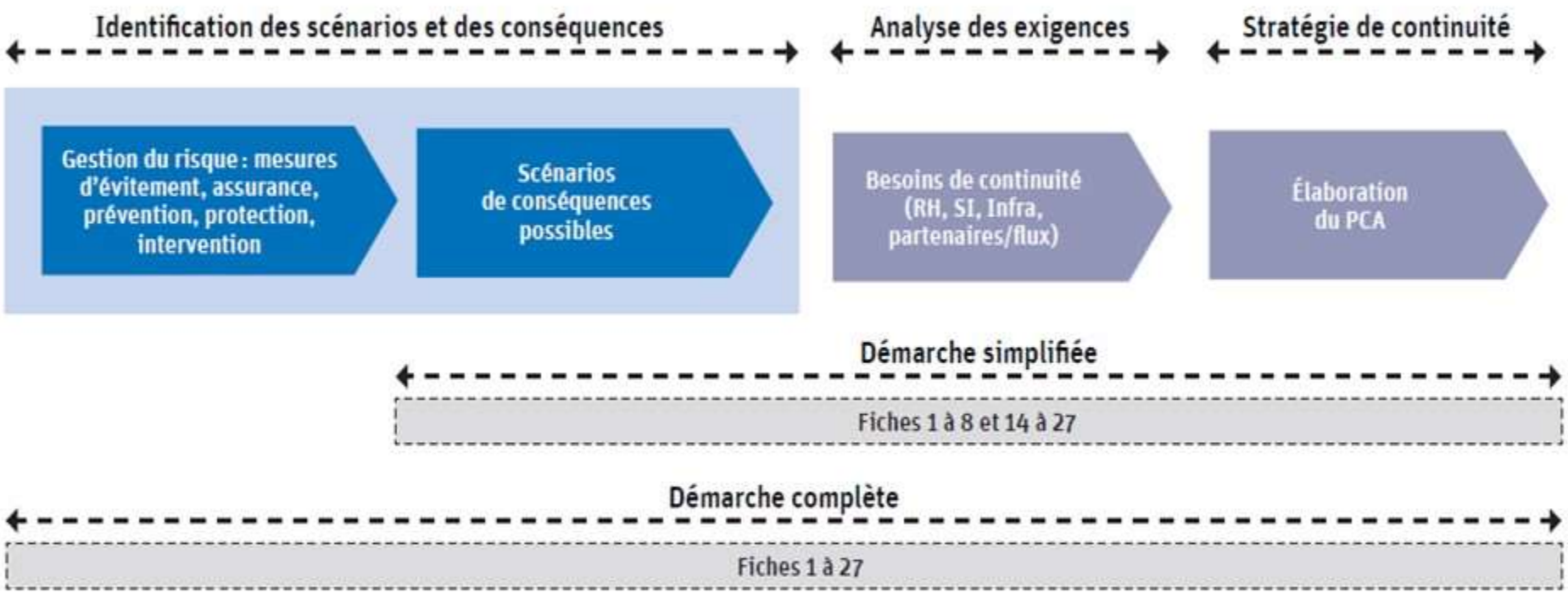
# PLAN DE CONTINUITE D'ACTIVITE




http://www.sgdsn.gouv.fr/IMG/pdf/Guide_PCA_SGDSN_110613_normal.pdf

*Contient ,en particulier, des fiches pratiques permettant l'élaboration d'un PCA.*

## DIFFÉRENTES APPROCHES POUR ÉLABORER UN PCA



# 3 LES FICHES PRATIQUES

# Besoins en continuité – DIMA /DPMA

| Processus ou données | Composants fournissant le service (humain, IT HW ou SW, réseau, composant industriel) | Nature du risque probable (RETEX) | Durée maximale interruption acceptable DMIA | Impacts<br>• Important<br>• Critique | Priorités |
|---|---|---|---|---|---|
| Données bancaires fournisseurs | Comptable<br>Logiciel comptable | • Remplacement du comptable<br>• Changement des données fournisseurs (malversation)<br>• Logiciel comptable HS<br>• Inondation : destruction HW SW | D0 : 1h<br>D1 : 4h<br>D2 : 1j<br>D3 : 2-4j | • Important | P1 |
| Design Processus industriel | Equipe projet<br>Plateforme collaborative<br>Emails<br>Transit données via Internet | • Remplacement membre équipe<br>• Vol ou destruction de données (piratage interne ou externe) | | Critique | P0 |

# Déterminer par groupes vos besoins en continuité sur vos processus critiques (4 au minimum)

| Processus ou données | Composants fournissant le service (humain, IT HW ou SW, réseau, composant industriel) | Nature du risque probable (RETEX) | Durée maximale interruption acceptable DMIA | Impacts<br>• Important<br>• Critique | Priorités |
|---|---|---|---|---|---|
| | | | D0 : 1h<br>D1 : 4h<br>D2 : 1j<br>D3 : 2-4j | | |
| | | | | | |

# Identifier les actions de continuité par niveau de responsabilité

Direction

?

Responsable système information / divisions opérationnelles

?

Employés / Clients

?

Infrastructure / IT

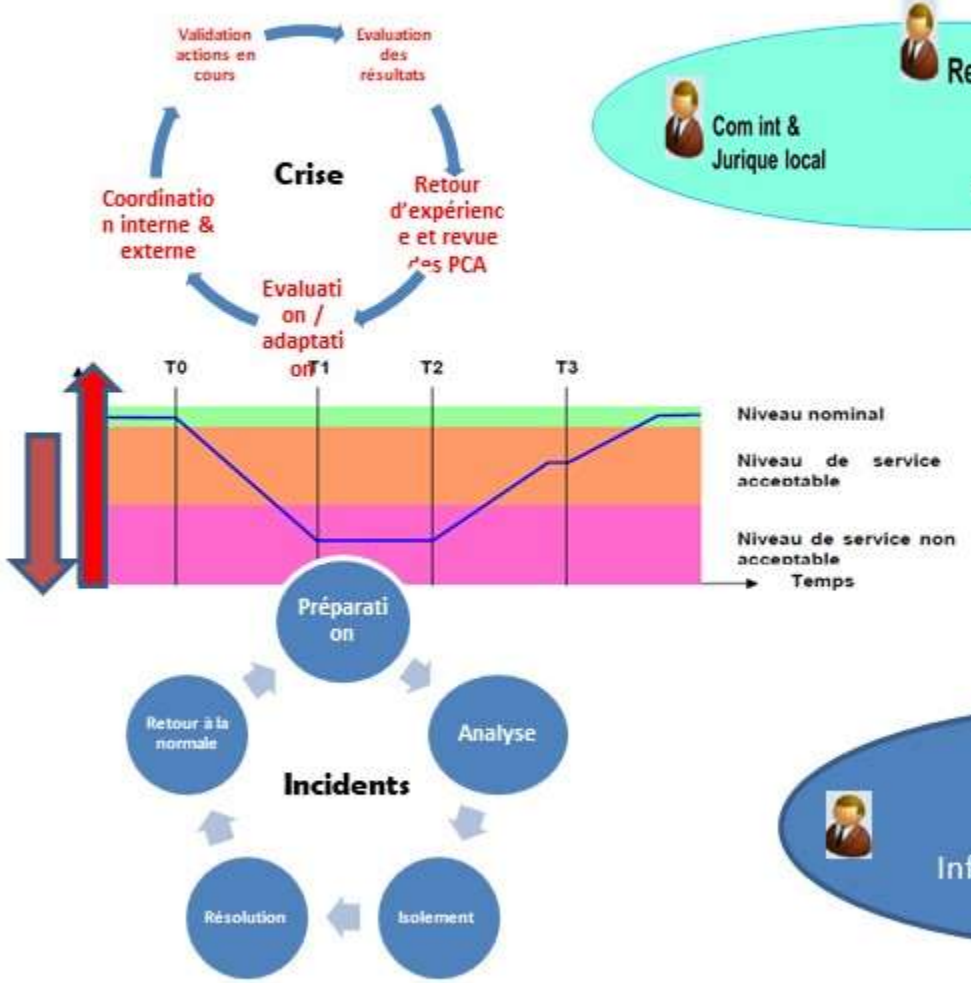
?

# PCI : Définir les solutions possibles de secours

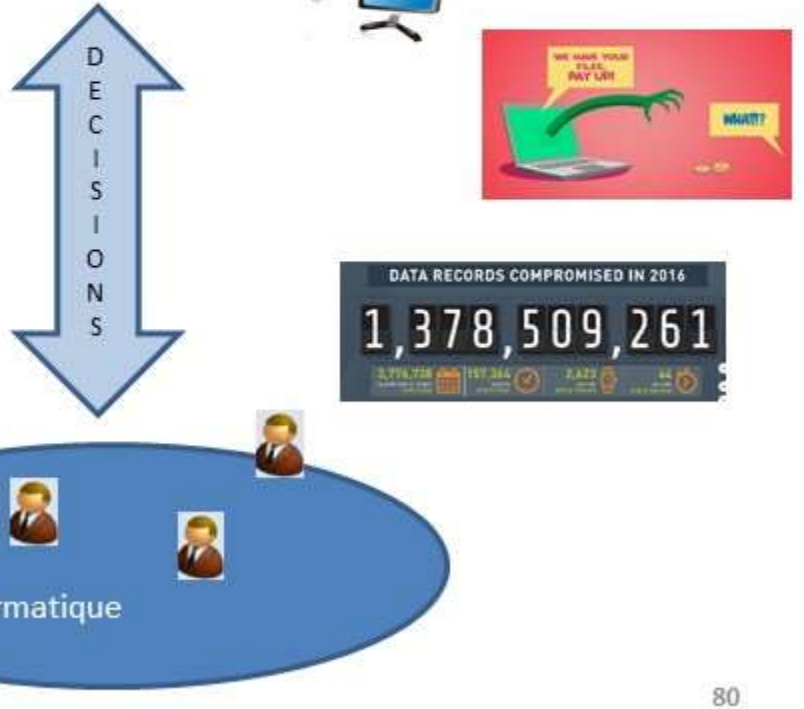
*Pour chaque couche technique SI, étude des solutions disponibles pour le secours.*

| | | | |
|---|---|---|---|
| **Applications** | **Matériel dédié** | **Actif** *(Clustering, partage de charge,…)* | **Activable** | **Dormant** |
| **Services d'infrastructure** *(annuaires, DNS, hyperviseur…)* | **Matériel mutualisé** | **Mutualisé interne** *(Pré-production, Intégration, Tests,…)* | **Mutualisé externe** *(chez un prestataire)* | |
| | **Matériel approvisionné** | **Commande lors du sinistre** | **Pré-contractualisation** | |
| **Stockage / Sauvegarde des données** | **Réplication baie** *Synchrone Asynchrone* | **Réplication serveurs** | **Sauvegarde** *Bandes magnétiques VTL* | |
| **Réseau** | **Réseau dupliqué** | **Réseau distincts** | **Réseau étendu** | **Réseau mixte** |
| **Hébergement** | **Nombre de sites** | **Hébergement interne ou externe** | **Résilience du datacenter** | |

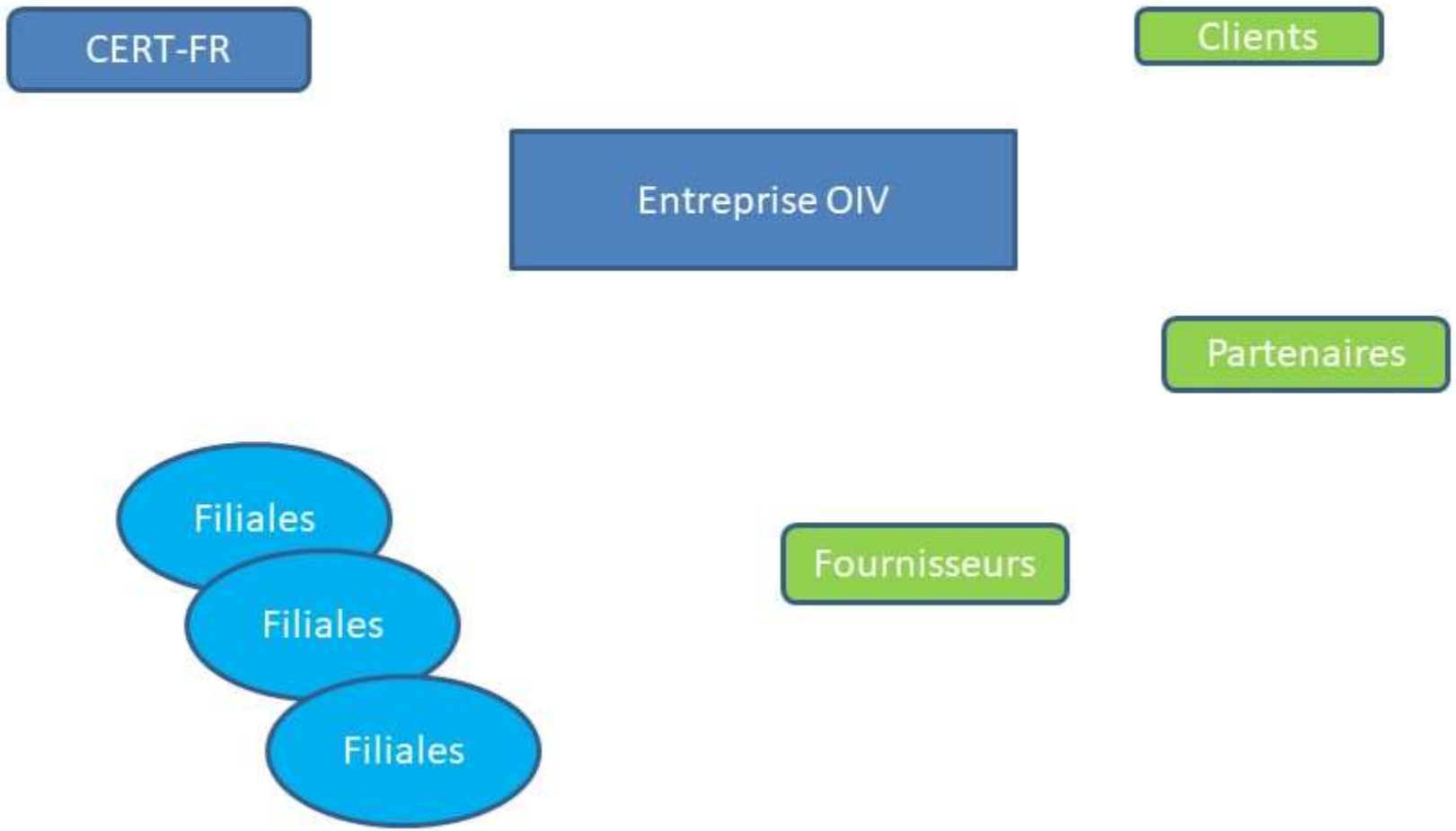
# PCO = gestion continuité – gestion des incidents



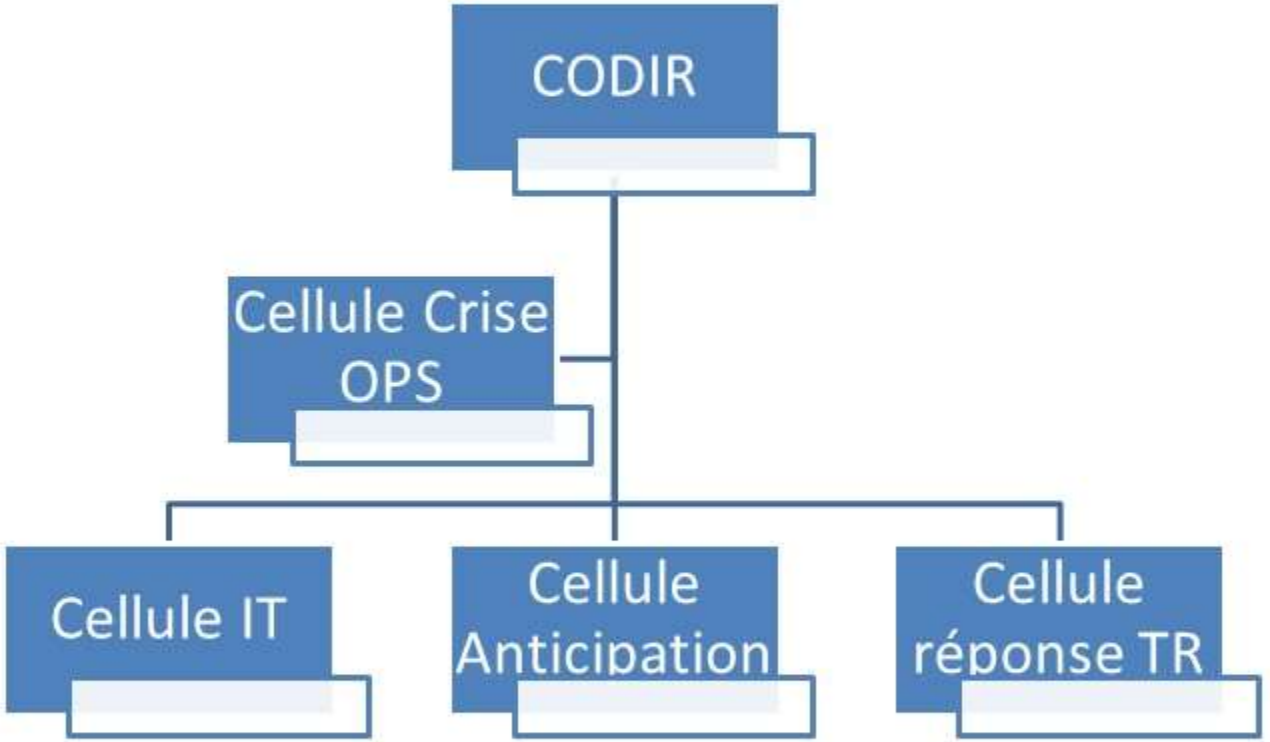




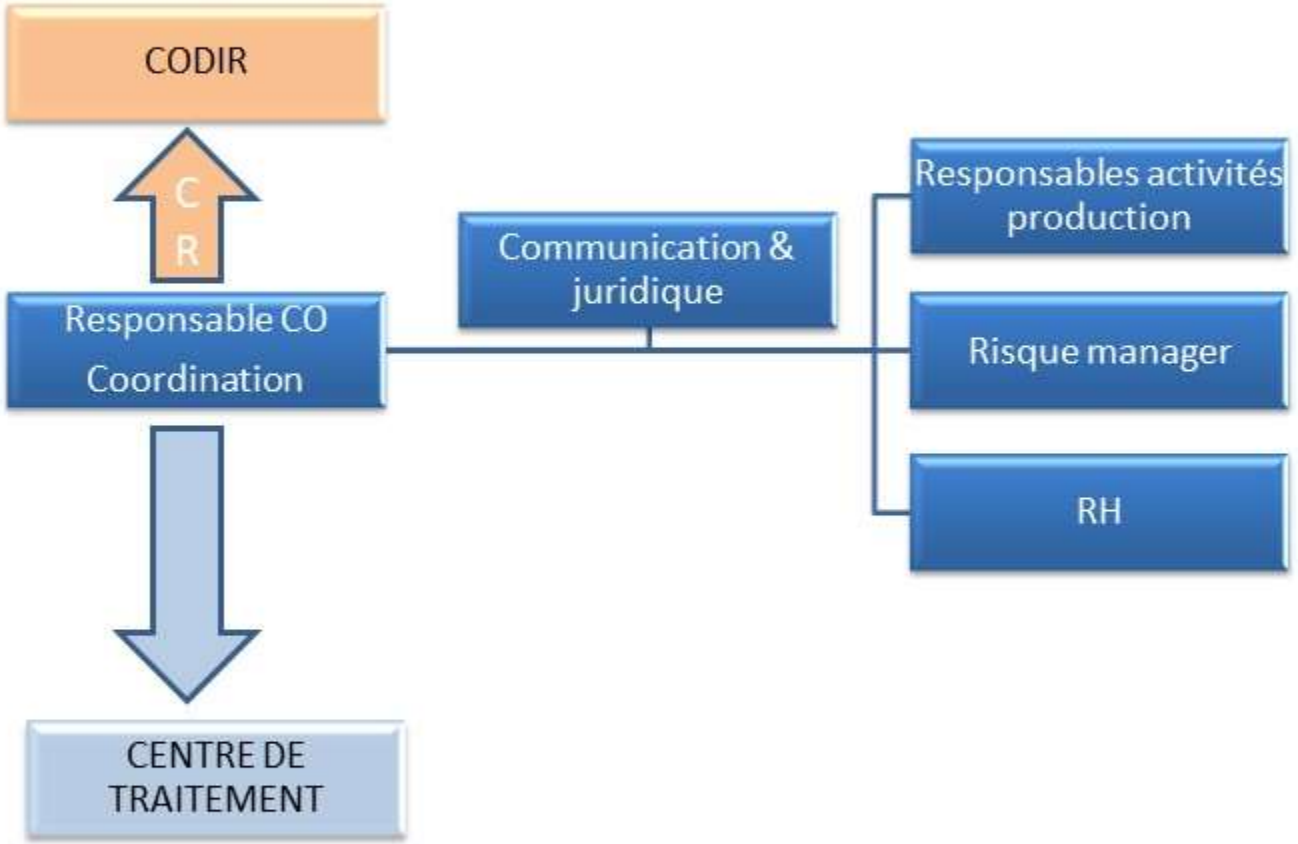

# Acteurs de gestion de crise



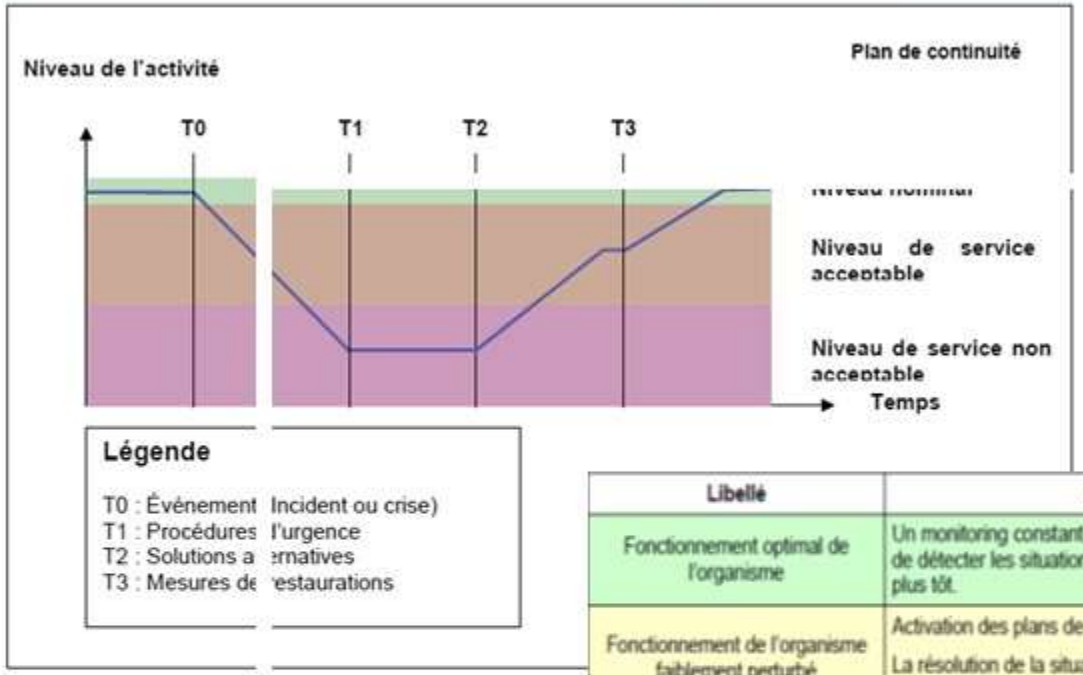
# Organisation cyber gestion (OIV)



# Cellule Crise OPS



# Procédure d'escalade




| Libellé | Activité | Atteinte | Impact |
|---|---|---|---|
| Fonctionnement optimal de l'organisme | Un monitoring constant de la situation est assuré afin de détecter les situations à risques et les alertes au plus tôt. | Aucune atteinte | Aucun impact |
| Fonctionnement de l'organisme faiblement perturbé | Activation des plans de continuité concernés<br>La résolution de la situation ne nécessite pas la mise à disposition de ressources exceptionnelles. | Pas d'interruption d'activités critiques. | Impact à court terme. |
| Fonctionnement de l'organisme fortement perturbé | Détection d'une crise ou d'une mauvaise gestion d'un incident.<br>Activation des plans de continuité concernés | Une ou plusieurs activités critiques sont menacées.<br>Interruption d'activités critiques possible. | Impact à moyen terme |
| Fonctionnement de l'organisme arrêté | Détection d'une crise ou d'un incident échappant au contrôle.<br>Activation des plans de continuité concernés (plan de crise)<br>Mise en place de la cellule de crise<br>Activation du site alternatif éventuel | Pérennité de l'organisme potentiellement remise en cause. | Impact à long terme. |

# Déroulement incident workflow - DDOS

**Monitoring:**
- Traffic réseau (netflow, IP FIX…)
- Processeur, RAM
- HDD
…

Comportant réseau inhabituel détecté

Zone affectée: coporate
Composant affecté: rout_corpo
Outil de détection: netflow

**Réseau surchargé.**
Disfonctionnement DNS?
Panne de routage pour cause de configuration?
Attaque DDOS sur routeur corporate

**Protocoles utilisés ?**
TCP
UDP

**Source**
Localisée
Non localisée

**Risque propagation?**
Oui
Non

**Impacts ?**

**Incident critique ?**

**Réponse court terme?**
- Blocage des adresses IP sources
- Blocage du type de traffic utilisé (UDP)

**Réponse Long terme?**
- Contacter opérateur pour élargir la bande passante
- Mesures légales

**Validation CTA blocage**
OK

**Résultat actions**
- Blocage du type de traffic utilisé (UDP) Résolu
- Contacter opérateur pour élargir la bande passante Résolu
- Mesures légales Résolu

***Rôles***
- *Employé alerte : Employé a*
- *Employé analyse : Employé d*
- *Employé réseau : Employé g*
- *Employé système: Employé i*

# Processus gestion  incident workflow - DDOS

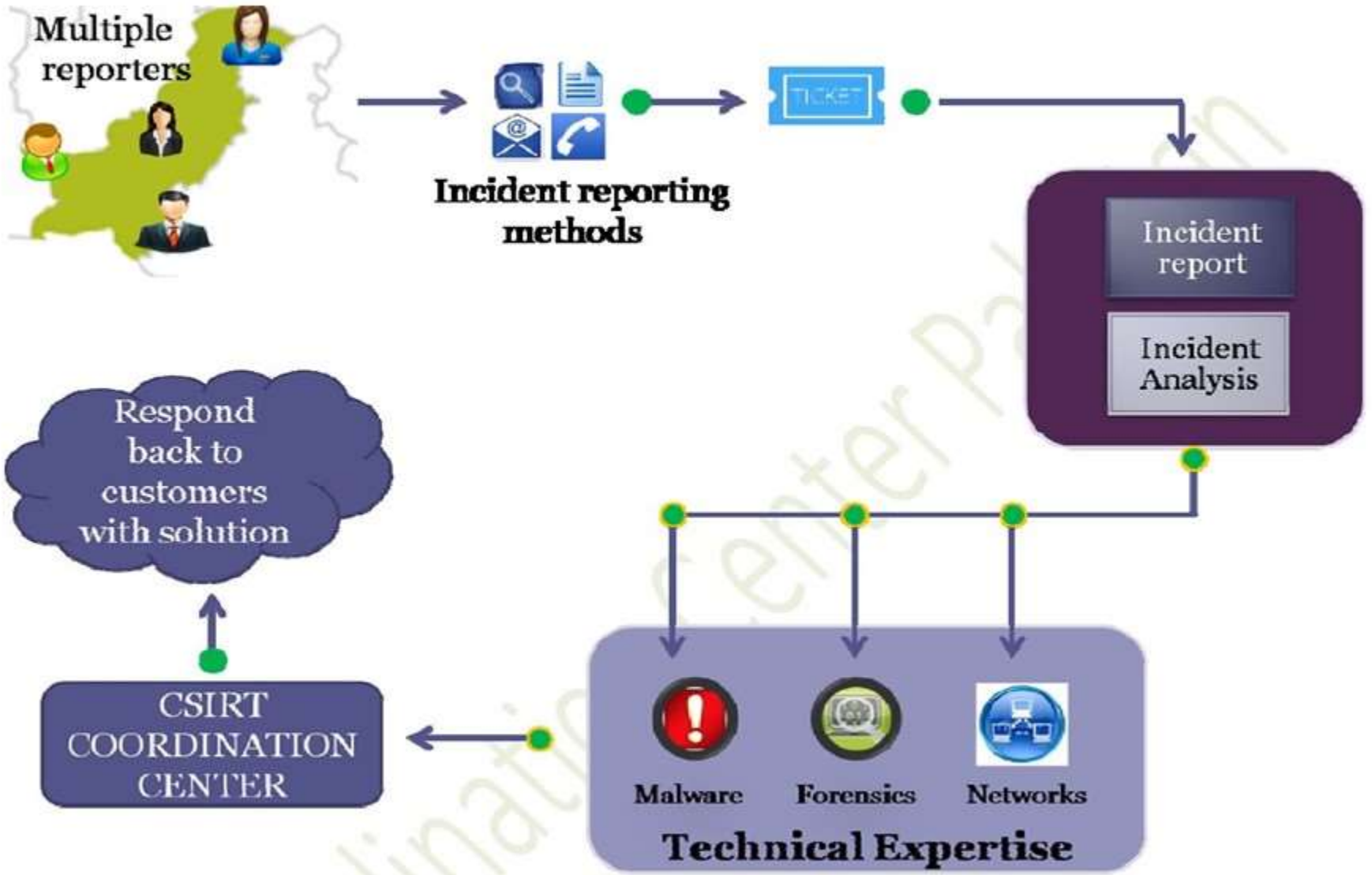
1. Remplissage fiche notification
2. Remplissage fiche notification détaillée
3. *Mise à jour du dashboard*
4. Remplissage fiche traitement avec planification & assignement des tâches à entreprendre
5. *Mise à jour du dashboard*
6. Remplissage de la fiche isolation pour demander validation au CTA
7. *Mise à jour du dashboard*
8. Remplissage du compte rendu de traitement suite aux actions prises
9. *Mise à jour du dashboard*


# RACI Gestion cyber incidents

| | TR | | | | | TA | | |
|---|---|---|---|---|---|---|---|---|
| | Alerte | Analyse | Admin. Sys. | Maintenance log. | Responsable CT TR | Manager risques & crise TA | Communication & juridique | Expertise technique |
| **Détection incident** | | | | | | | | |
| Détection incident système ou réseau | I | | R - A | | | | | |
| Détection incident applicatif | I | | | R - A | | | | |
| Remplir fiche notification incident<br>- A quelles heure et date l'incident est-il arrivé ?<br>- Quel moyen de détection a été utilisé ?<br>- Quelle est la (ou les) zone affectée ? | I | | R - A | R - A | | | | |
| **Qualification incident** | | | | | | | | |
| Qualification incident | R - A | C | | | I | | | |
| Pré-analyse incident<br>- Analyse des moyens à disposition (logs réseaux, firewalls, outils de détection d'intrusion, antirivus…)<br>- Quels sont les composants & systèmes affectés ?<br>- Quelle est la source de l'incident ? (attaque -> identité attaquant, erreur humaine…)<br>- Des outils indésirables sont-ils présents dans le système ?<br>- Il y a-t-il un risque de propagation de l'incident ? | R - A | C | | | I | | | |
| Pré-analyse impacts<br>- L'incident est-il une menace sérieuse pour l'organisation ? (activités, financiers, sécurité des employés, fuite de données stratégiques…)<br>- Quelle est la criticité de l'incident ? | R - A | C | | | I | | | |
| Remplir Fiche incident détaillée | R - A | | | | | | | |


| | TR | | | | | TA | | |
|---|---|---|---|---|---|---|---|---|
| | Alerte | Analyse | Admin. Sys. | Maintenance log. | Responsable CT TR | Manager risques & crise TA | Communication & juridique | Expertise technique |
| **Analyse de l'incident** | | | | | | | | |
| Enregistrement de l'incident dans l'incident log & tableau de bord | | R - A | | | I | | | |
| Analyse de l'incident<br>- Revoir les éléments présents dans la fiche d'incident détaillée<br>- A quel point les composants, voir les opérations, sont-ils affectés ?<br>- Ré-évaluer les impacts sur l'organisation (activités, financiers etc)<br>- Quelle est la priorité de l'incident ? Doit-on escalader immédiatement ? | I | R - A | C | C | I | | | |
| Planification d'une réponse adaptée<br>* Gestion court terme & isolation<br>- Peut-on contenir l'incident ?<br>- Dans quelles conditions peut on le contenir ? (coupure totale de la production, isolation d'une zone....)<br>- Identifier les actions pour contenir l'incident<br>- Doit-on prendre des actions urgentes pour contenir ou éradiquer le problème ?<br>* Eradication<br>- Comment supprimer l'incident ? (nettoyage, patching...)<br>- Peut-on supprimer l'incident sans couper la production ou une zone ?<br>- Doit-on faire une image du système affecté ? (légal, lesson learned...)<br>* Rétablissement<br>- Quand peut-on planifier la rétablissement du système affecté ?<br>- Comment rétablir le système ? (point de restauration/image...)<br>- Comment sera testé la restauration ? (critères, benchmark fonctionnement précédent vs nouveau...)<br>- Faut-il monitorer le système suite à la restauration ? (outils, durée...)<br><br>--> Assigner les ressources les plus adaptées pour chaque action identifiée | C | R - A | C | C | C | | | |
| Remplir Fiche Traitement Incident | I | R - A | I | I | C | | | |
| Valider le plan de traitement de l'incident | | C | | | R-A | | | |
| **Réponse à l'incident & Enregistrement** | | | | | | | | |
| Appliquer les mesures identifiées comme urgentes | I | I | R - A | R - A | I | | | |
| Appliquer les mesures techniques d'isolation | I | I | R - A | R - A | I | | | |
| Faire une image du système (ou zone) affecté & la stocker en lieu sur | I | I | R - A | R - A | I | | | |
| Appliquer les mesures techniques d'éradication | I | I | R - A | R - A | I | | | |


| | TR | | | | | TA | | |
|---|---|---|---|---|---|---|---|---|
| | Alerte | Analyse | Admin. Sys. | Maintenance log. | Responsable CT TR | Manager risques & crise TA | Communication & juridique | Expertise technique |
| **Retour à la normale** | | | | | | | | |
| Appliquer les mesures techniques de rétablissement | I | I | R - A | R - A | I | | | |
| Monitorer le bon fonctionnement de la production suite aux mesures | | | R - A | R - A | | | | |
| Remplir Compte Rendu de traitement d'incident | | | | | | | | |
| Mettre à jour le log d'incident & tableau de bord | | R - A | | | I | | | |
| Clotûrer l'incident | I | R - A | I | I | I | | | |
| Pilotage de l'équipe TR | C | C | C | C | R - A | | | |
| **Escalade vers CTA (en cas de blocage résolution, impacts critiques, besoin validation)** | | | | | | | | |
| Escalder vers l'équipe CTA avec la documentation nécessaire<br>- Joindre documentation pertinente (fiche traitement incident, CR échec traitement...) | | | | | R - A | C | | |
| Coordination de l'équipe CTA | | | | | | R - A | | |
| Pilotage d'une gestion de crise | | | | | | R - A | | |
| Coordination avec risques CO | | | | | | R - A | I | I |
| Analyse détaillée des impacts opérationnels<br>- quels sont les dangers potentiels pour l'entreprise ? (activité, humain, financiers etc)<br>- quels sont les impacts sur l'extérieur ? (public, clients, partenaires...) | | | | | | R - A | | |
| Communication locale & interne | | | | | | A | R | |
| Analyse des risques liés au légal | C | C | C | C | C | I | R - A | I |
| Analyse poussée de l'incident<br>- reprends l'analyse faite par le CTR en apportant une plus grand expertise<br>- peut faire appel à des externes / experts pour assistance spontanée | | | | | | C | | R - A |
| Identification de scénarios de résolution<br>- identification de scénarios techniques (isolation/éradication/rétablissement)<br>- analyse des impacts potentiels sur chaque scénario (activité, financier...) | | | | | | C | I | R - A |
| Validation du (nouveau) plan de traitement d'incident | | | | | C | R - A | I | I |
| Assignation du plan de traitement d'incident aux équipes techniques<br>- reprend ensuite le flux initial (Compte rendu traitement, mise à jour log incident...) | | | | | R - A | | | |


Multiple reporters
Incident reporting methods
TICKET
Incident report
Incident Analysis
Respond back to customers with solution
CSIRT COORDINATION CENTER
Malware
Forensics
Networks
Technical Expertise

# Base de connaissances

Attaques temps réel


PCA , ISO 2700x, MRT

Scénarios

Evaluations

Vidéos


Architectures systèmes d'information

Vulnérabilités - Risques

Formulaires de suivi


Fiches Pratiques de Résolution


Logiciels libres

# Mesures de prévention / protection

- Identification et classification des données et des doits à en connaître
- Plan de  Gestion des droits
- Services d'identification renforcés
- Plan de sauvegarde adapté aux besoins en continuité

# Information présente dans tous les secteurs

- Classification de l'information
  - Public
  - Restreinte
  - Confidentiel
- Contraintes réglementaires
  - CNIL
  - Durée de conservation

# Confidentialité – Intégrité – Disponibilité

- Confidentialité

Quelles sont les données sensibles (stratégiques pour l'entreprise et celles relevant de la Loi Informatique et Liberté) à protéger absolument et comment assurer leurs confidentialités?

- Intégrité

Quelles sont les informations dont il faut absolument protéger le contenu et quelles mesures dois-je prendre pour quelles ne soient pas modifiées accidentellement ou intentionnellement ?

- Disponibilité

Quels sont les besoins de disponibilité pour l'ensemble de mon information et comment assurer cette disponibilité?

# Classification des données et droit à en connaître

## Exercice – compléter le tableau et expliquer vos choix

| | Direction | RH | Compta | Production | Marketing | Vente |
|---|---|---|---|---|---|---|
| RH | | | | | | |
| Compta | | | | | | |
| Production | | | | | | |
| Marketing | | | | | | |
| Vente | | | | | | |
| Clientèle | | | | | | |
| Prestataires externes | | | | | | |

# Le plan accès management

- Identification de l'utilisateur
- Authentification de son accès au SI
- Habilitation aux différentes ressources du SI
- Implémentation d'outil et de service pour gérer les identités et habilitation
- Contrôle des procédures de gestion et de conformité des identités et des droits définis

# Identification

- **Objectif : fournir une identité de référence fiable pour une personne**

Une identité est composée d'un ensemble d'informations propres à une personne. Celle-ci peut posséder un ou plusieurs identifiants et à un ensemble de droits (attributs)

- La multiplication des sources d'information et la manière d'y accéder rendent la gestion plus difficile :
- BYOD
- Existence de différentes catégories d'utilisateurs (salarié, fournisseurs, etc)
- Hétérogénéité des applications et incompatibilité des structures de gestion d'accès ( annuaire LDAP, SGBD, fichier CSV etc)

La constitution d'un annuaire de référence est importante . La technologie dominante pour les référentiels d'identité est l'annuaire LDAP

# Authentification = « prouver qui l'on est »

- Objectif : garantir la légitimité d'un accès à une ressource basée sur des moyens différents :
  - « Ce que je connais » : Mot de passe, code PIN, passphrase
  - « Ce que je possède » : certificat numérique, token, authentificateur
  - « Ce que je suis » : empreinte digitale, iris, paume de la main

- Service commun d'authentification (SSO –Single Sign On) qui facilite l' 'authentification de l'utilisateur aux ressources du SI en propageant la permission d'accès obtenue ainsi que le niveau d'authentification (mot de passe, authentification forte) vers les ressources du SI.

- Pratiques les plus répandues : mot de passe ou authentification forte par cartes à puce

# Le chiffrement pour éviter l'exploitation des données à votre insu

Le chiffrement débute avec le code de César : substituer des lettres en les décalant

# Code César

Le code de César : Le ROT-13

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Deviennent

N O P Q R S T U V W X Y Z A B C D E F G H I J K L M

# Clef de chiffrement symétrique ou clef privée


**ENCRYPT**

```
  00110101  Plaintext
⊕ 11100011  Secret Key
-----------
= 11010110  Ciphertext
```

**DECRYPT**

```
  11010110  Ciphertext
⊕ 11100011  Secret Key
-----------
- 00110101  Plaintext
```

# Clef de chiffrement asymétrique ou clef publique


Protocole de chiffrement permettant à 2 parties sans connaissance de l'autre de partager une clef secrète

*Figure 15. Ron Rivest, Adi Shamir, and Leonard Adleman*

Chiffrement RSA

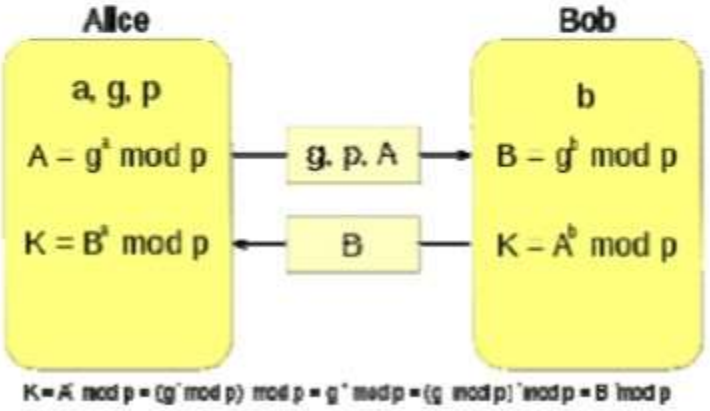



*Figure 14. Diffie-Hellman Key Exchange protocol.*

# Disponibilité : politique de sauvegarde 3--1

- Menaces : déni de service, ransomware , défaillance de matériel

- Politique des sauvegardes des données : politique des 3 -2 -1
  - 3 copies des fichiers importants (1 primaire, 2 back-ups)
    - Disque dur amovible + cloud public ou privé

- Etablir un plan de conservation des documents

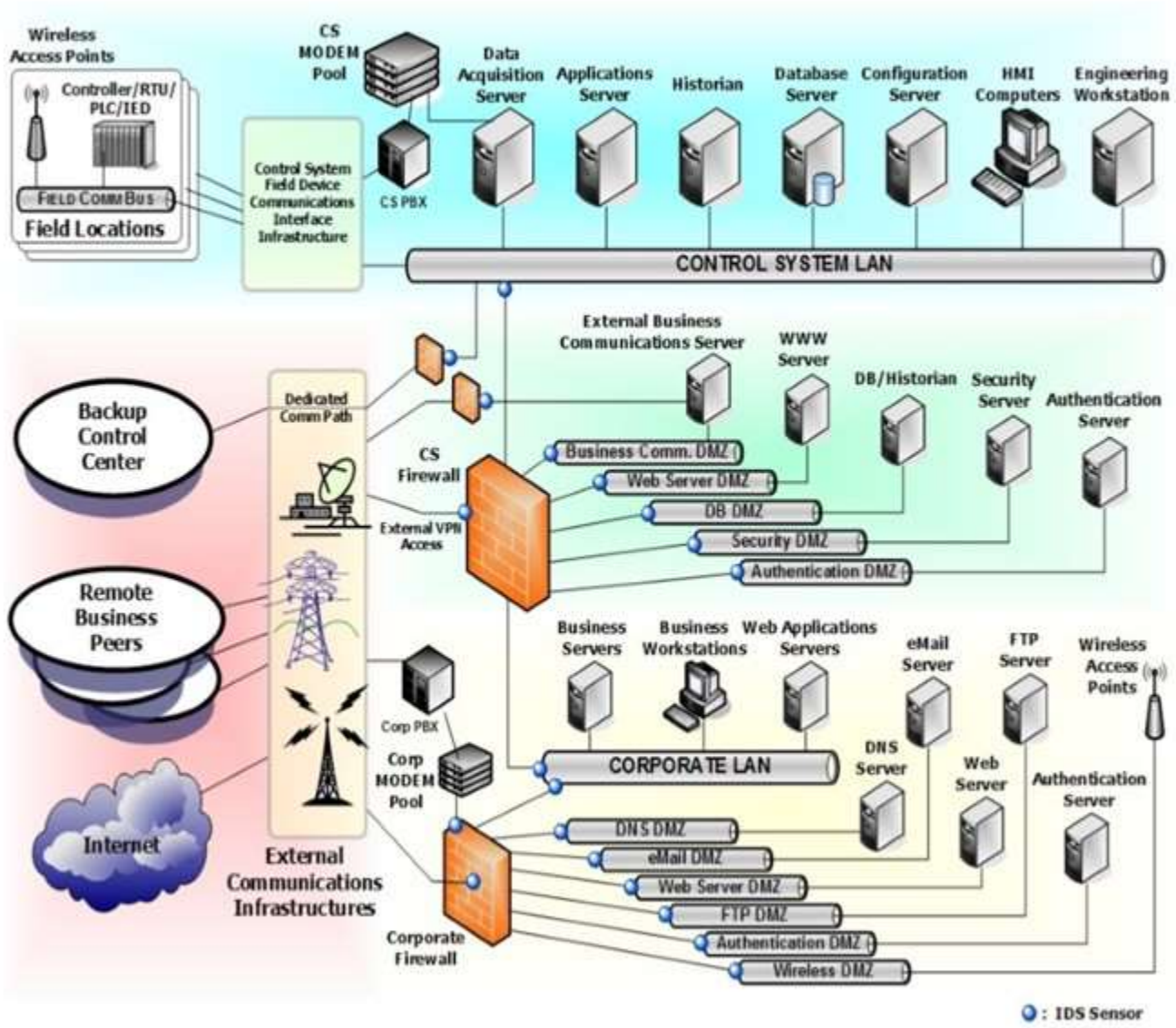
- Un fichier en plusieurs endroits mais avec des moyens d'accès différents : localement, serveur d'entreprise, cloud

# Elaboration de fiches de gestion technique d'incidents

| | |
|---|---|
| **Préparation** | **Objectifs : liste de contacts – procédures – collecte information**<br>• **Environnement applicatif du site web**<br>• **Site de secours prêt**<br>• **Procédure de redirection vers site de de secours**<br>• **Sauvegarde des logs** |
| **Identification** | **Objectifs : détection – analyse – communication**<br>• Réception & analyse notification interne / externe => fiches de suivi d'incident<br>• Vérification du défacement et détection de l'origine<br>• Etude du source code et vérification des bases de données |
| **Isolation** | **Objectifs : préservation des preuves et isolation de l'attaque**<br>• Copier complète bit-par-bit pour analyse ultérieure (forensics)<br>• Vérification du serveur et de ses connections<br>• Analyse de l'attaque et actions pour la contrer |
| **Résolution** | **Objectifs : actions pour contrer et éviter de futurs défacements**<br>• Mise en route serveur de secours – résolution nom de domaine (DNS)<br>• Mise à jours des composants % vulnérabilités détectées<br>• Changement des mots de passe et des niveaux d'accès |
| **Retour d'expérience** | **Objectifs : Documentation de l'incident, leçons apprises et mises à jour des plans de défense**<br>• Détection initiale<br>• Actions et délais<br>• Mesures d'amélioration<br>• Coût de l'incident |

DEFACEMENT SITE WEB

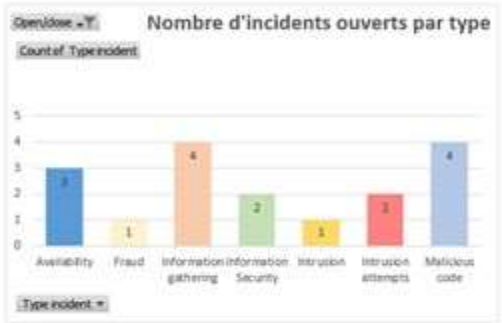
# Mesures techniques : cloisonnement

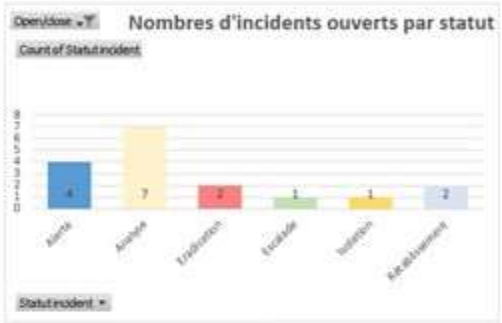


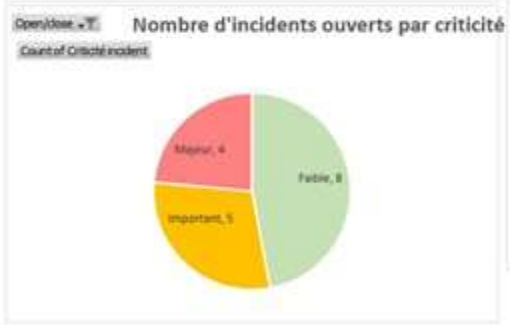
# Reporting incidents – gestion crise

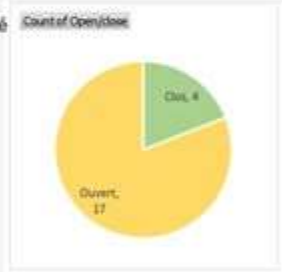
Tableau de bord incidents

Dashboard Incidents

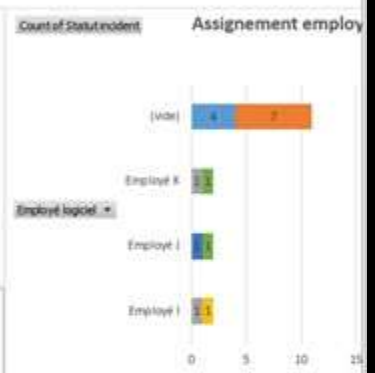


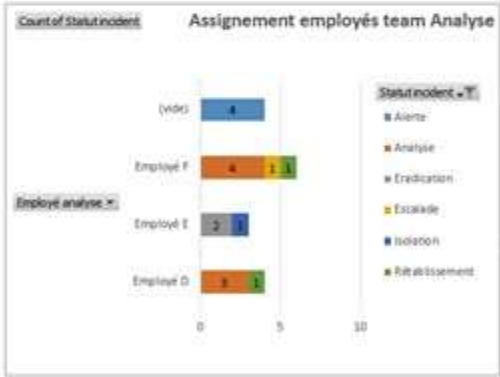



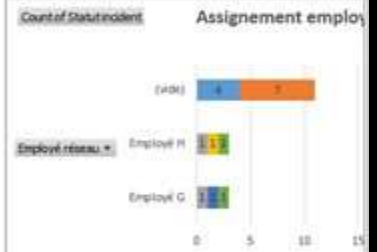




Dashboard ressources

# Mesures de gouvernance documentées

# Politique de gouvernance d'une entreprise ou collectivité

- Désignation de l'équipe de gestion de risques pluridisciplinaires (sponsor, production, RH, Juridique & communication, moyens généraux, IT, ICS)

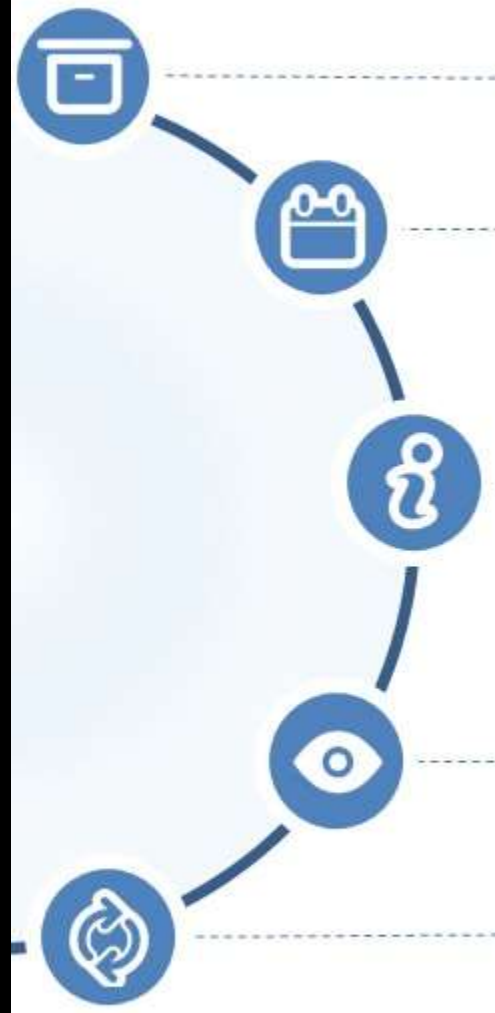
- Gestion des incidents et des risques :
  - évolution en fonction des nouvelles menaces
  - test des procédures mises en place
  - entraînement des équipes gestion des incidents & gestion de crise

- Politique de sensibilisation de tout le personnel et intervenants extérieurs aux cyber-risques

- Maîtrise de la communication par la mise en place d'une politique de confidentialité concernant la rédaction de références (validation par Linpac avant publication)

- Mise en place d'une charte de sécurité

# Missions du responsable cyber-risques de l'entreprise



S'informer sur les menaces, les tendances et les options de sécurité

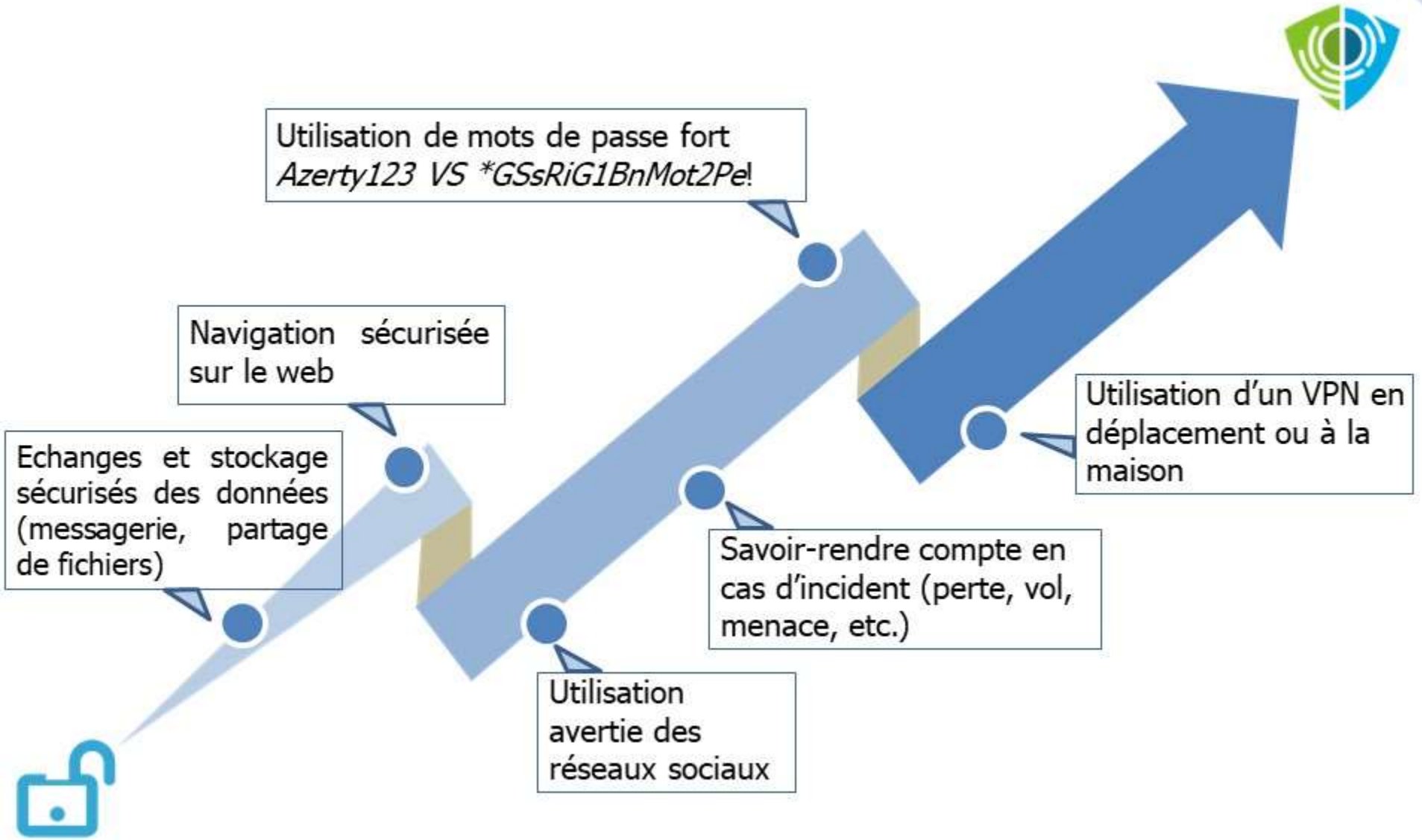
Planifier et mettre en œuvre les mesures de sécurité

Aider les autres membres du personnel à comprendre les politiques et les bonnes pratiques en matière de cyber sécurité (formation initiale, réunions d'information, webinaires…)

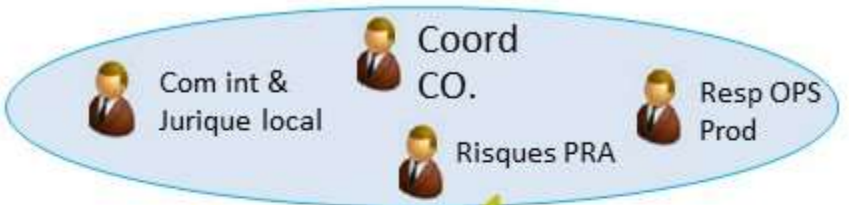
Contrôler la mise en œuvre des consignes de cyber sécurité

Remettre à jour les consignes de cyber sécurité en fonction de l'évolution des menaces ou des retours d'expérience

# Formation cyber hygiène pour tout le personnel sans exception



# Entraînement à la gestion d'incidents et de crise

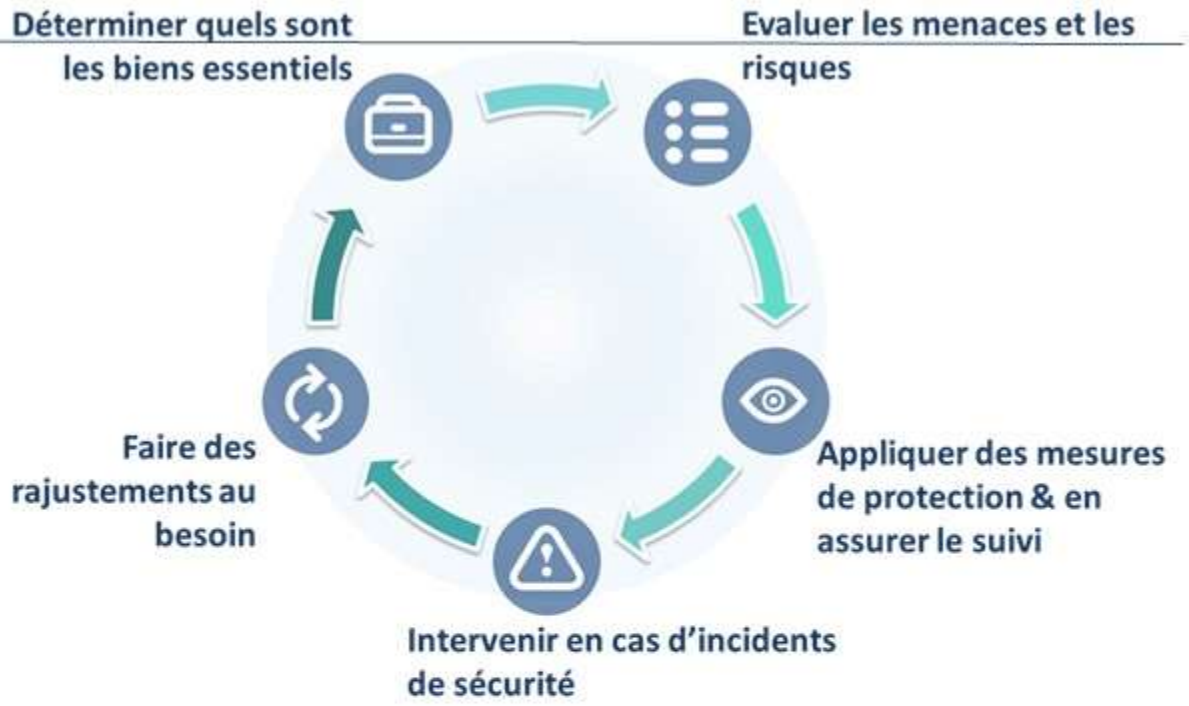


Escalade gestion d'incidents / gestion de crise



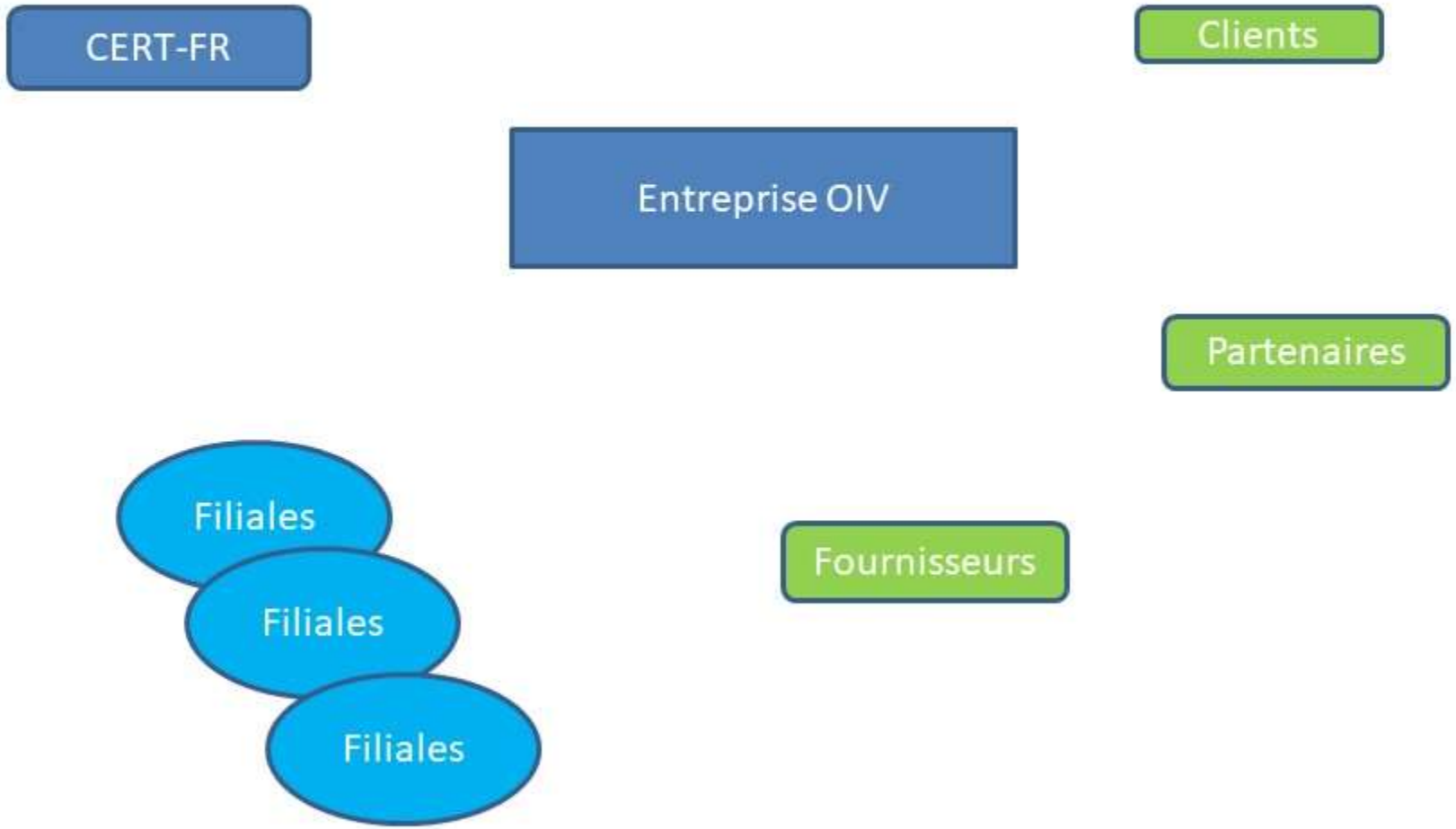
# Mesures de protection

- Architectures sécurisées et documentées
- Mise à jour des applications et systèmes (attention aux systèmes non maintenus officiellement ex Windows XP)
- Plan de continuité, procédures de restauration testées
- Systèmes nomades avec VPN et moyens de chiffrement
- Mettre en place une stratégie de sauvegarde de données




# Gestion d'incidents et de crise

# Acteurs de gestion de crise



# Les 12 secteurs d'activités d'importance vitale

**Secteurs étatiques :**

- activités civiles , militaires, judiciaires de l'Etat
- espace et recherche

**Secteurs de la protection des citoyens :**

- santé
- gestion de l'eau
- alimentation

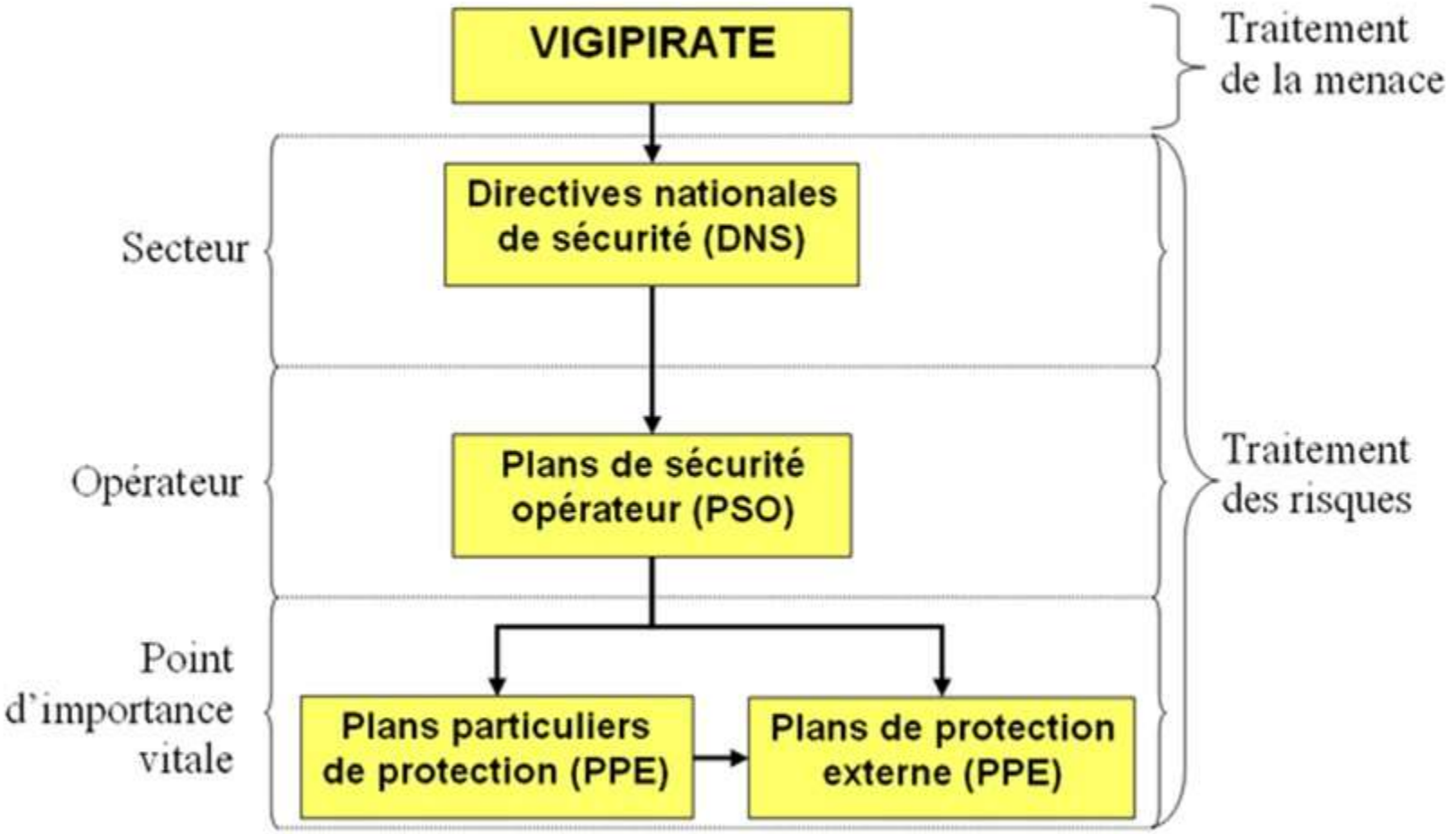
**Secteurs de la vie économique et sociale de la nation :**

- énergie ;
- communications électroniques, audiovisuel et information
- transports
- finances
- industrie

# Les obligations des OIV

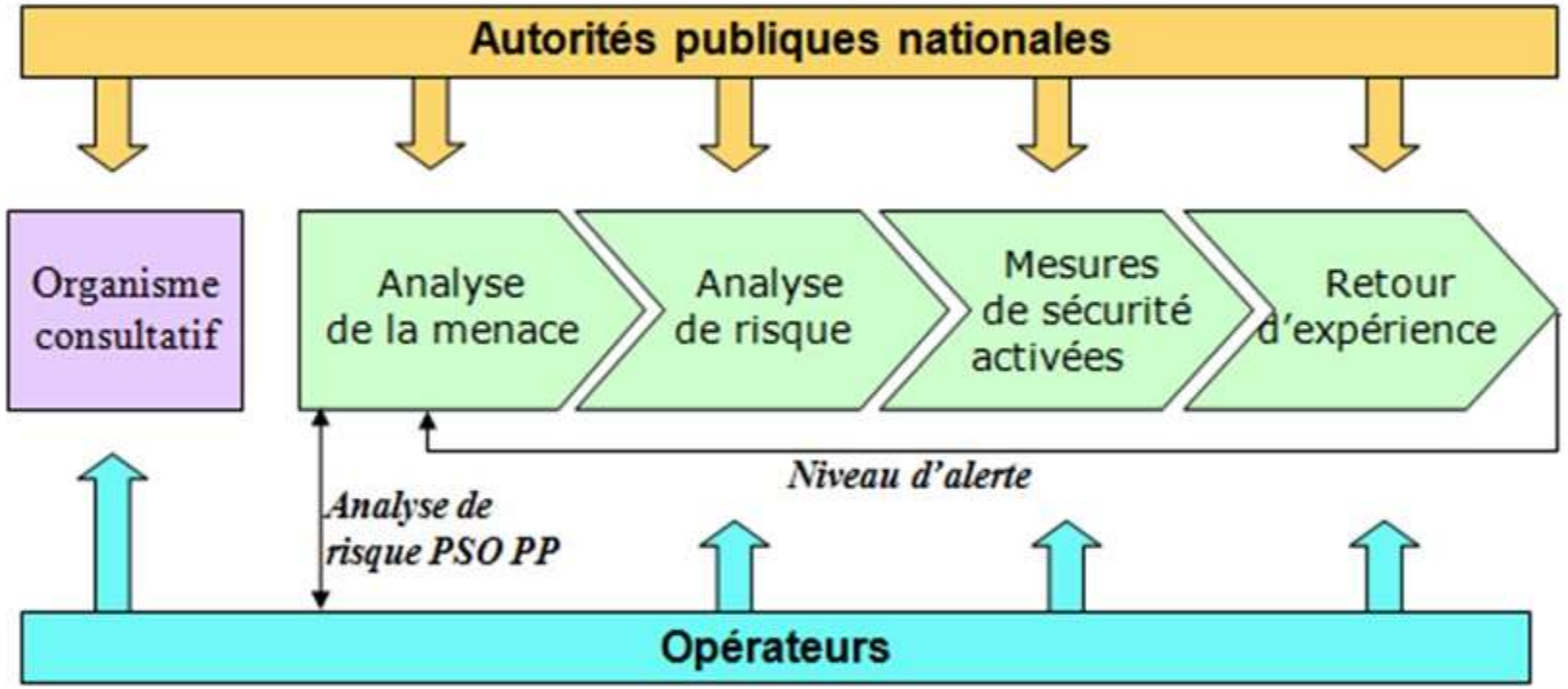
- Former leurs responsables et leurs directeurs de la sécurité tant au niveau central qu'au niveau local.
- - Après une analyse de risques, établir un plan de sécurité opérateur prenant en compte les attendus de la directive nationale de sécurité au titre de laquelle ils ont été désignés opérateurs d'importance vitale.
- - Identifier leurs points d'importance vitale qui feront l'objet d'un plan particulier de protection (PPP) à leur charge et d'un plan de protection externe (PPE) à la charge du préfet de département.

# Obligations



# Décret 2006

**Organisation générale du décret de 2006 :**



# ANSSI –COSSI-CERT-FR

Au sein du Centre Opérationnel de la Sécurité des Systèmes d'Information (COSSI) de l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI), le CERT-FR apporte son soutien en matière de gestion d'incidents aux ministères, institutions, juridictions, autorités indépendantes, collectivités territoriales et OIV (Opérateurs d'Importance Vitale).

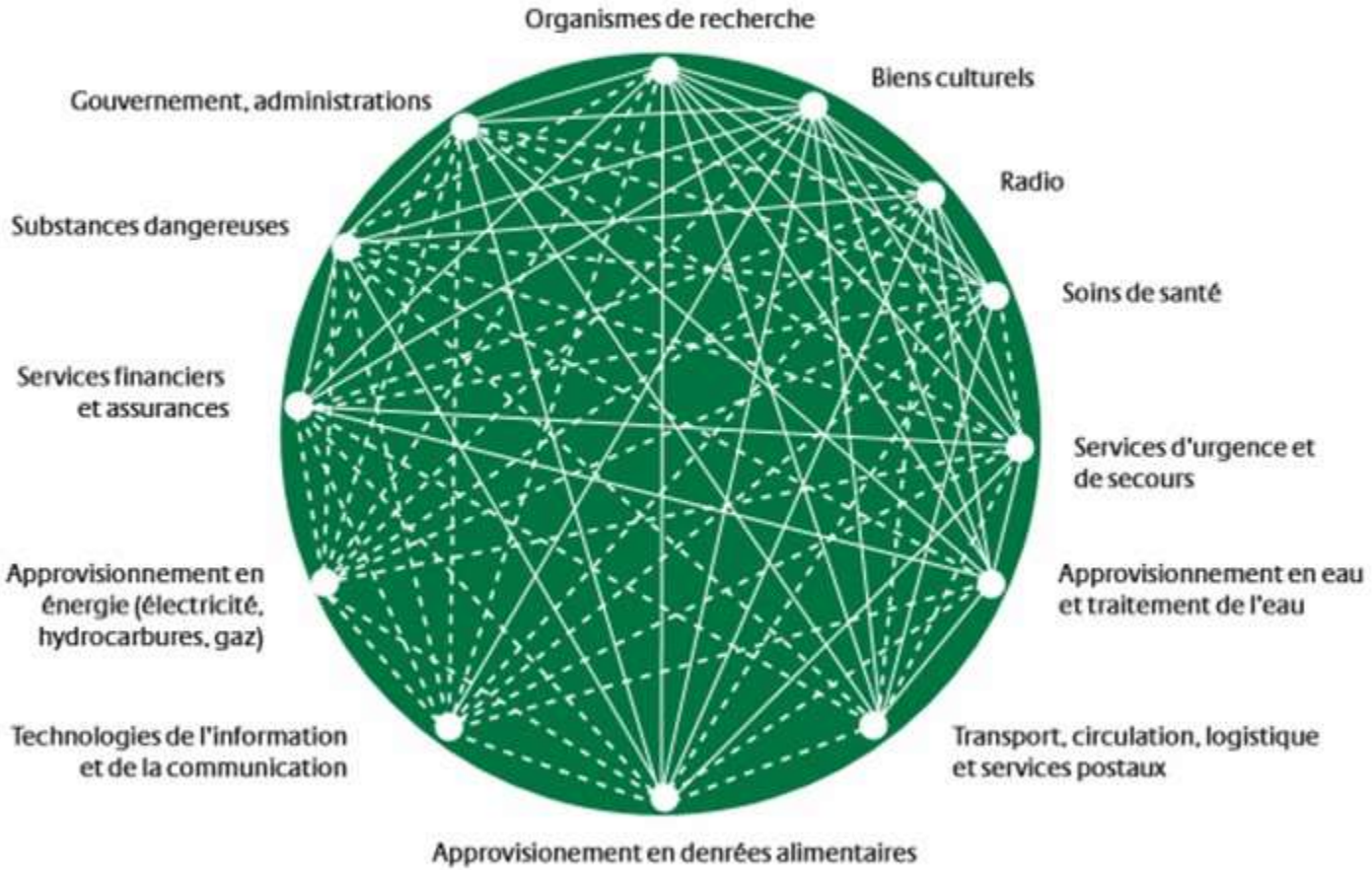
Le CERT-FR est chargé d'assister les organismes de l'administration à mettre en place des moyens de protection nécessaires et à répondre aux incidents ou aux attaques informatiques dont ils sont victimes

# Caractéristiques des infrastructures critiques

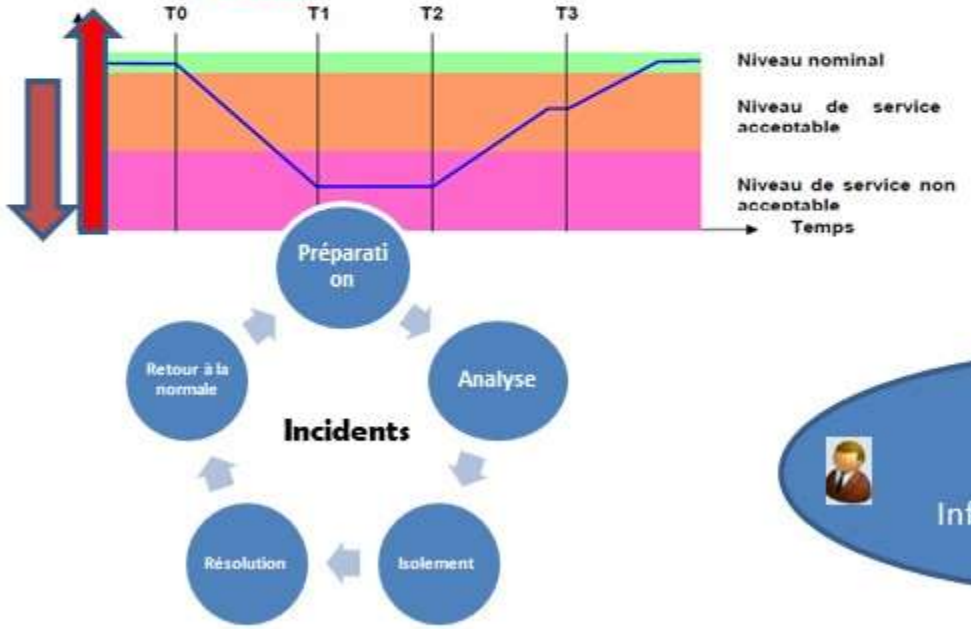
- Interdépendance
- Evolution de l'environnement technologique
- Exigences juridiques relatives à la gestion des risques et des crises

# Interdépendance des infrastructures

**Illustration 1 : Interdépendances entre certaines infrastructures critiques**

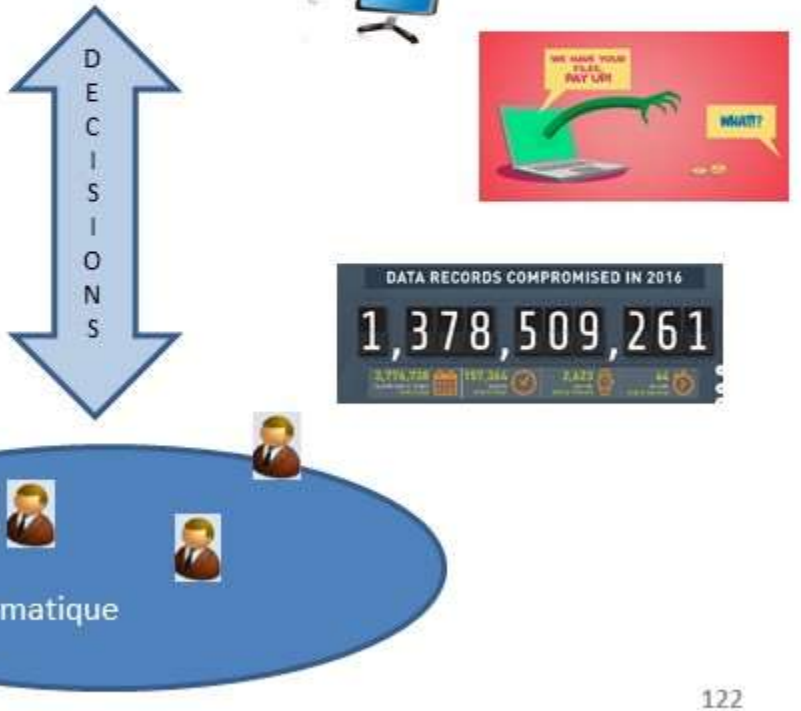


# Escalade –> Gestion de crise



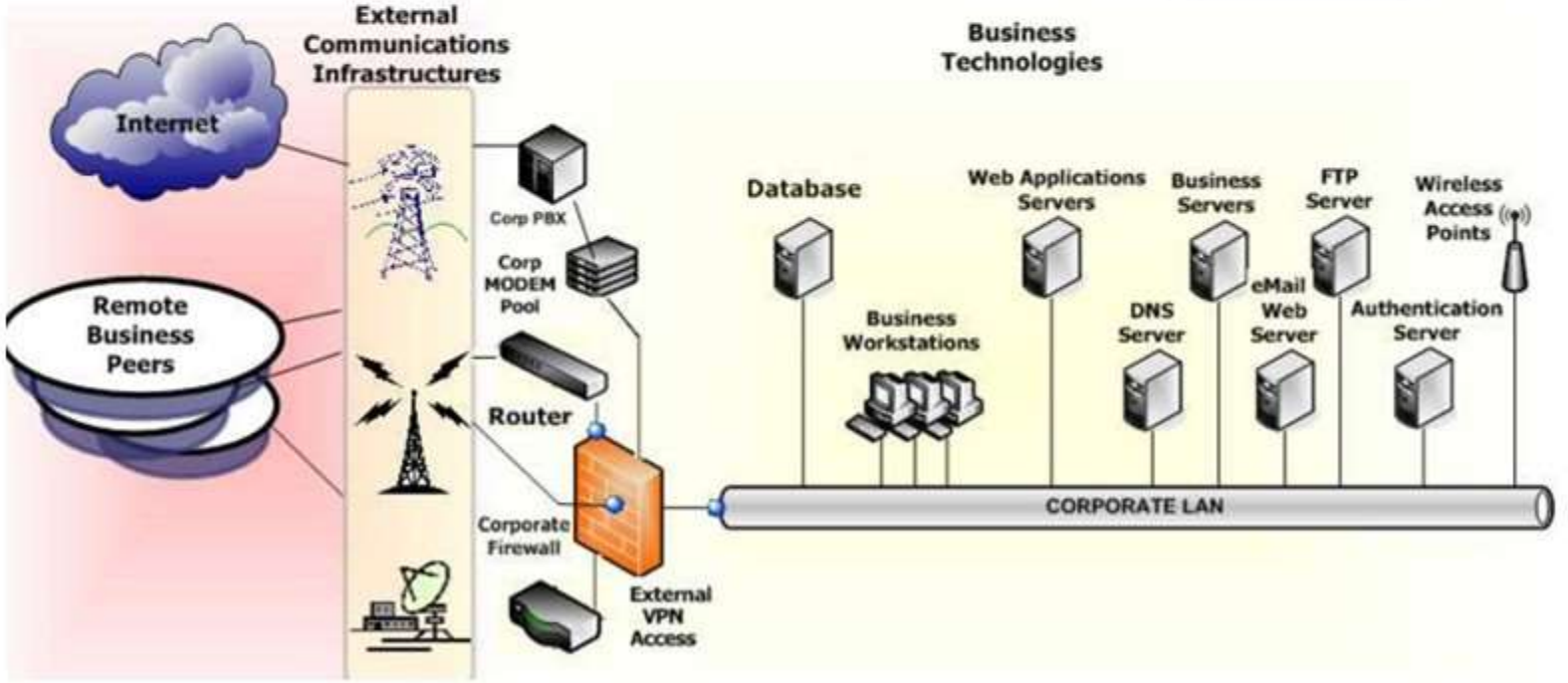






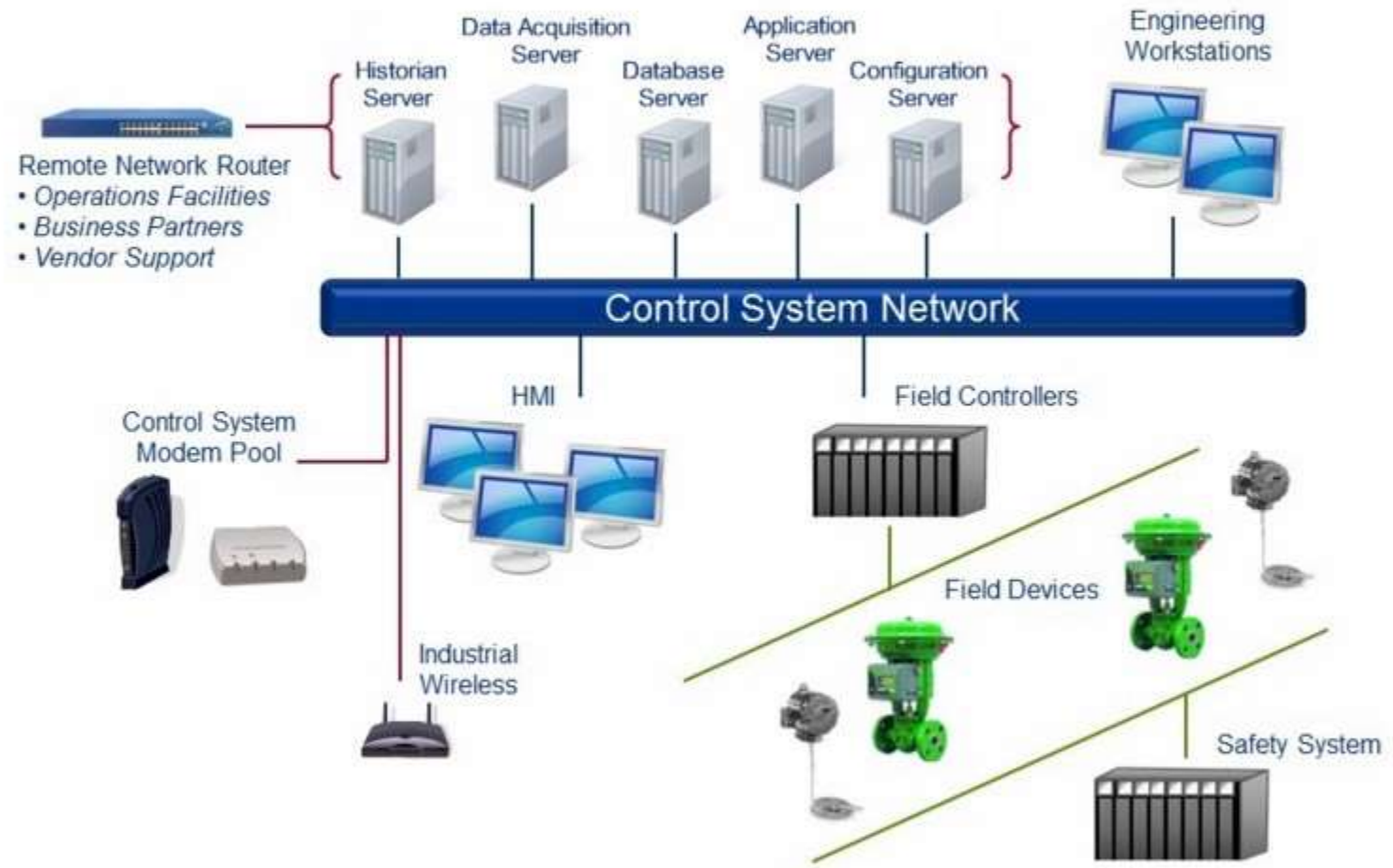
Risques numériques
MRT de sécurisation
Sécurisation des architectures SI et ICS
Datacenter et Cloud Computing
RGPD

# Infrastructure IT

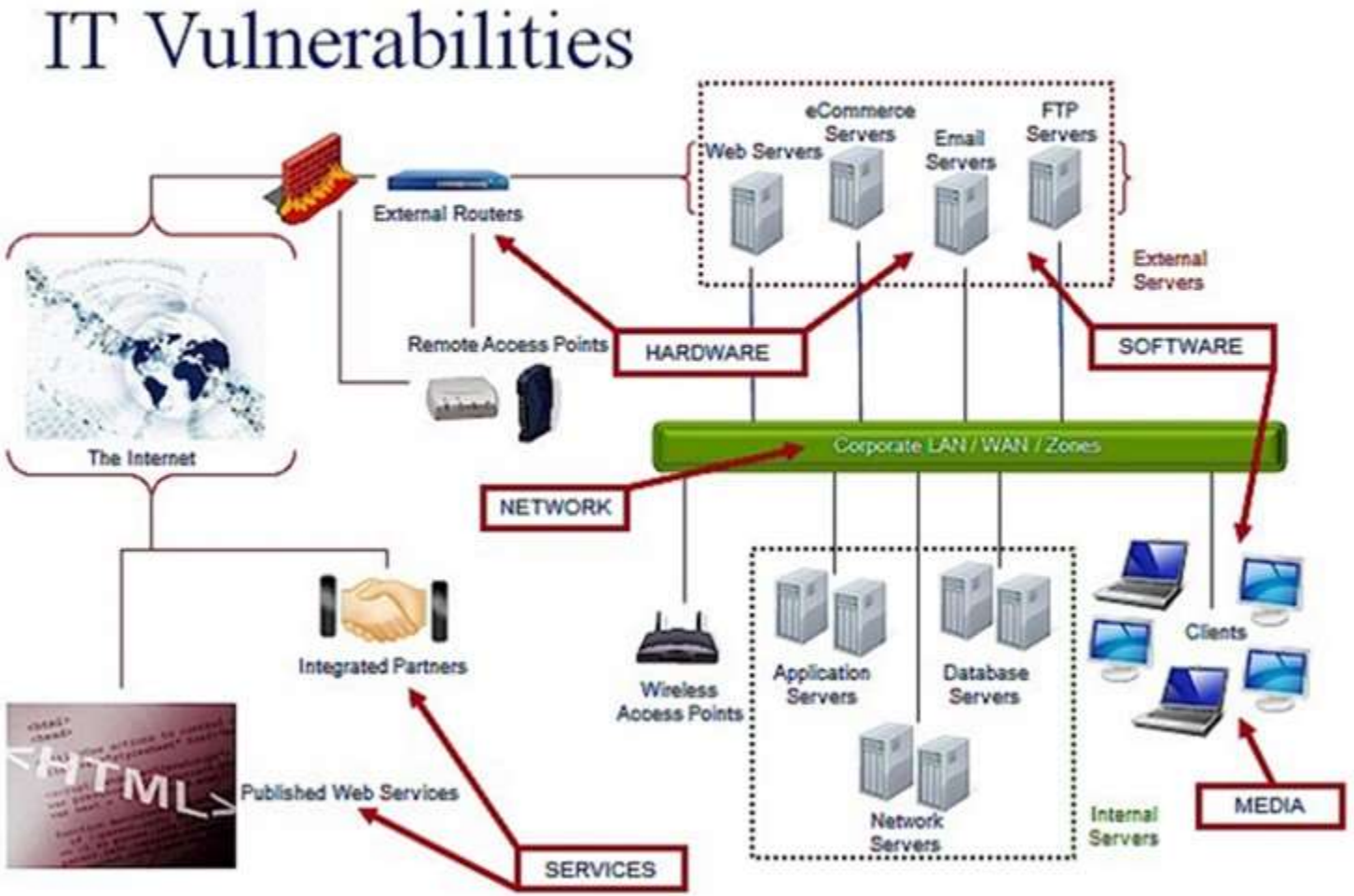
# Architecture ICS (Industrial Command System)

## ICS Architecture

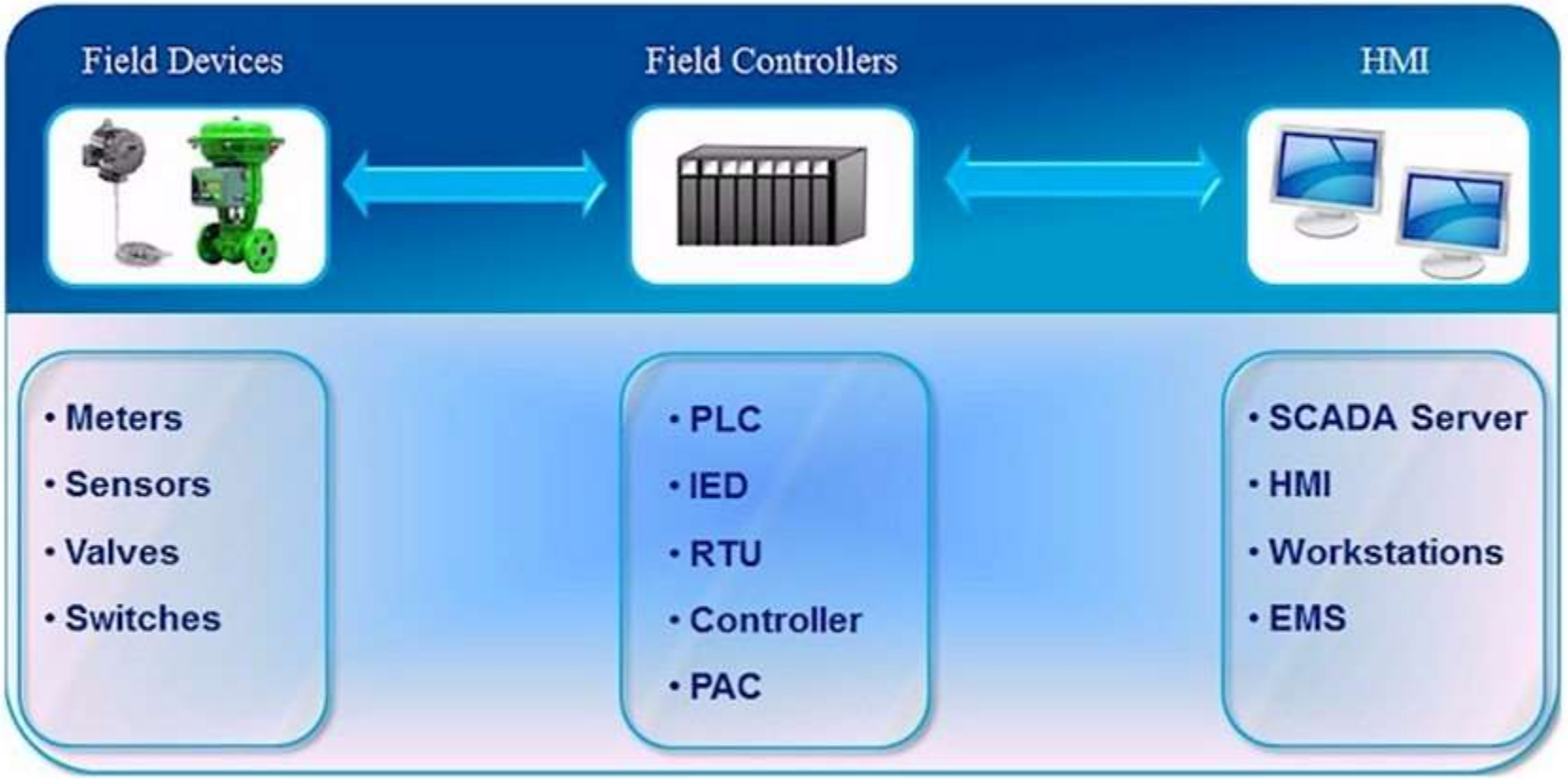


# Architecture ICS (Industrial Command System)

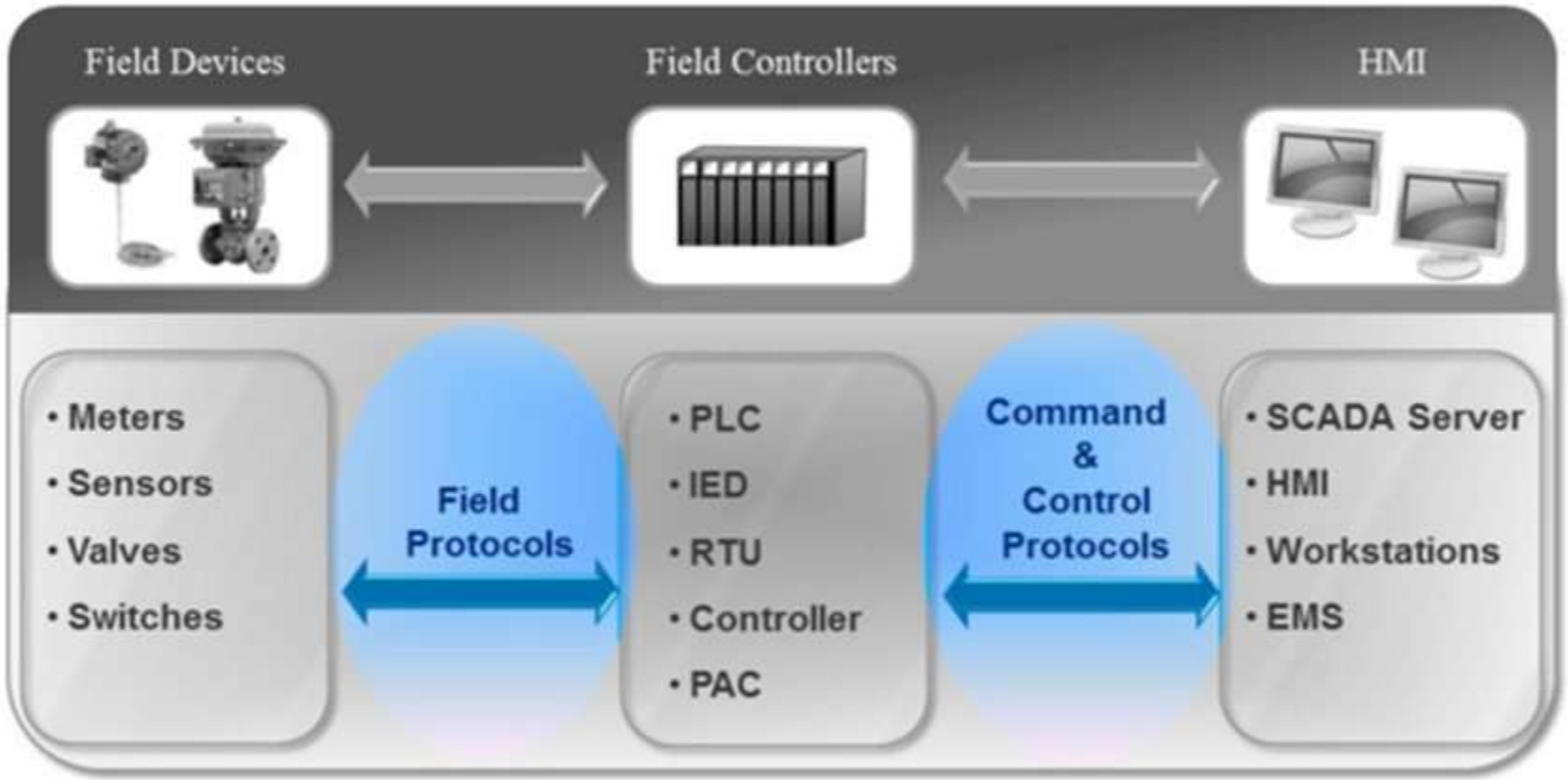
## - IT Vulnerabilities -



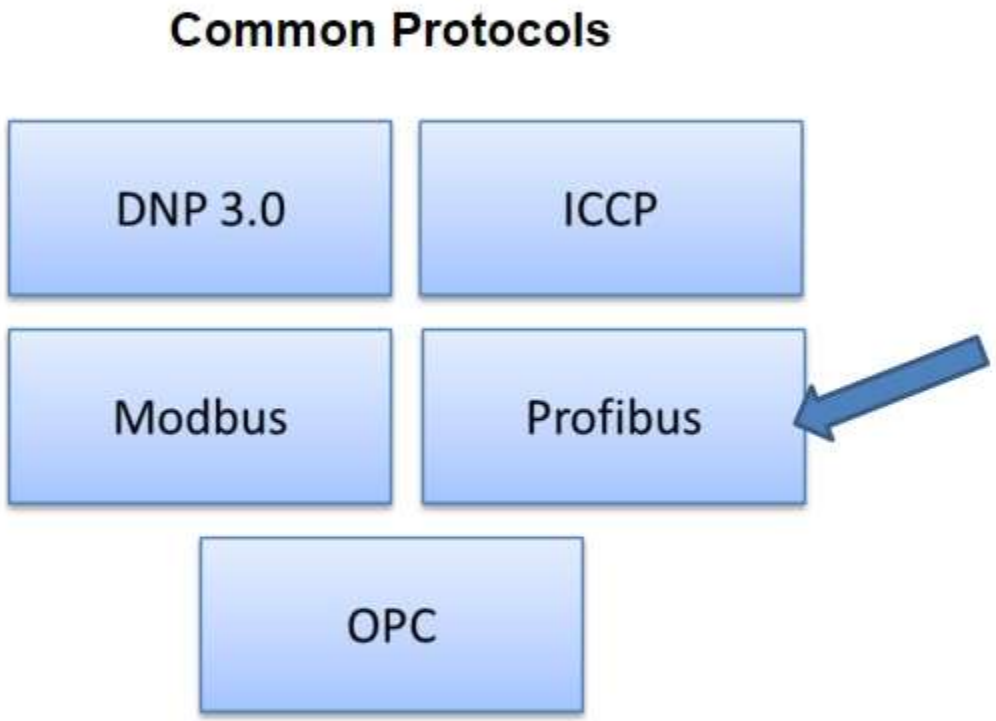
# Processus de production (lignes de production)



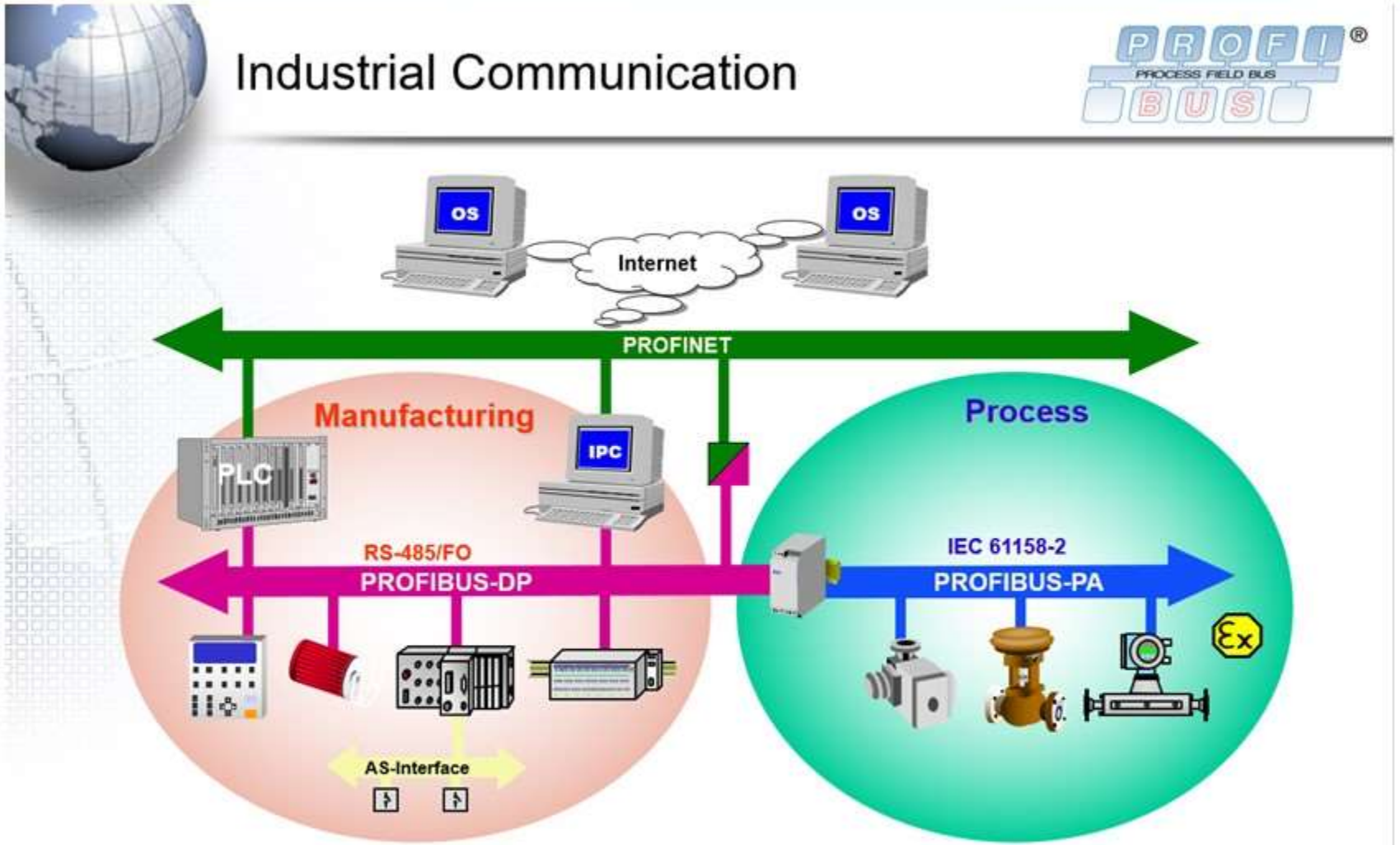
# Protocoles


Field Devices
Field Controllers
HMI
• Meters
• Sensors
• Valves
• Switches
Field Protocols
• PLC
• IED
• RTU
• Controller
• PAC
Command & Control Protocols
• SCADA Server
• HMI
• Workstations
• EMS

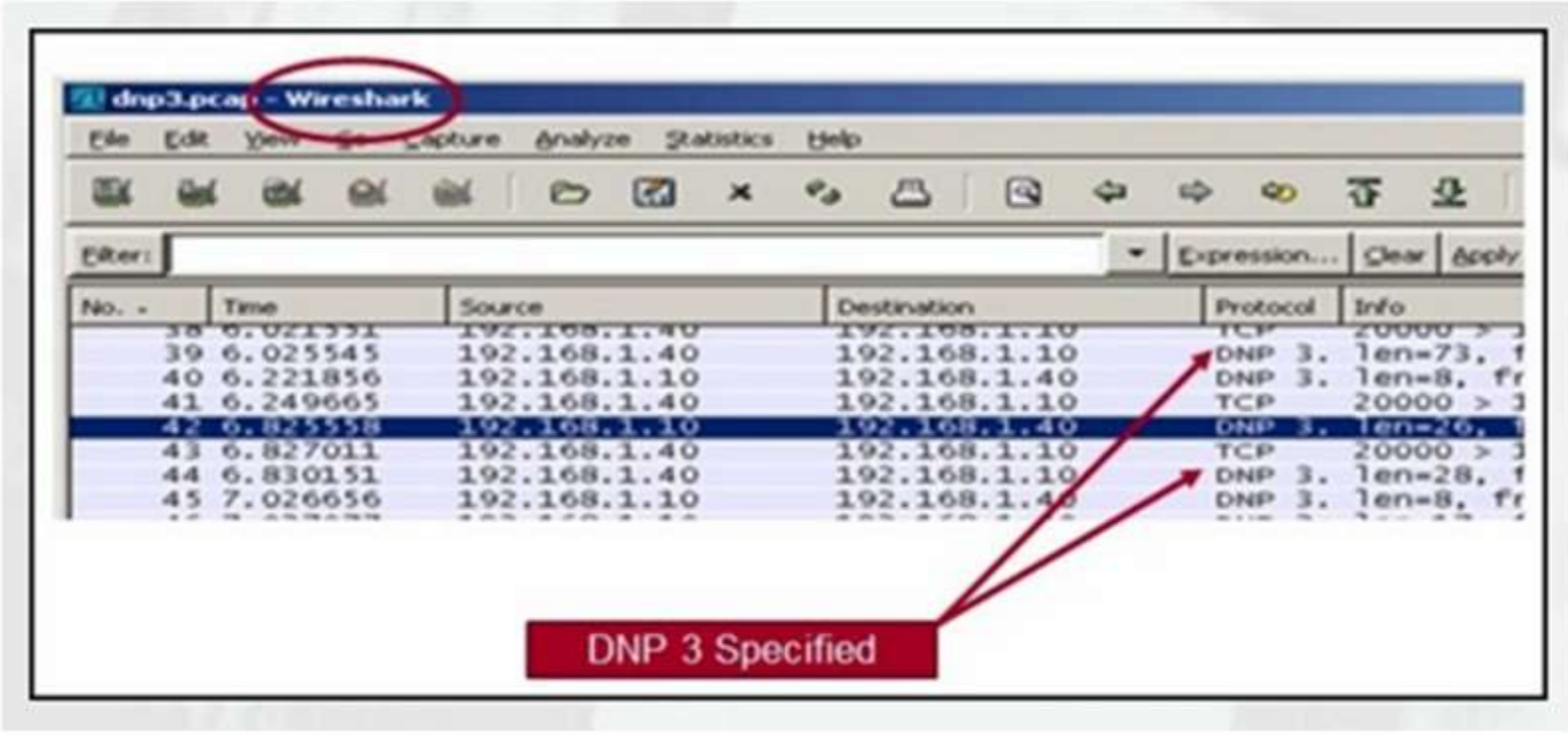
# Profibus : un des protocoles identifiés



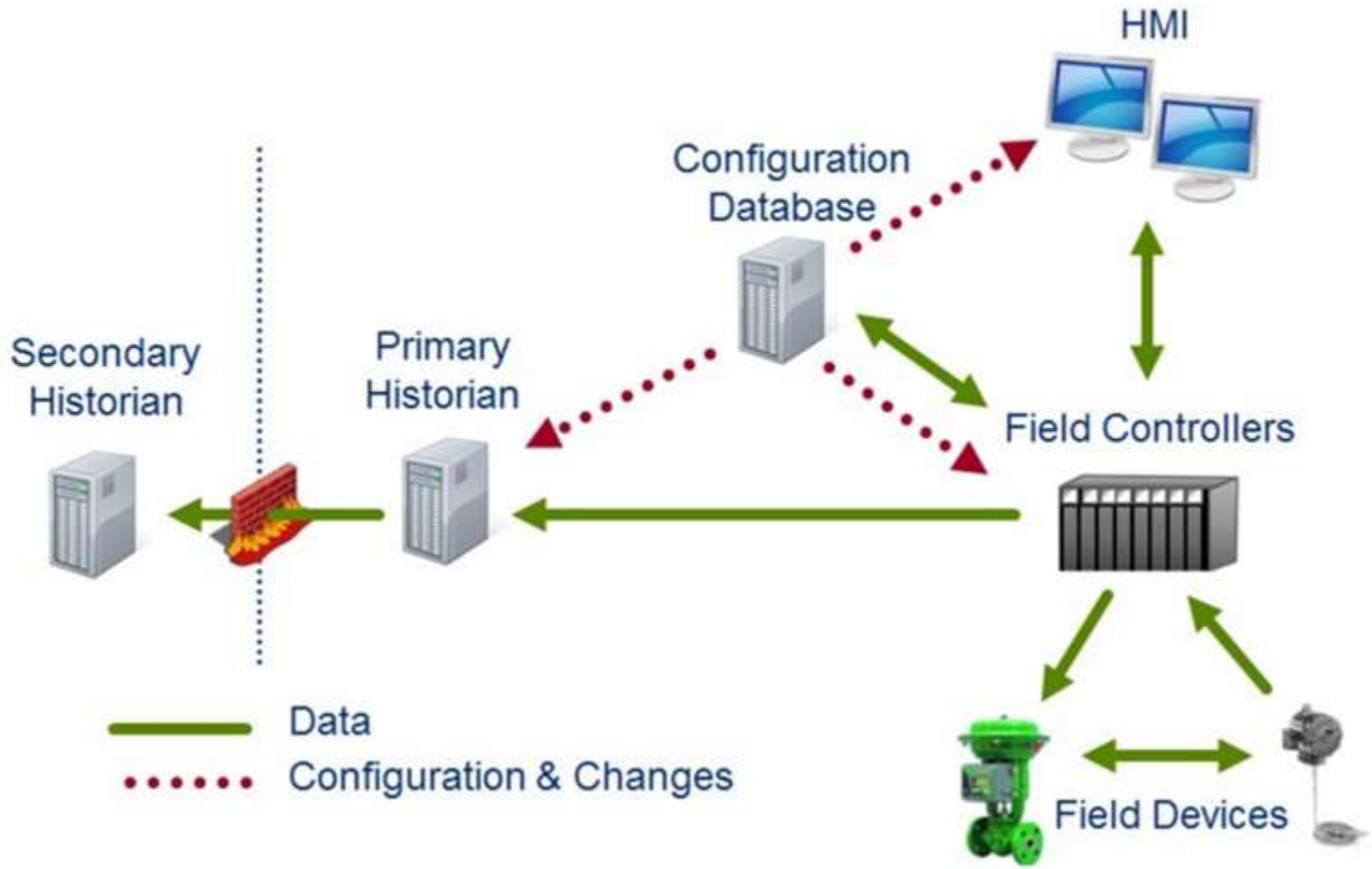
# Incompatibilité avec les pratiques de sécurité IT



# Attention à l'utilisation des outils de scan réseaux !



# Flux de données ICS



# Confidentialité, Intégrité, Disponibilité

Dans le monde de l'ICS :

**D – I - C**

→ la disponibilité est la priorité

Dans le monde de l'IT :

**C – I - D**

→ la confidentialité est la priorité

# Les facteurs techniques

Pour l'ICS, les facteurs techniques sont les contributeurs les plus importants aux risques cybersécurité. De nombreux facteurs techniques contribuent au cyber risque pour les systèmes de contrôle.

### *Historiquement*

Les concepteurs ICS ne prenaient pas en compte une possible menace cyber.

Cela se résulte pas des vulnérabilités exploitables au niveau réseau et physique aussi bien au niveau des systèmes hérités que dans certains designs actuals.

### *Interconnectivité*

L'interconnectivité entre l'IT et les domaines de système de contrôle créée de nouveaux vecteurs d'attaque.

Cela inclus les accès à distance, les réseaux peer-to-peer, connexion direct…

### *Incidents*

Il y a une augmentation notable de rapports de cyberattaques sur les systèmes ICS à travers le monde.

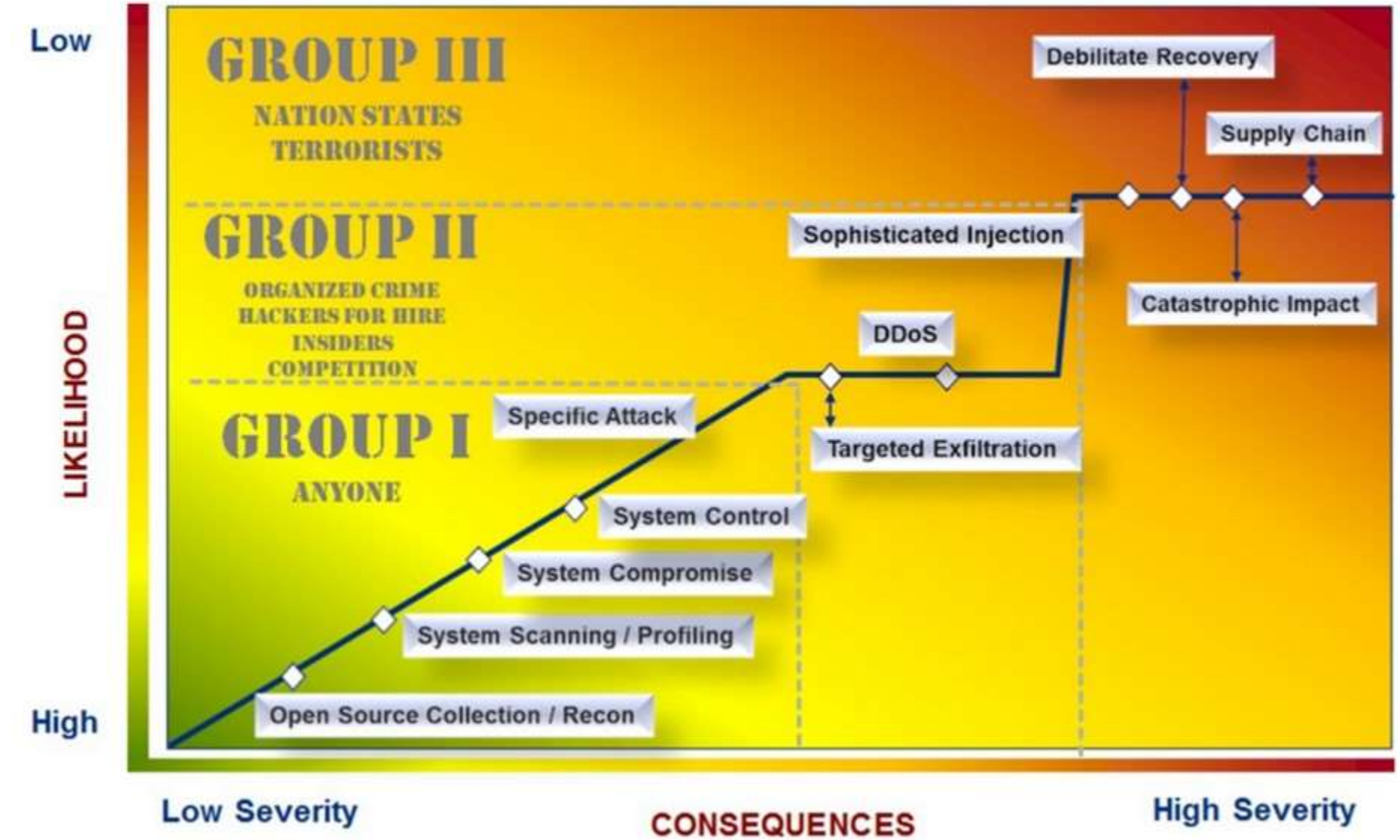
De plus, des logiciels malicieux ciblant spécifiquement les systèmes ICS sont découverts régulièrement.

### *Évolutions*

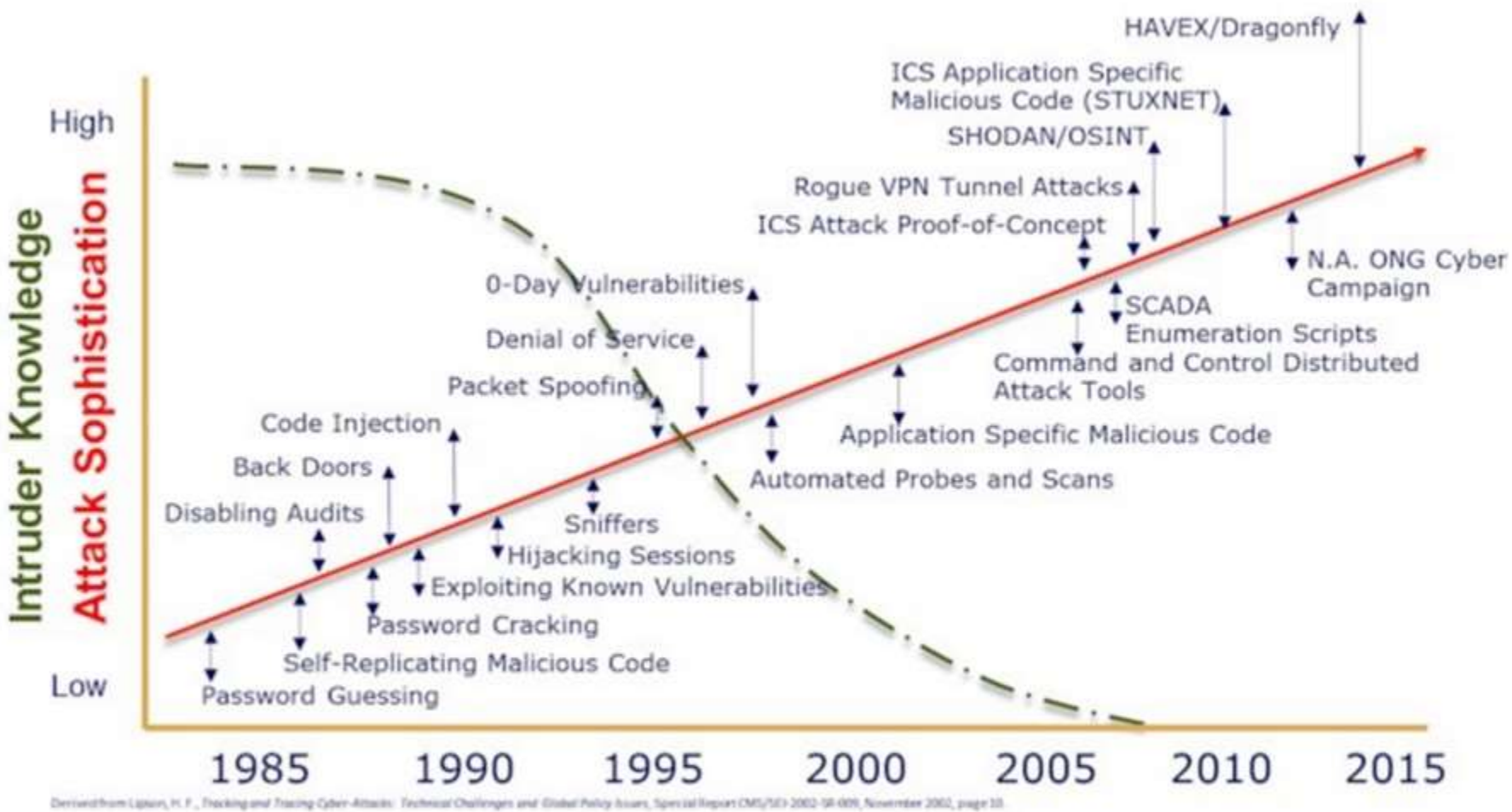
Bien que les vendeurs et la communauté de chercheurs font un excellent travail pour couvrir les vulnérabilités.

La mise en œuvre des contre mesures peuvent parfois avoir pour résultat un comportement du système de contrôle non désirable ou inattendu.

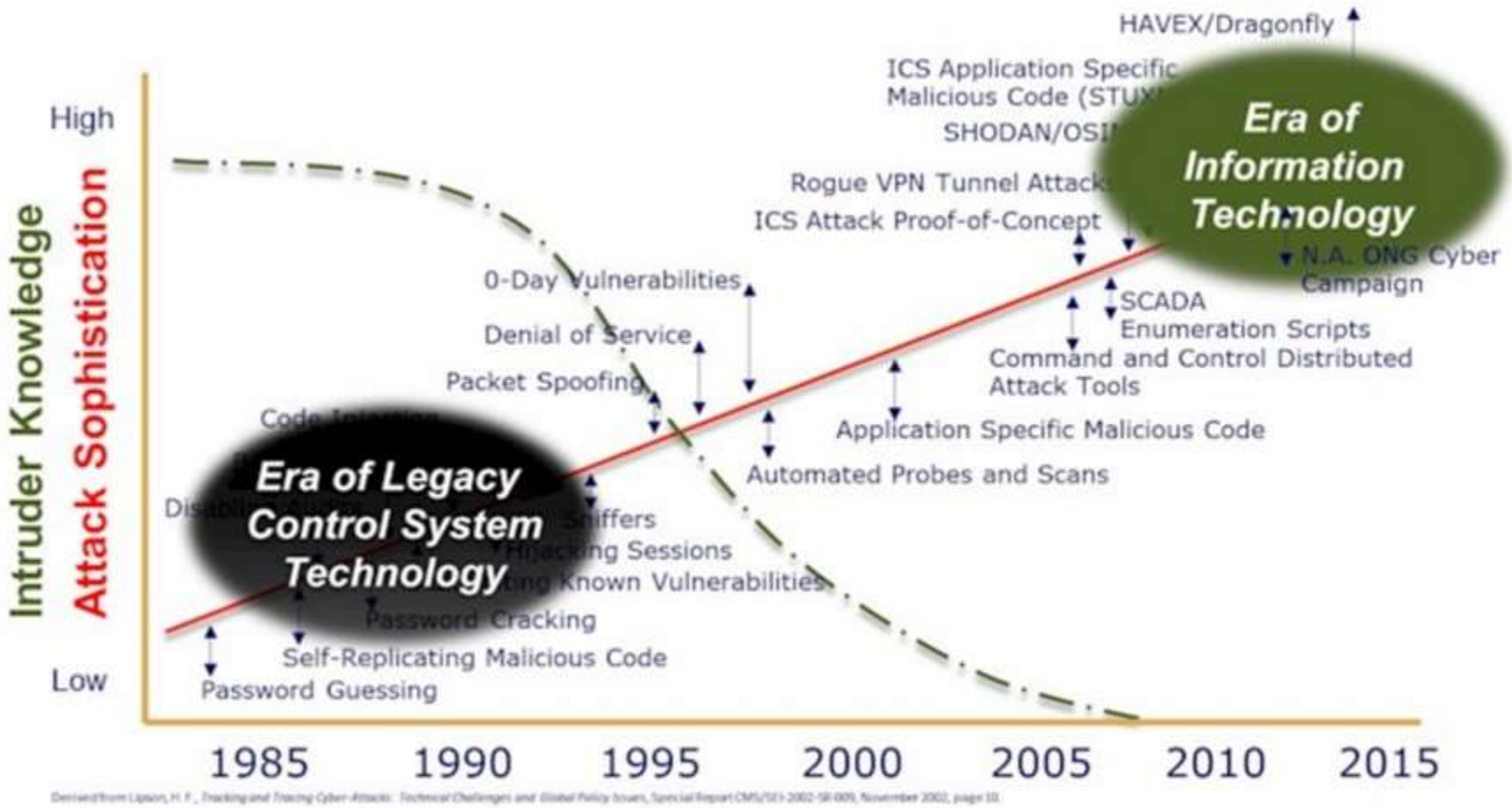
# La courbe des risques 4/4



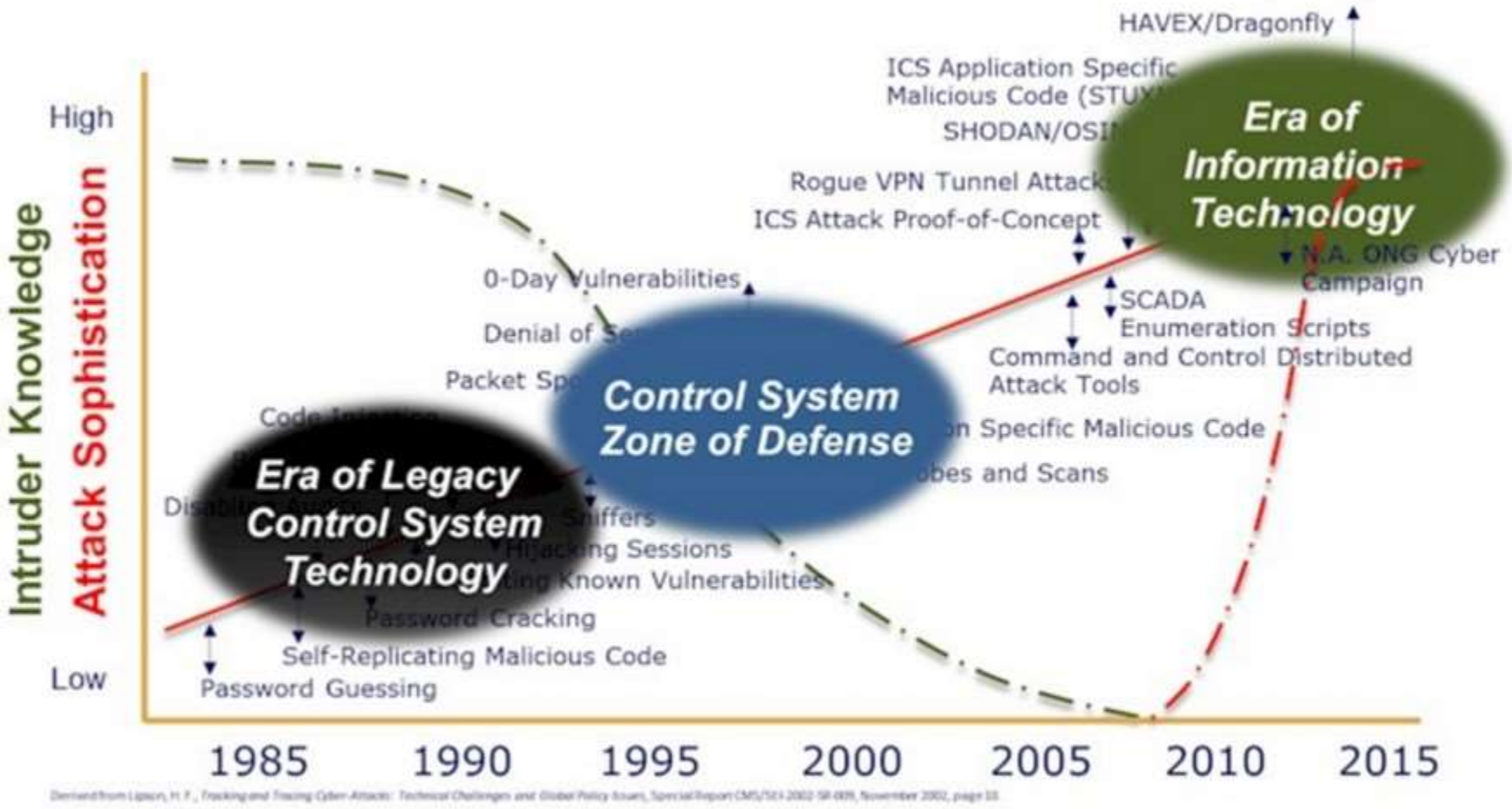
# Tendance des menaces



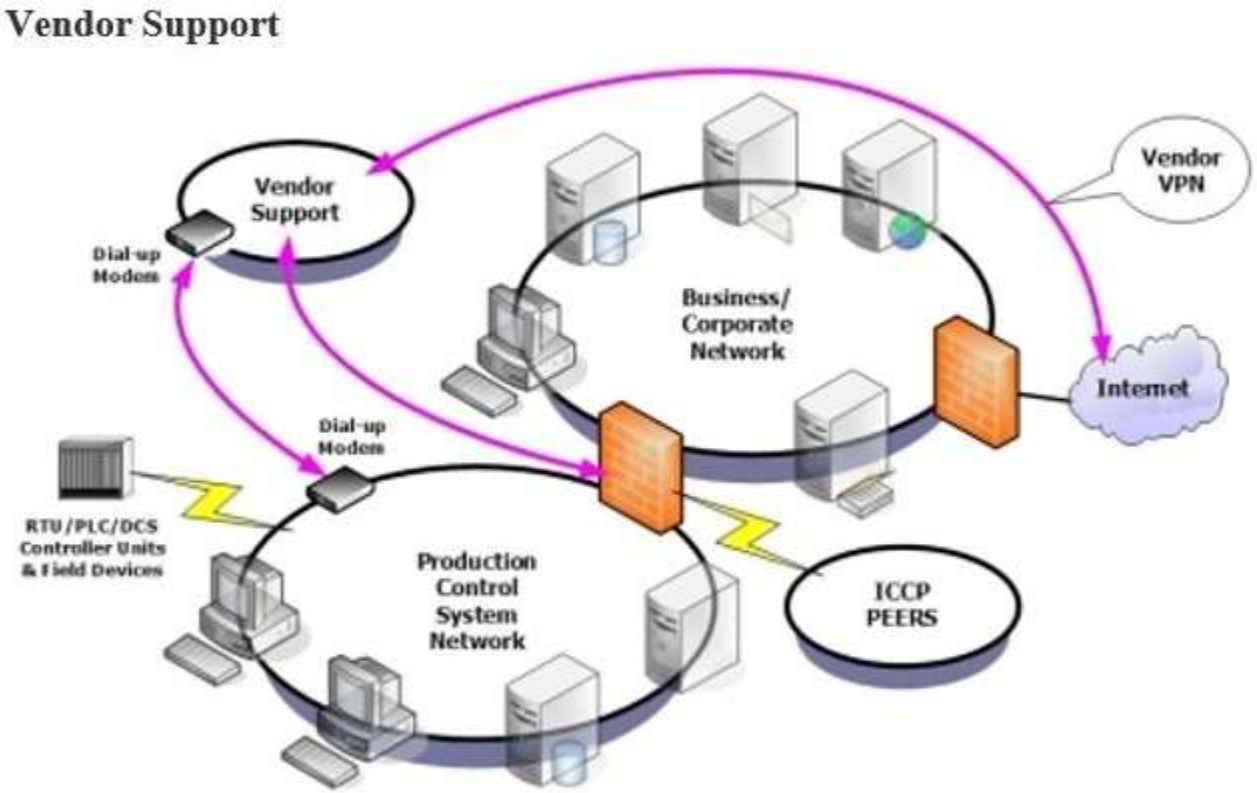
# Tendance des menaces



# Tendance des menaces



# Architecture système industriel multiples localisations & acteurs



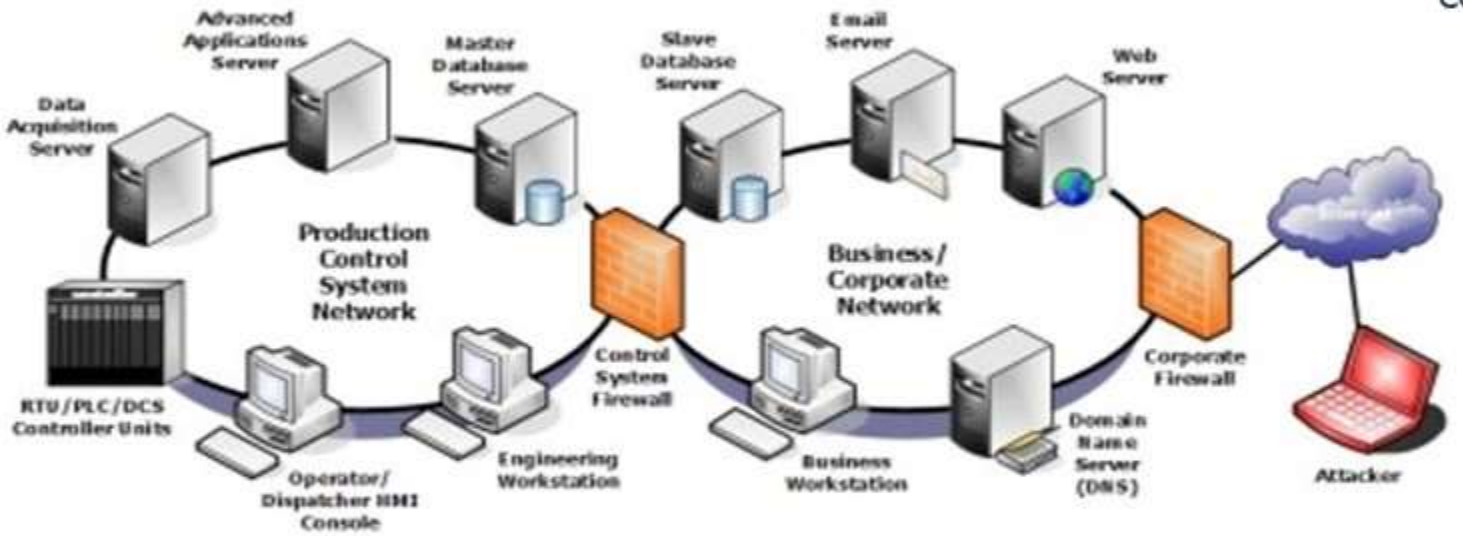

large version

**Figure 8: Vendor support**

- Accès à distance multiples
- Protocoles multiples
- Acteurs multiples

# Firewall mal configuré

- Vulnérabilité Firewall mal configuré

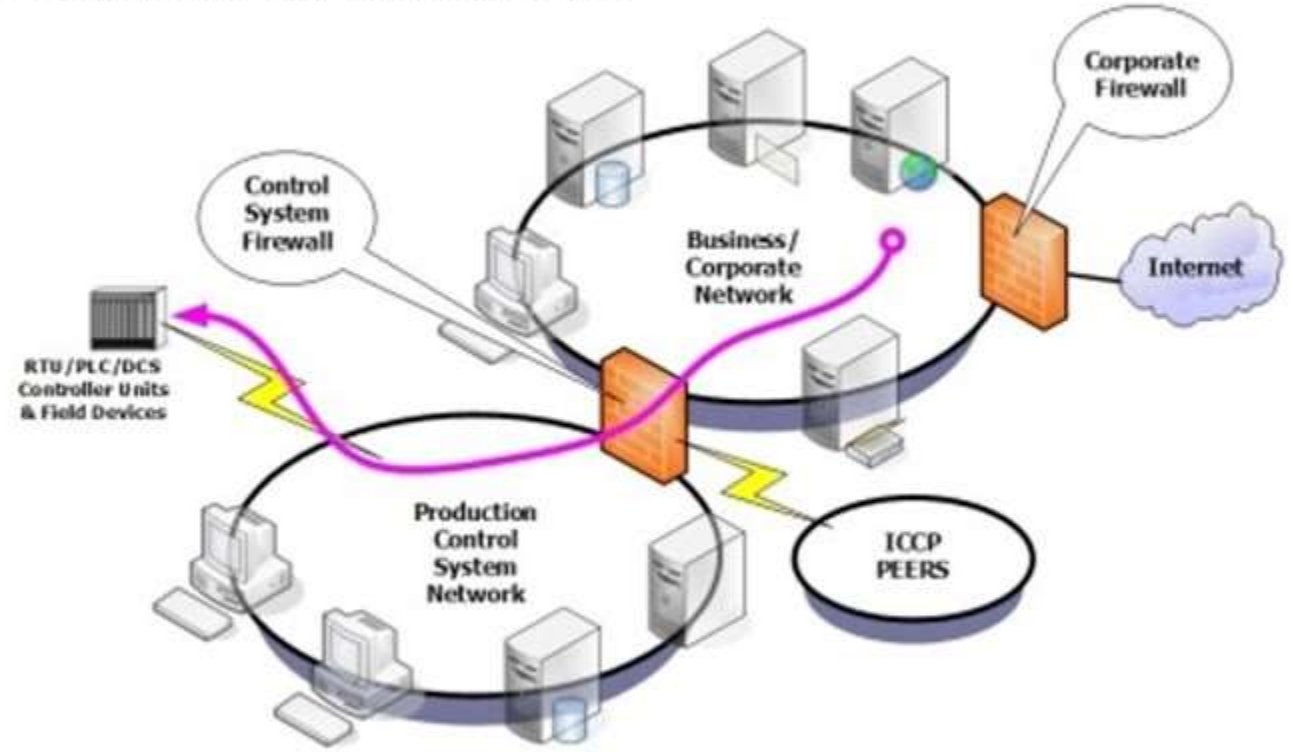



large version

**Figure 2: Typical two-firewall network architecture**

# Canal accès interne vers composants décentralisés

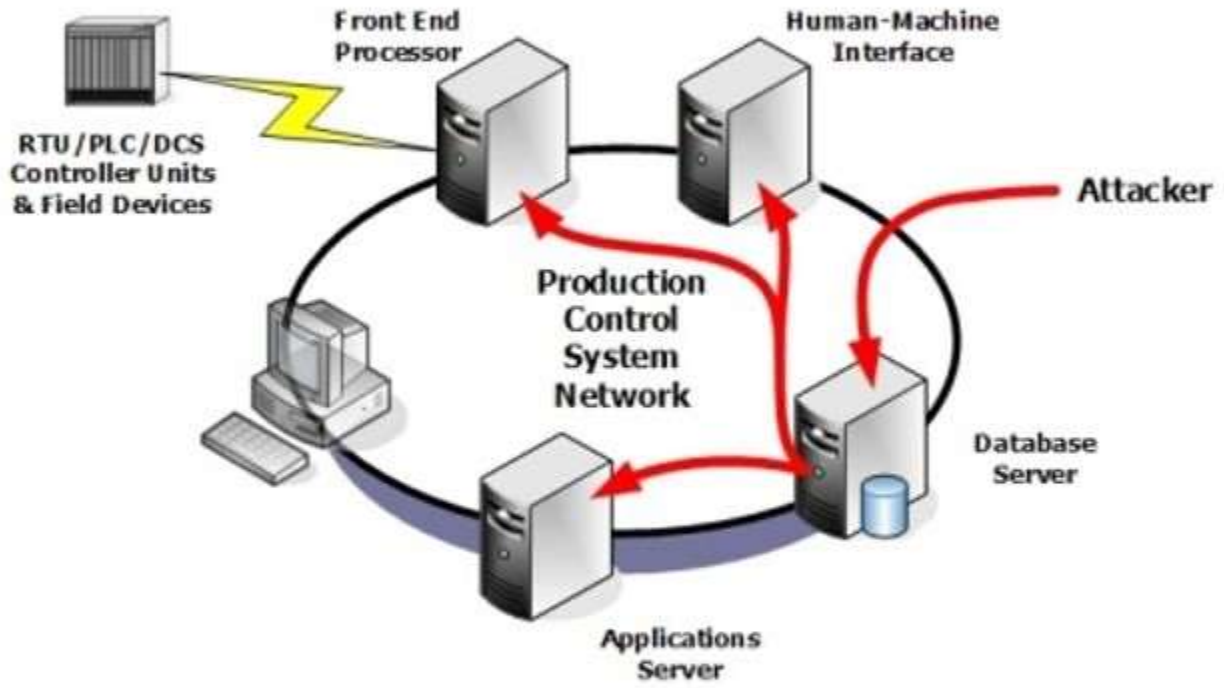
**IT Controlled Communication Gear**




large version

**Figure 9: IT Controlled Communication Gear**

# Propagation attaque via base de données




large version

**Figure 15: Changing the database**

# Les mesures classiques de l'IT

Outsourcing

Pare-feu

Antivirus &
Antimalware

Patch
Management

Security testing

# ICS & Outils de détection / antivirus = incompatibilité

- Outil de scan tels que Nmap ou Superscan incompatibles avec ICS (ralentissement communication, pertes d'information pour le processus industriel)
- Outils de détection IT basés sur les signatures peuvent causer des dommages considérables car incompatibles avec les contraintes temps réel de la production et les protocoles utilisés
- Ressources ICS limitées en CPU, RAM, bande passante
- Pas encore de vendeurs spécialisés pour les virus ICS

# Mesures de défense : de notables différences entre IT & ICS

- IT :

  Bonne connaissance, de la part des personnels IT et des vendeurs, des processus et technologies de protection des réseaux et des systèmes face aux cyber attaques :

  - Solutions de prévention Pare-feu, DMZ, outil de détection et d'intrusion
  - Plan de reprise d'activité et réversibilité (image système / back-up)
  - Mise à disposition de correctifs (patchs) réactive & rapide
  - Mots de passe robustes, changeables régulièrement et individuels

- ICS :

  Mise en place de mesure de sécurité est un challenge pour les administrateurs ICS et les fournisseurs :

  - Utilisation d'OS et d'applications vulnérables (MS Windows, Base de données SQL)
  - Connections TCP/IP, WIFI, séries, protocoles industriels (texte en clair)
  - Pas de possibilité de tester l'impact des correctifs sur la production (irréversibilité)
  - Peu de partage d'information sur les vulnérabilités
  - Délai important entre mise à disponibilité des patchs et mise en production
  - Mots de passe partagés entre les équipes de production et de maintenance (couplage avec badge ID? )
  - Téléchargements correctifs certifiés par les vendeurs (problèmes du Waterhole)

# Personnel de maintenance ICS

- Les opérateurs commandent et surveillent le processus de production. Une erreur humaine ou une attaque intentionnelle peut stopper la production.

- Des opérateurs non sensibilisés aux cyber risques peuvent infecter le système avec des virus : utilisation clefs USB, accès internet, téléchargement, emails ; et donc mettre la production ou l'installation en péril (en fonction des motifs des attaquants)

- Intervenants extérieurs utilisent souvent un même ordinateur pour effectuer la maintenance ou travailler. La planification de leur intervention doit être supervisée :
  - Gestion des droits utilisateurs doit être particulière et limitée dans le temps
  - Composant TCP/IP plug-in : délai entre l'installation et l'intégration du nouveau composant dans l'architecture sécurisée en particulier sur des sites distants
  - Utilisation d'un VPN entre l'intervenant et son entreprise :
    - Mot de passe faible :=> compromission possible
    - Introduction de virus : USB, connexion directe
  - Accompagnement obligatoire dans les zones ou sur des équipements critiques

# Outsourcing ICS

De nouveaux service, issus de l'IT, apparaissent pour le monde du contrôle industriel (ICS) :

- Cloud computing as a service
- Security as a service

- Niveau de maturité insuffisant
- A utiliser avec précautions

# Audit & test de sécurité

- Attention à l'utilisation des outils IT en particulier scanner de réseaux et antivirus
- Processus temps de fabrication = Temps réel
- Composants et protocoles ont des ressources limitées
- Elaborer des scénarios d'attaque et regarder les procédures de défense associées

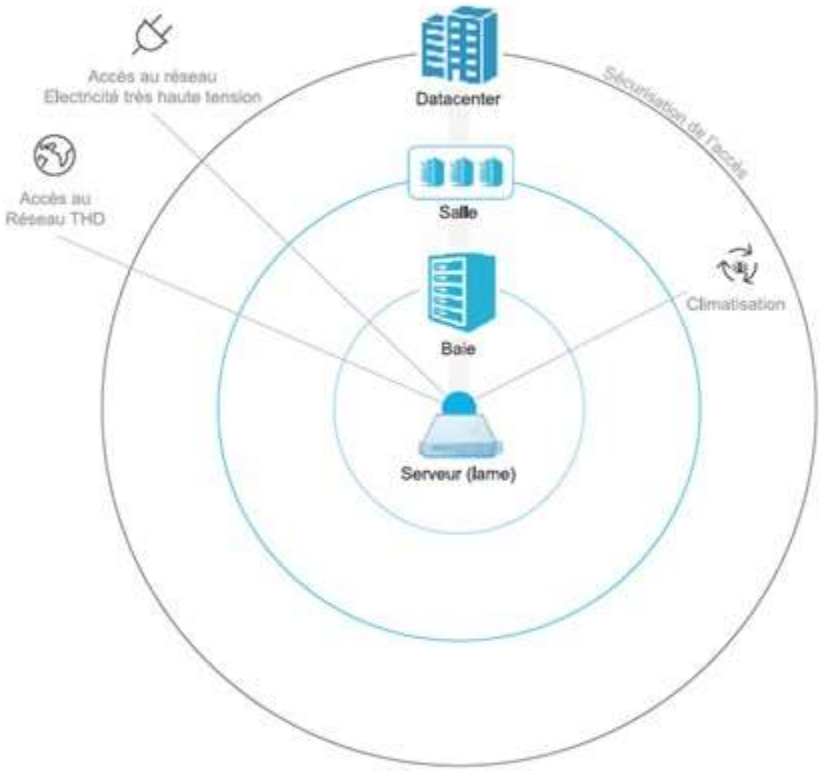

Risques numériques
MRT de sécurisation
Sécurisation des architectures SI et ICS
Datacenter et Cloud Computing
RGPD


DATA CENTER
CLOUD COMPUTING
RISQUES INFOGERANCE

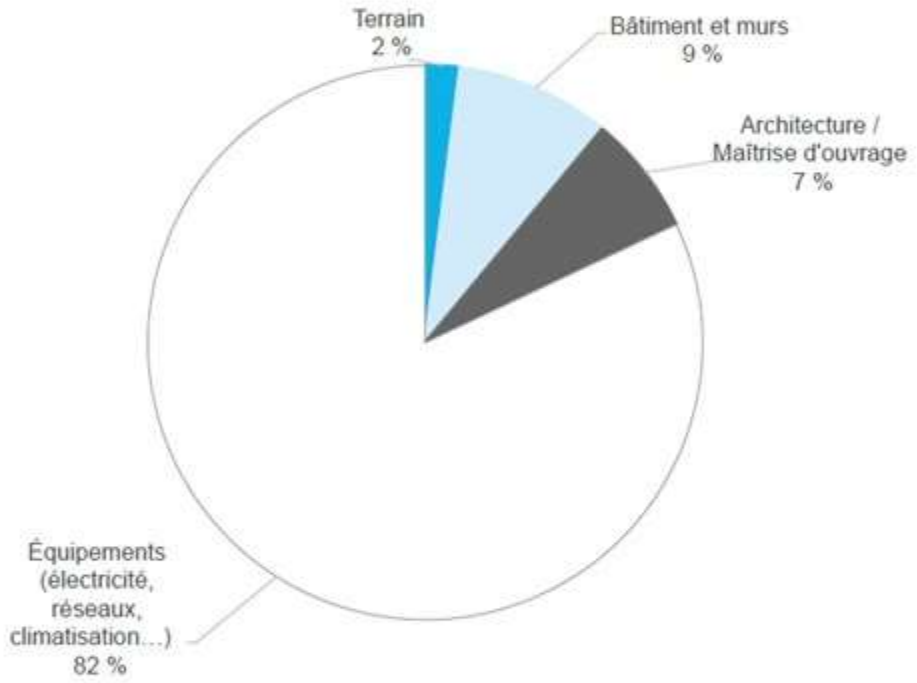
# Datacenter pour héberger des services numériques à haute disponibilité

**Datacenter = infrastructure au cœur des services numériques**

- **Salles sécurisées** pour accueillir les équipements informatiques (baies, serveurs applicatifs, serveurs de données, équipements réseaux interconnectant les serveurs (routeurs, pare-feu, répartiteurs et commutateurs)
- **Infrastructures techniques** (alimentation électrique, refroidissement des serveurs, accès réseaux THD très haut Débit )
- **Bâtiment spécialisée et sécurisé**



# Principaux postes de coûts d'un datacenter




Source : Les Echos / Microsoft

# Acteur spécialisés : Datacenters haute densité

- Acteurs spécialisés

interxion



TelecityGroup

# Nouveaux entrants français – offres de colocation (housing)

- CIV
- Cheops
- Energy4data

- Location d'une surface en m2 ou en nombre de baies

- Pas d'intervention sur la partie serveur ou services

- Le client est responsable

# Enjeux pour la mise en œuvre d'un datacenter

**La haute disponibilité**

**Disponibilité =Temps de disponibilité du service / Temps de disponibilité + d'indisponibilité du service**

La haute disponibilité est définie par ITIL2 comme « la caractéristique d'un service des Systèmes d'information qui minimise ou masque les effets d'une panne de composant sur les activités utilisateurs ». Un service en haute disponibilité doit donc rester continuellement disponible pour ses utilisateurs.

Pour assurer une « Haute disponibilité », il est important que les ressources nécessaires à la mise à disposition d'un service **puissent pallier toute défaillance**. Les Datacenters **dupliquent donc les infrastructures et incluent des mécanismes de redondance** permettant de basculer automatiquement les données et applications sur un site de repli en cas de défaillance du site principal.

## Efficacité énergétique d'un Datacenter

La performance d'un Datacenter est déterminée en fonction de la puissance énergétique mise à
disposition du client final par rapport à celle nécessaire à l'alimentation du Datacenter.
L'indice d'efficacité énergétique ou PUE en anglais (Power Usage Effectiveness) est utilisé pour
déterminer l'énergie réellement disponible pour les ressources informatiques. Il permet ainsi de
mesurer l'efficience énergétique d'un Datacenter et son empreinte écologique.

**PUE = Énergie totale consommée par le Datacenter / Énergie consommée par les serveurs informatiques**

En Europe, les Datacenters ont en moyenne un PUE de 2.

Les constructeurs sont engagés depuis 10 ans dans une course à la réduction des PUE pour
améliorer l'image écoresponsable de leurs équipements, mais surtout pour

# Enjeux critiques

## Continuité de l'alimentation électrique

- Pourquoi ?
  - Détériorations des serveurs hébergés
- Exigences
  - garantie de puissance électrique : le Datacenter doit avoir accès à un poste source4 permettant l'accès à un courant à haute tension de 20 kV ;

• **garantie de qualité de la tension électrique** : pour ne pas endommager les équipements électriques, la variation de la tension électrique ne doit pas excéder 2 %. Si les microcoupures peuvent être évitées par l'installation d'équipements palliatifs comme les onduleurs, la proximité du poste source est essentielle ;

• **garantie de continuité en cas de panne** : un Datacenter doit être alimenté par une double artère électrique, pour permettre le basculement automatique d'une source à l'autre en cas de panne. Le Datacenter doit enfin disposer **de générateur de secours** en capacité de produire sa propre énergie localement sur une durée minimale supérieure à la garantie de temps de rétablissement du fournisseur d'électricité.

## Maîtrise du froid

La distribution et la consommation d'énergie électrique par les équipements informatiques dégagent

beaucoup de chaleur. Dans un Datacenter, où la densité des équipements est importante,

la température dépasse rapidement les seuils recommandés pour le bon fonctionnement

des équipements.

**le refroidissement des** baies (armoires dans lesquelles sont rangés les équipements), réalisé par

pulsion d'air froid avec convection forcée ou/et refroidissements à eau

**l'optimisation de la circulation** de l'air dans le Datacenter, en alternant des allées chaudes et

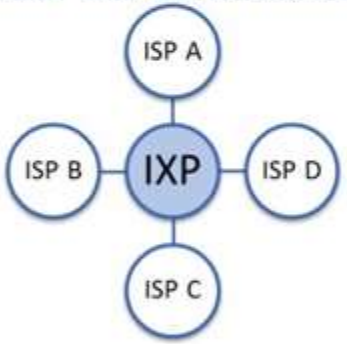
froides, pour proposer un refroidissement optimal

Ce poste de coût est un des plus importants, car la maintenance des équipements doit être

réalisée à une fréquence mensuelle

## Accès réseau

**Pour offrir une accessibilité optimale à ses clients, un Datacenter doit disposer d'une bande passante importante sur les réseaux des opérateurs. On privilégiera la proximité d'un pointd'échange interne pour implanter un Datacenter et bénéficier nexion avec un maxin ur un réseau Très Haut**




Lien direct

Service de peering

Source : http://www.internetexchangemap.com/

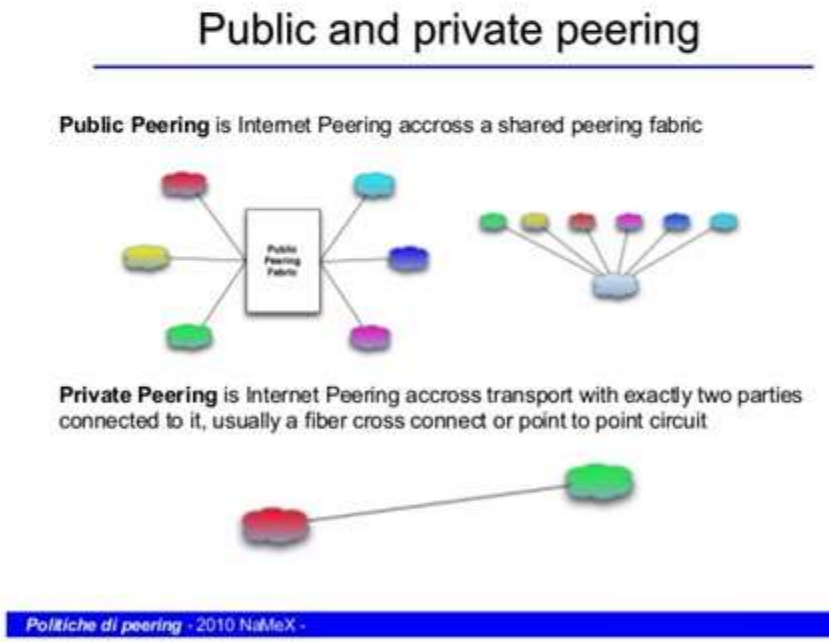
D'autres ressources sont également disponibles sur Internet :

- Euro-IX l'association Européenne des IXP : https://www.euro-ix.net/ixps/ixp-map/
- Wikipedia : https://en.wikipedia.org/wiki/List_of_Internet_exchange_points_by_size

Le peering consiste à échanger du trafic qui a son origine sur le réseau de l'un des opérateurs (ou de ses clients) et aboutit sur le réseau de l'autre (ou de l'un de ses clients) et ne fait généralement pas l'objet d'une facturation de l'un à l'autre.

## Bénéfices des points d'échanges internet (IXP)

- Optimisation du trafic mondial
- Optimisation de la latence (exemple ville de montréal – shodan – tracert 104.20.15.35)
- Optimisation de la bande passante
- Optimisation du coût (facturation)



# Classement des datacenters

| | TIER 1 | TIER 2 | TIER 3 | TIER 4 |
|---|---|---|---|---|
| Niveau de redondance | N | N+1 | N+1 | 2 (N+1) |
| Équipements électriques, climatiseurs et générateurs | ✗ Sans redondance | ✓ Redondance des composants critiques | ✓ Doublés ou plus | ✓ Doublés ou plus |
| Réseaux d'alimentation (électricité, refroidissement, communication) | ✗ Uniques | ✗ Uniques | ✓ Doublés ou plus (actif / passif) | ✓ Doublés ou plus (actif / actif) |
| Indépendance physique des composants de secours et des réseaux d'alimentation | ✗ Non | ✗ Non | ✗ Non | ✓ Oui, nécessite deux distributeurs d'électricité indépendants |
| Double alimentation des composants | ✗ Non | ✗ Non | ✓ Oui | ✓ Oui |
| Refroidissement continu | ✗ Non | ✗ Non | ✗ Non | ✓ Oui |
| Réserve pour les générateurs de secours | 12 heures | 12 heures | 12 heures | 12 heures |
| Temps d'arrêt annuel<br>Taux de disponibilité | 28,8 h<br>99,67 % | 22 h<br>99,75 % | 1,6 h<br>99,982 % | 0,4 h<br>99,995 % |

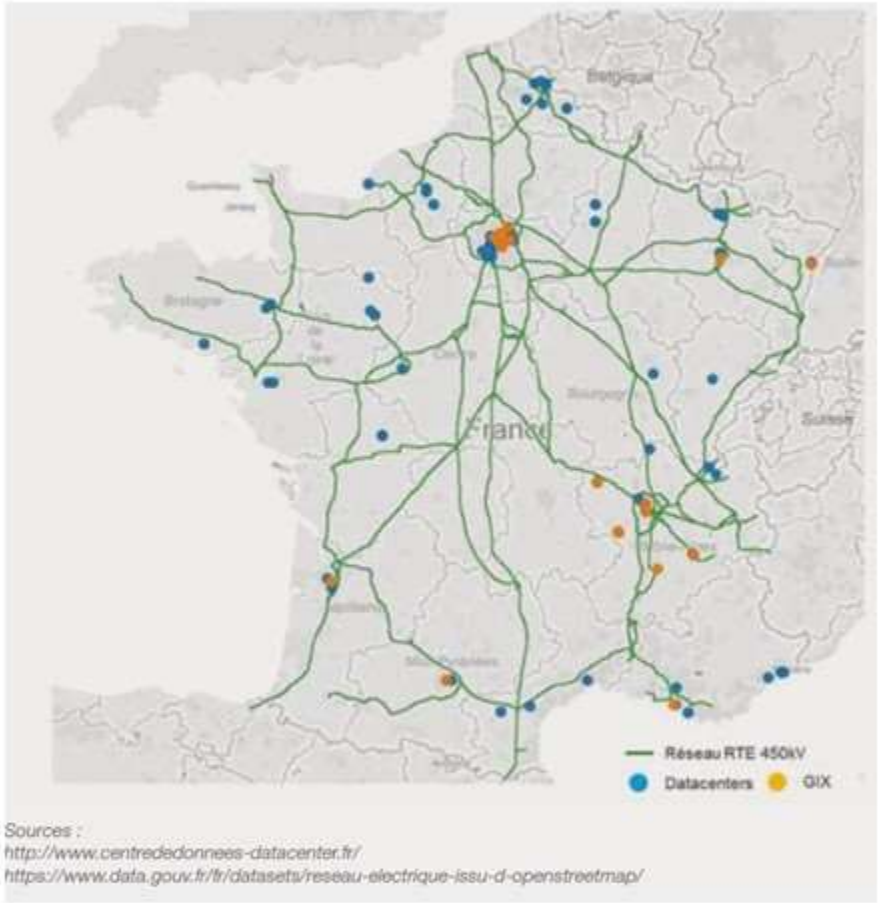
**Greenfield, Datacenter** privé de Crédit Agricole SA près de Chartres (TIER 4) ;

**DC3 d'Online**, filiale hébergement du groupe Iliad à Vitry-sur-Seine (TIER 3) ;

**Data Center Tours (DCT),** infrastructure privée de Gemalto, à Chambray-lès-Tours (TIER 3).

| Caractéristiques des Datacenters | TIER 2 | TIER 3 | TIER 3+ | TIER 4 | Non communiqué | TOTAL |
|---|---|---|---|---|---|---|
| Nombre de sites en France (Paris / Régions) | 5 | 56 | 21 | 8 | 47 | 137 |

# Implantation des datacenters conditionnés par le fournisseur RTE




*Sources :*
*http://www.centrededonnees-datacenter.fr/*
*https://www.data.gouv.fr/fr/datasets/reseau-electrique-issu-d-openstreetmap/*

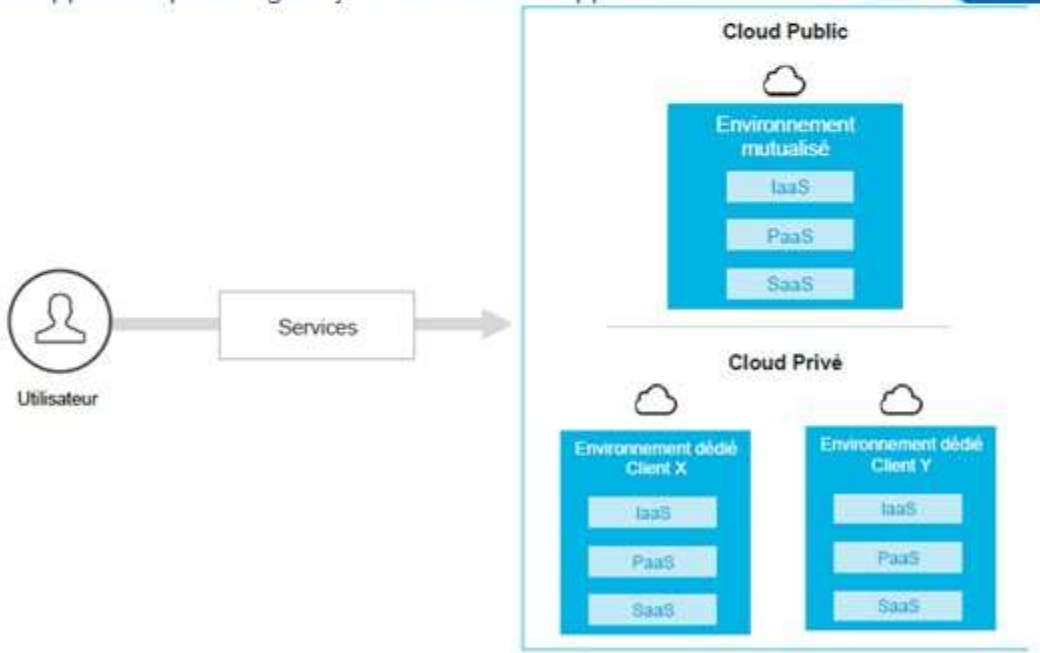
# Notre démarche

# Cloud computing – services hébergés dans des Datacenters

## Définition

Le Cloud computing est un modèle d'accès à travers le réseau internet à un ensemble de ressources numériques, pouvant être allouées et libérées à la demande et pour lesquelles le fournisseur du service assure l'ensemble des activités de maintenance, de support et d'exploitation

Ce modèle offre des services de différentes natures, allant des services d'infrastructure (location de capacités de stockage ou de calcul), des services de plateforme (location d'environnements de développement préconfigurés) ou de services d'applications (location d'applicatio

# Cloud Computing – fourniture de ressources informatiques

**une large accessibilité via le réseau** : les services sont accessibles en ligne et sur tout type de support (ordinateur de bureau, portable, smartphone, tablette

**mesurabilité du service :** l'utilisation du service par le client est supervisée et mesurée afin de pouvoir suivre le niveau de performance et facturer le client en fonction de sa consommation réelle

**une solution multitenant ou multiclient :** une même instance d'un logiciel est partagée par l'ensemble des clients de façon transparente et indépendante. Tous les clients utilisent la même version du logiciel et bénéficient instantanément des dernières mises à jour. Chaque client dispose d'un paramétrage utilisateur qui lui est propre

**une disponibilité à la demande** : le service peut être souscrit rapidement et rendu opérationnel automatiquement avec un minimum d'interaction avec le fournisseur

**l'élasticité immédiate des ressources :** des ressources supplémentaires peuvent être allouées au service pour assurer la continuité du service en cas de pic de charge, ou être bien réallouées à un autre service dans le cas inverse ;

# IaaS, PaaS et SaaS :

IaaS : Infrastructure as a Service

PaaS : Platform as a Service

SaaS : Software as a Service

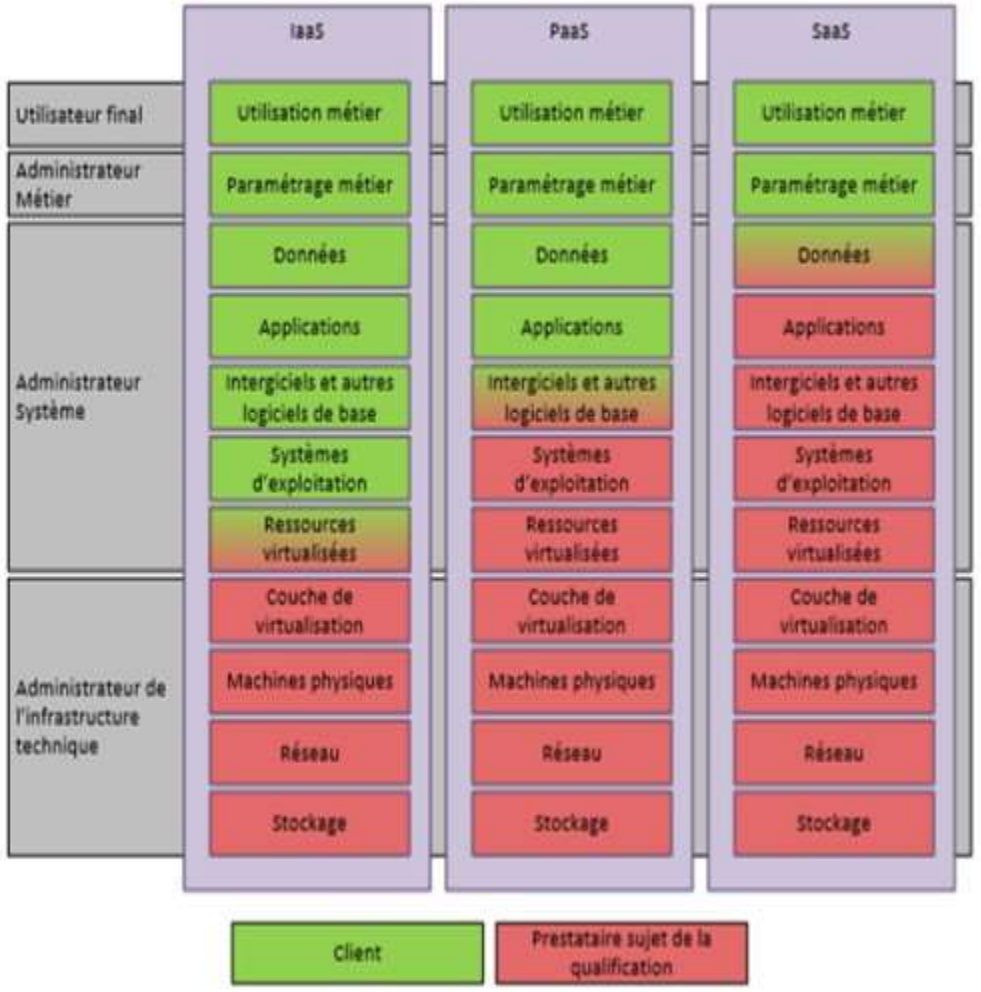



**Figure 1 - Répartition des responsabilités par type de service**

# IaaS Infrastructure as a service – des serveurs virtuels à la demande

**Location de capacité de calcul et de stockage**

**Mise à disposition par le fournisseur de ressources matérielles virtualisées** comprenant :

- la puissance de calcul ;
- les unités de stockage des données ;
- les réseaux ;
- les couches de virtualisation

**A charge du client les systèmes d'exploitation**

Le client prend en charge la gestion et l'exploitation de toutes les couches supérieures, *middlewares*,

bases de données, applications.

La souscription à une offre *IaaS* permet au client d'externaliser son parc matériel serveur et de

s'affranchir des compétences de conception et d'exploitation des infrastructures techniques

**Offre intermédiaire**

# PaaS – Platform as a Service, des plateformes de développement prêtes à l'emploi

**Mise à à disposition une plateforme middleware opérationnelle**, incluant des serveurs d'applications, des bases de données et les outils permettant au client de développer et de déployer ces propres applications

## Client – pour disposer de plateformes de développement

Cette configuration est très employée pour disposer de plateformes de développement ou de

tests disposant de l'ensemble des outils et middleware nécessaires, en évitant ainsi les taches

de construction et de maintenance de ces plateformes non critiques. Elle se destine donc naturellement

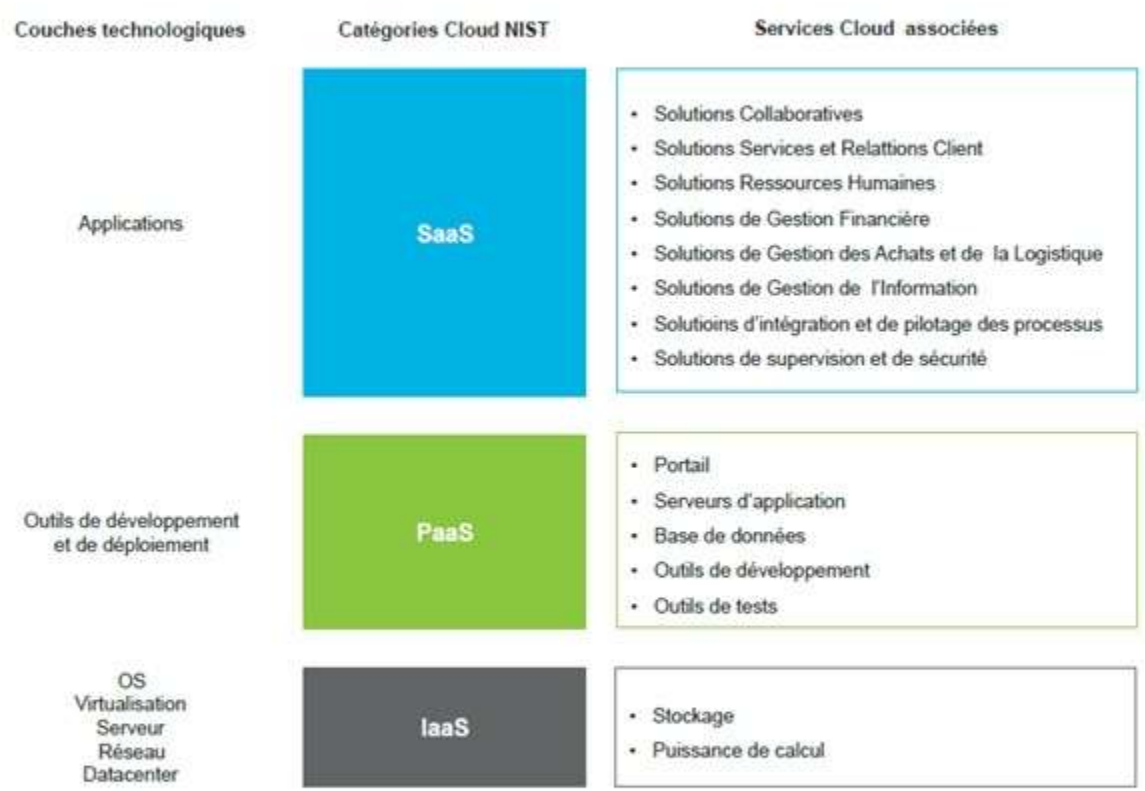
avant tout aux développeurs

# SaaS – Software as a Service, des services métiers à la demande

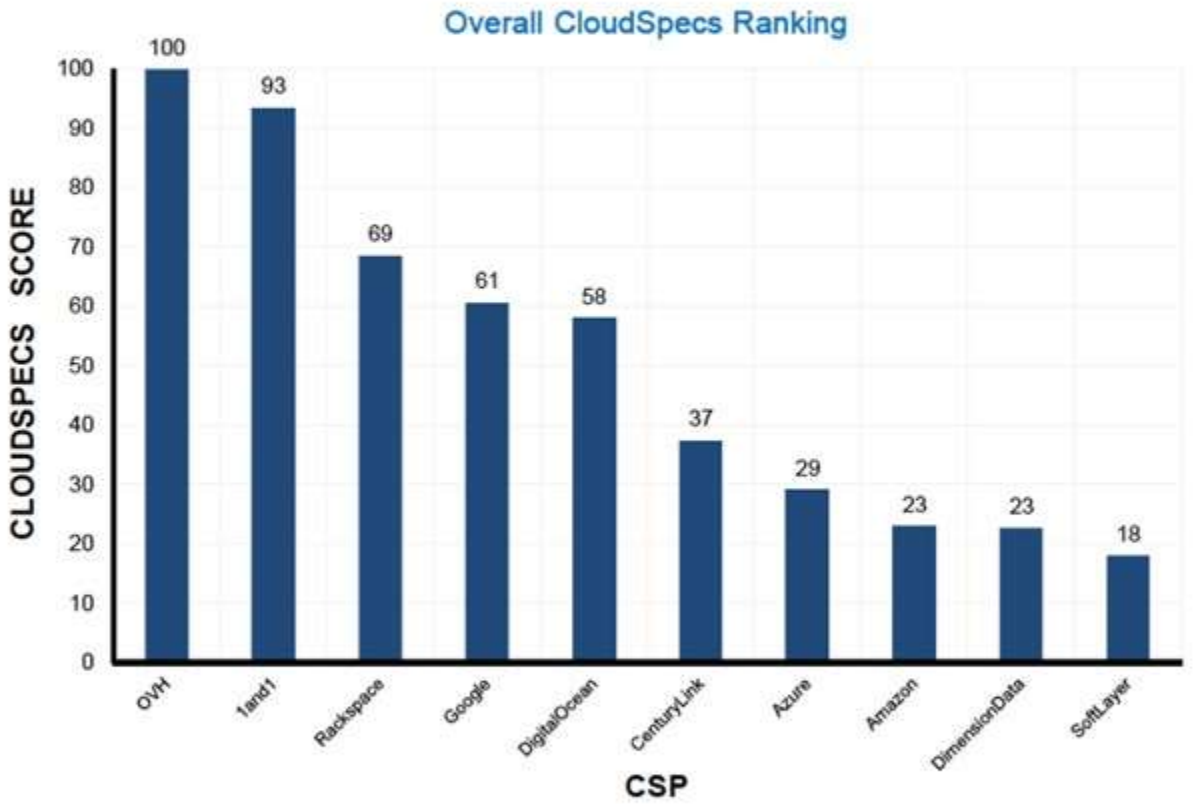
**Offre tout compris**

Le prestataire met à disposition une application qu'il administre et configure en majeure partie. Le client externalise ainsi ses applications (logiciels métiers ou solutions techniques à destination des DSI), auxquelles il accède à la demande.

Il paie à l'usage, selon le nombre d'utilisateurs et/ou le temps d'utilisation du logiciel.



# IaaS, PaaS et SaaS : des offres de services à valeur ajoutée


CSP CloudSpecs Price

# Cloud privé  Cloud public

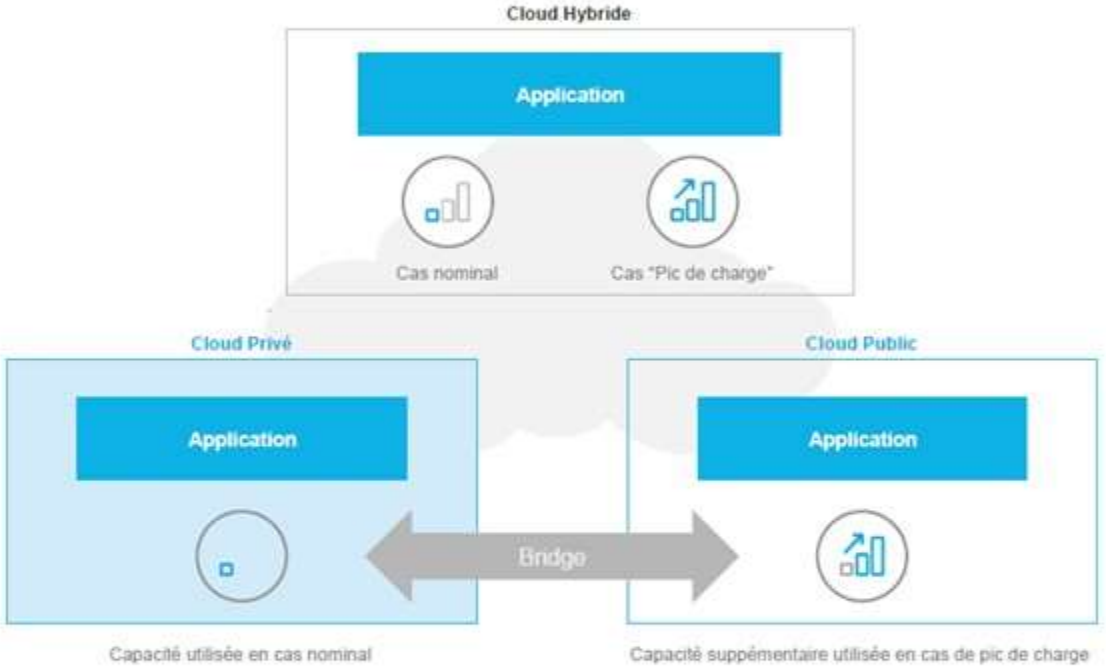
Selon le degré de mutualisation des ressources, on distingue plusieurs modes de déploiement, garantissant une réservation plus ou moins exclusive au client utilisateur des capacités physiques qui lui sont allouées. Dans tous ces modes, l'étanchéité entre les ressources allouées à chaque client est toujours
garantie.

Principales différences entre *Cloud* public et *Cloud* privé

| | ***Cloud* public** | ***Cloud* privé** |
|---|---|---|
| **Type d'infrastructure** | Environnement externe multilocatif | Environnement interne ou externe dédié au client |
| **Élasticité / disponibilité en capacité** | Illimitée (en théorie) | Limitée |
| **Allocation de ressources** | Immédiate | Immédiate dans la limite des capacités disponibles |
| **Localisation des données** | Dépend des partenaires du tiers fournissant le service en *Cloud* public | Définie par contrat |
| **Sécurité et niveaux de services** | Identiques pour tous les clients | Les niveaux d'exigences peuvent être définis de façon spécifique en fonction des besoins du client |
| **Coût à long terme** | Inférieur au coût d'un *Cloud* privé | Élevé en raison des niveaux de services spécifiques |

# Architecture hybride

*Figure 8 - Les architectures hybrides*




Le terme d'**Architecture hybride** s'applique également pour désigner les environnements hétérogènes mixant des ressources hébergées sur un environnement interne (ou parle de ressource on-premise ou à demeure) et un *Cloud* public ou plusieurs environnements *Cloud* public.

# Notre démarche

# Externalisation des systèmes d'information – gestion des risques

# Objectifs du guide

Faire prendre conscience aux décideurs informatiques des risques en matière de sécurité des systèmes d'information (SSI) liés à toute opération d'externalisation

Fournir une démarche cohérente de prise en compte des aspects SSI lors de la rédaction du cahier des charges d'une opération d'externalisation

Fournir un ensemble de clauses types ainsi qu'une base d'exigences de sécurité, à adapter et personnaliser en fonction du contexte particulier de chaque projet d'externalisation.

**Les publications de l'ANSSI sont diffusées sur son site Internet : http://www.ssi.gouv.fr/publications/**

# Risques liés à la perte de maîtrise de son SI

- **Risques liés à la sous-traitance** au sein d'un groupement d'entreprises répondant à un appel d'offres (co-traitance solidaire, sous-traitances déclarées)

- **Risques liés à la localisation des données (CID)**

  - **Réglementation RGPD** , autres obligations légales et réglementaires (Opérateurs d'importance vitale, santé publique)

  - **Obligations de sécurité physique et cyber sécurité**

  - **Localisation des données (infrastructures réparties) non maîtrisée**
    - difficulté à exercer un droit de regard et de contrôle sur les personnels du prestataire
    - difficulté à effectuer un audit de sécurité de l'infrastructure sous-jacente
    - difficulté à répondre à d'éventuelles injonctions de la justice, pour des raisons fiscales par exemple, ou d'autres raisons d'ordre juridique

# Risques liés à la perte de maîtrise de son SI

- **Risques liés aux données à caractère personnel**
  - **Responsabilité du titulaire des données** avec obligations de contrôle vis-à-vis du fournisseur
  - En effet, il faut garder à l'esprit que le donneur d'ordres, en tant que responsable de traitement, encourt des sanctions pénales en cas de non-respect des dispositions de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés

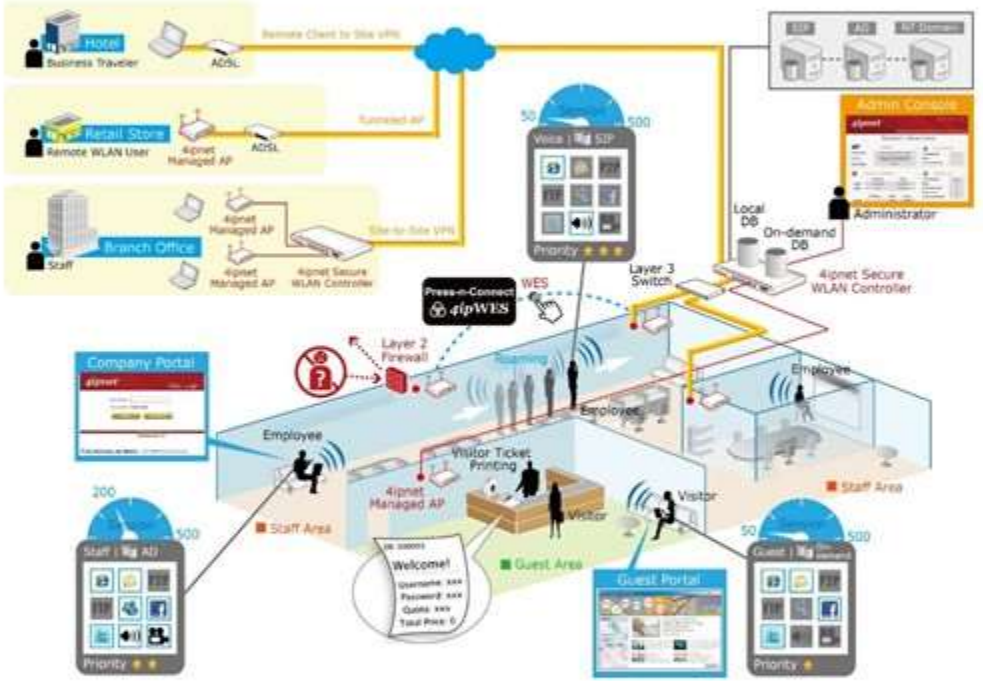
- **Risques liés aux choix techniques du prestataire**
  - Pour des raisons économiques d'où nécessité de valider les solutions proposées par le prestataire
  - Interopérabilité et format standard pour réversibilité, portabilté

# Risques liés aux accès à distance

**le télédiagnostic** : supervision d'équipements réseau et sécurité, diagnostic d'anomalies sur une application, etc.

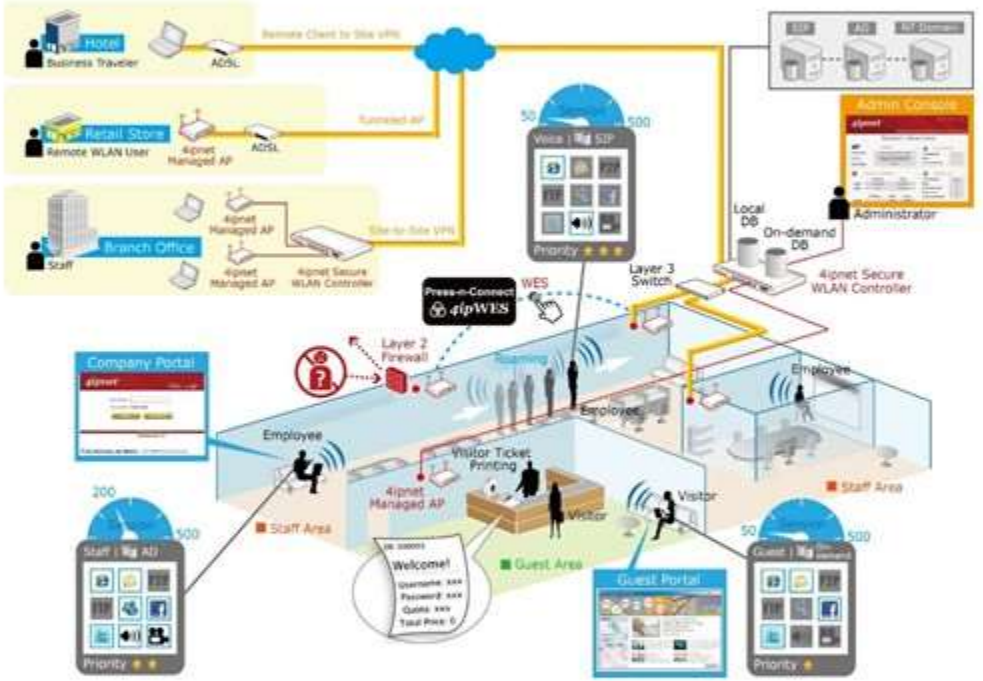
**la télémaintenance** : réalisation, après le diagnostic, des opérations à distance sur le dispositif

**la télédistribution** : mise à jour d'une application à distance



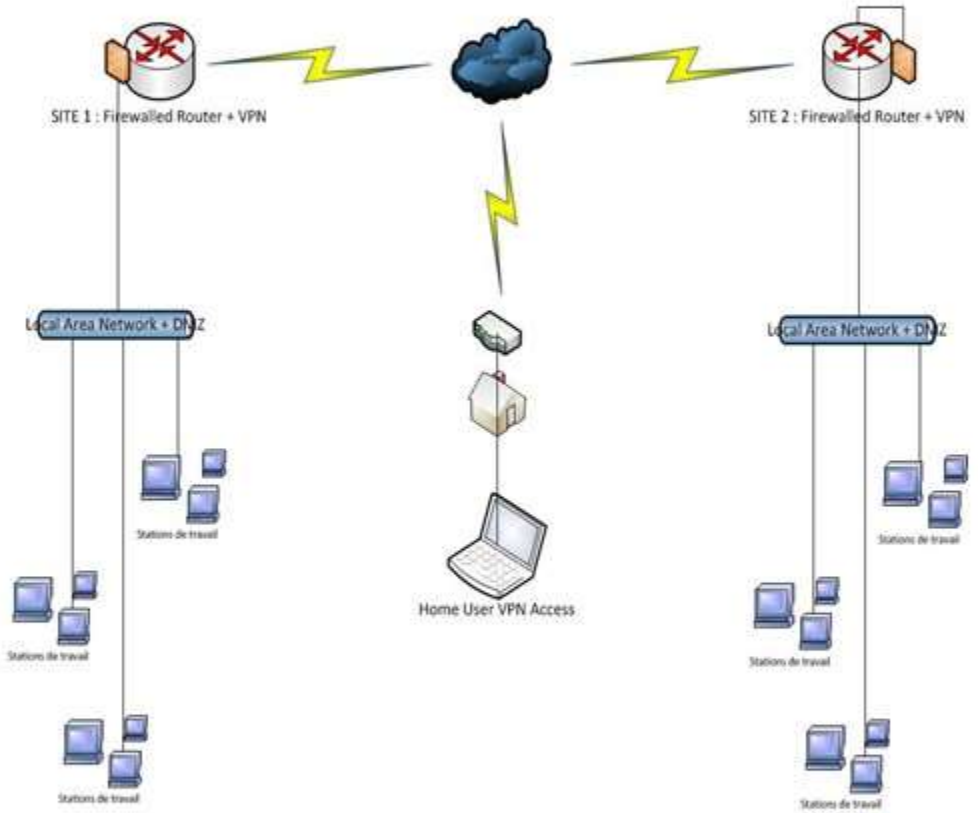
# Risques liés aux accès à distance

- **liaison établie de façon permanente** avec l'extérieur
- **mots de passe par défaut** (connus dans le monde entier) ou faibles
- **présence de failles** dans les interfaces d'accès
- **systèmes d'exploitation** des dispositifs non tenus à jour
- **absence de traçabilité** des actions
- **personnels responsables** de ces dispositifs non conscients des problèmes de sécurité ou mal formés
-
- **interconnexion de systèmes sécurisés** de confiance à des systèmes de niveau faible (internet par exemple).



# Mise en œuvre d'une solution sécurisée

- **authentifier** la machine distante et la personne en charge du support
- mettre en place une **politique de gestion des accès rigoureuses**
- **prévenir l'exploitation de vulnérabilités** ou de portes dérobées sur le dispositif de télémaintenance ;
- **garantir la confidentialité et l'intégrité des données** sur le SI
- assurer une **traçabilité de confiance des actions effectuées par le technicien du centre de support**
- **garantir l'innocuité de la fonction de télémaintenance** vis-à-vis du système faisant l'objet du télédiagnostic ainsi que des systèmes connexes
- **garantir l'absence de fuite d'informations** vers l'extérieur



# Risques inhérents à l'hébergement mutualisé

- **Perte de disponibilité : DDOS**
  - Problèmes si plusieurs services sont hébergés sur le même serveur (effets collatéraux)
  - Problème matériel côté héherbeur (cas d'une mise à jour par exemple , panne matérielle)

- **Perte d'intégrité**
  - Vulnérabilités (Spectre et Meldown) aboutissant à l'installation d'une porte dérobée, défiguration de site web, vol d'informations, rebond d'attaques  cryptomining
  - Changement d'un logiciel (voulu ou non) ayant une répercussion indirecte sur un service hébergé

- **Perte de confidentialité**
  - Partage de services dans un même environnement physique peut aboutit à des croisements d'information (contenu des fichiers clients de plusieurs sites dans la même base de données  ex ants –immatriculation)
  - Contrôle des accès par du personnel du fournisseur

## Prestataires de services d'informatique en nuage (SecNumCloud)
## Synthèse du référentiel d'exigences – niveau Essentiel

L'approche consistant à contractualiser au cas par cas la sécurité dans chaque projet de mise en nuage montre ses limites, les offres étant le plus souvent packagées ; de plus, il est également illusoire d'inciter chaque client à procéder à des audits réguliers des services offerts.

Une approche unifiée autour d'un référentiel a été préférée, favorisant ainsi l'émergence et la promotion d'offres qualifiées, les offreurs disposant d'un cadre stable dans lequel s'inscrire pour aller vers la qualification et les usagers pouvant baser leur confiance sur cette qualification.

Le référentiel de qualification de prestataires proposant une offre de services en nuage couvre les trois types d'activité (SaaS, PaaS et IaaS).

Les exigences, déclinées en 19 chapitres, sont relatives au prestataire et portent notamment sur le contrôle d'accès et gestion des identités, la cryptologie, la sécurité liée à l'exploitation et la gestion des incidents liés à la sécurité de l'information. Ces exigences seront vérifiées par une évaluation documentaire, organisationnelle, physique et technique des processus, infrastructures et lieux liés à la prestation visée par la qualification.

# Contrôle d'accès et gestion des identités

- **Politique et gestion d'accès** (cloisonnement, droit à en connaître, procédures entrant / sortants)

- **Enregistrement et désinscription des utilisateurs** (procédure via une interface de gestion des comptes et des droits d'accès)

- **Revue et contrôle planifié des droits d'accès utilisateurs**

- **Gestion des authentifications des utilisateurs**
  - la gestion des moyens d'authentification (émission et réinitialisation de mot de passe, mise à jour des CRL et import des certificats racines en cas d'utilisation de certificats, etc.). - > authentification à multiples facteurs
  - la mise en place des moyens permettant une authentification à multiples facteurs afin de répondre aux différents cas d'usage du référentiel
  - les systèmes qui génèrent des mots de passe ou vérifient leur robustesse, lorsqu'une authentification par mot de passe est utilisée. Ils doivent suivre les recommandations de [NT_MDP]. b) Tout mécanisme d'authentification doit prévoir le blocage d'un compte après un nombre limité de tentatives infructueuses.

# Sécurité de l'information – fonction, formation, communication

- **Documentation à jour** sur l'organisation interne (RACI)
  - Un responsable de la sécurité des systèmes d'information
  - Un responsable de la sécurité physique

- **Procédures claires pour coopération avec les autorités**
  - Sécurité de l'information
  - Protection des données à caractère personnel

- **Sécurité des ressources humaines**
  - Embauche (casier judiciaire, signature charte éthique, respect charte informatique)
  - Sensibilisation, apprentissage et formation à la sécurité de l'information (plan de formation adapté aux besoins)
  - Processus disciplinaire en cas d'infraction aux règles (connues et respectées)
  - Rupture, terme ou modification du contrat de travail
    - Gestion des arrivées et départ ( messagerie, mots de passe, accès distants, etc)

# Gestion des actifs

- **Inventaire et propriétés des actifs à jour**
  - les informations d'identification de l'équipement (nom, adresse IP, adresse MAC, etc.) ;
  - la fonction de l'équipement ;
  - le modèle de l'équipement ;
  - la localisation de l'équipement ;
  - le propriétaire de l'équipement ;
  - le besoin de sécurité des informations
  -
- **Restitution des actifs en fin de contrat (réversibilité)**

Le prestataire doit documenter et mettre en œuvre une procédure de restitution des actifs permettant de s'assurer que chaque personne impliquée dans la fourniture du service restitue l'ensemble des actifs en sa possession à la fin de sa période d'emploi ou de son contrat

- Prise en compte des besoins en sécurité (cas d'information sensible de l'entreprise : hôpital, PI)

# Cryptologie

- **Chiffrement des données stockées**
  - Protection de récupération des données clients en cas de réallocation d'une ressource physique ou de remplacement de cette dernière
  - Chiffrement suivant les recommandations de l'ANSSI

- Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr

- **Chiffrement des flux**
  - **Protocole TLS** : Le protocole TLS1 est une des solutions les plus répandues pour la protection des flux réseau. Dans ce modèle client–serveur, les données applicatives sont encapsulées de manière à assurer la confidentialité et l'intégrité des échanges. Le serveur est nécessairement authentifié, et des fonctions additionnelles permettent l'authentification du client lorsqu'un tel besoin a été identifié.

  - **Protocole IPSEC** : IPsec est une suite de protocoles de communication sécurisée permettant la protection des flux réseau. Elle est éprouvée, mais souvent mal maîtrisée et reste encore trop peu ou mal employée.

  - **Protocole SSH**,ou Secure SHell,est unprotocole applicatif(couche7dumodèledel'OSI)qui vise à corrigerles déficiences connue s dans les protocoles FTP, RSH, RCP et TELNET

# Cloud et RGPD

L'entrée en vigueur du nouveau Règlement Général de Protection des Données (RGPD) , prévue en 2017 par la Commission Européenne, amènera à une revue des contrats cloud. Traitant notamment de la confidentialité des données dans le cloud, cette directive engage les DSI qui se doivent de vérifier la localisation de celles-ci et la réglementation applicable au cas par cas avec tous leurs fournisseurs

## Services cloud, sécurité et confidentialité

Nécessité de vérifier que toutes les obligations réglementaires et les pratiques de sécurité appliquées dans l'organisation sont appliquées à l'identique par ses fournisseurs. Des garanties supplémentaires et des contrôles sont requis pour assurer la protection du patrimoine de données qui est remis entre les mains de ces parties tierces.

## Evaluations des risques spécifiques aux services du cloud

Liste des parties impliquées, rôles et responsabilités (entreprise- fournisseur)

Localisation des datacenters où sont stockées les données ou fournis les services

Engagements contractuels entre le contrôleur de l'entreprise cliente et le fournisseur de traitement dans le cloud

# Cloud et RGPD

En raison des implications figurant dans le nouveau Règlement Général de la Protection des Données (RGPD), la plupart des organisations globales utilisant des services cloud devront suivre d'une façon ou d'une autre les recommandations de cette loi. La conséquence la plus directe de son application est que **autant les clients que les fournisseurs auront des responsabilités accrues dans l'accomplissement de leurs obligations, quoi que, d'après l'art. 22, les entreprises clientes resteront les seules finalement responsables et devront vérifier que les activités de traitement numérique sont effectuées en accord avec la réglementation.**

# Références

- Guide sur le Cloud Computing et les Datacenters à l'attention des collectivités locales DGE – Caisse des Dépôts – cget
- Prestataires de services d'informatique en nuage (SecNumCloud) référentiel d'exigences – niveau Essentiel

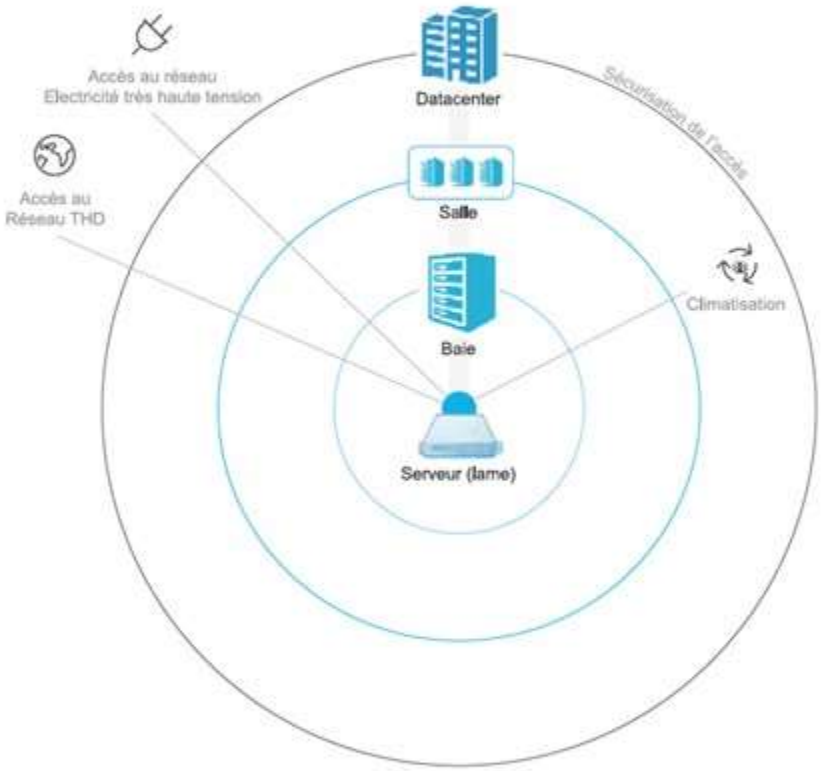
Version 3.0 du 8 décembre 2016


DATA CENTER
CLOUD COMPUTING
RISQUES INFOGERANCE

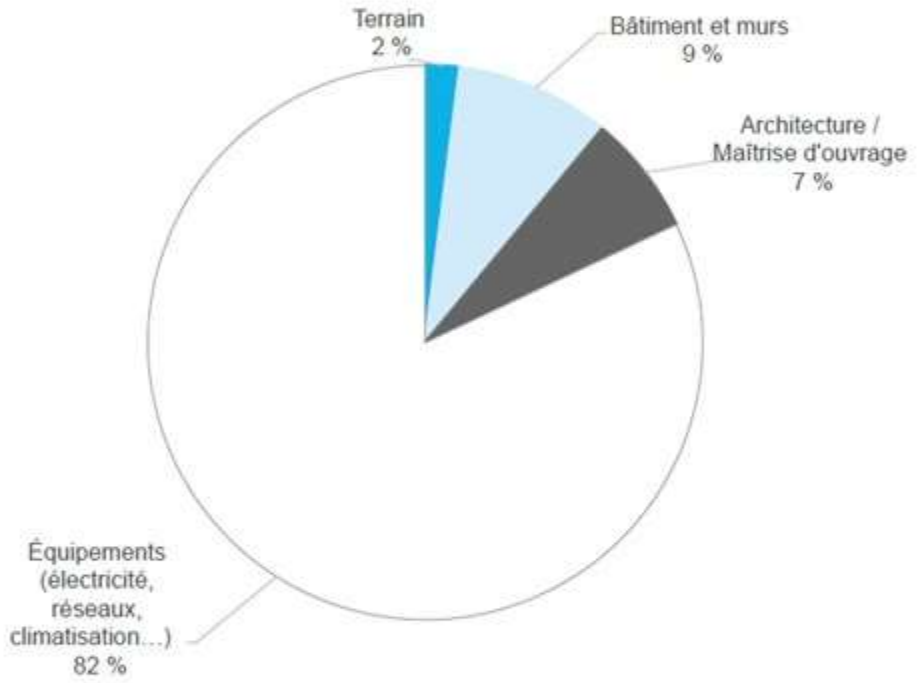
# Datacenter pour héberger des services numériques à haute disponibilité

**Datacenter = infrastructure au cœur des services numériques**

- **Salles sécurisées** pour accueillir les équipements informatiques (baies, serveurs applicatifs, serveurs de données, équipements réseaux interconnectant les serveurs (routeurs, pare-feu, répartiteurs et commutateurs)
- **Infrastructures techniques** (alimentation électrique, refroidissement des serveurs, accès réseaux THD très haut Débit )
- **Bâtiment spécialisée et sécurisé**



# Principaux postes de coûts d'un datacenter




Source : Les Echos / Microsoft

# Acteur spécialisés : Datacenters haute densité

- Acteurs spécialisés

interxion



TelecityGroup

# Nouveaux entrants français – offres de colocation (housing)

- CIV
- Cheops
- Energy4data

- Location d'une surface en m2 ou en nombre de baies

- Pas d'intervention sur la partie serveur ou services

- Le client est responsable

# Enjeux pour la mise en œuvre d'un datacenter

**La haute disponibilité**

**Disponibilité =Temps de disponibilité du service / Temps de disponibilité + d'indisponibilité du service**

La haute disponibilité est définie par ITIL2 comme « la caractéristique d'un service des Systèmes d'information qui minimise ou masque les effets d'une panne de composant sur les activités utilisateurs ». Un service en haute disponibilité doit donc rester continuellement disponible pour ses utilisateurs.

Pour assurer une « Haute disponibilité », il est important que les ressources nécessaires à la mise à disposition d'un service **puissent pallier toute défaillance**. Les Datacenters **dupliquent donc les infrastructures et incluent des mécanismes de redondance** permettant de basculer automatiquement les données et applications sur un site de repli en cas de défaillance du site principal.

## Efficacité énergétique d'un Datacenter

La performance d'un Datacenter est déterminée en fonction de la puissance énergétique mise à
disposition du client final par rapport à celle nécessaire à l'alimentation du Datacenter.
L'indice d'efficacité énergétique ou PUE en anglais (Power Usage Effectiveness) est utilisé pour
déterminer l'énergie réellement disponible pour les ressources informatiques. Il permet ainsi de
mesurer l'efficience énergétique d'un Datacenter et son empreinte écologique.

**PUE = Énergie totale consommée par le Datacenter / Énergie consommée par les serveurs informatiques**

En Europe, les Datacenters ont en moyenne un PUE de 2.

Les constructeurs sont engagés depuis 10 ans dans une course à la réduction des PUE pour
améliorer l'image écoresponsable de leurs équipements, mais surtout pour

# Enjeux critiques

## Continuité de l'alimentation électrique

- Pourquoi ?
  - Détériorations des serveurs hébergés
- Exigences
  - garantie de puissance électrique : le Datacenter doit avoir accès à un poste source4 permettant l'accès à un courant à haute tension de 20 kV ;

• **garantie de qualité de la tension électrique** : pour ne pas endommager les équipements électriques, la variation de la tension électrique ne doit pas excéder 2 %. Si les microcoupures peuvent être évitées par l'installation d'équipements palliatifs comme les onduleurs, la proximité du poste source est essentielle ;

• **garantie de continuité en cas de panne** : un Datacenter doit être alimenté par une double artère électrique, pour permettre le basculement automatique d'une source à l'autre en cas de panne. Le Datacenter doit enfin disposer **de générateur de secours** en capacité de produire sa propre énergie localement sur une durée minimale supérieure à la garantie de temps de rétablissement du fournisseur d'électricité.

## Maîtrise du froid

La distribution et la consommation d'énergie électrique par les équipements informatiques dégagent

beaucoup de chaleur. Dans un Datacenter, où la densité des équipements est importante,

la température dépasse rapidement les seuils recommandés pour le bon fonctionnement

des équipements.

**le refroidissement des** baies (armoires dans lesquelles sont rangés les équipements), réalisé par

pulsion d'air froid avec convection forcée ou/et refroidissements à eau

**l'optimisation de la circulation** de l'air dans le Datacenter, en alternant des allées chaudes et

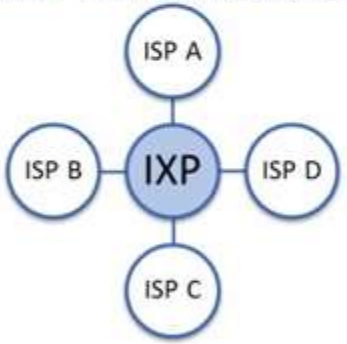
froides, pour proposer un refroidissement optimal

Ce poste de coût est un des plus importants, car la maintenance des équipements doit être

réalisée à une fréquence mensuelle

## Accès réseau

**Pour offrir une accessibilité optimale à ses clients, un Datacenter doit disposer d'une bande passante importante sur les réseaux des opérateurs. On privilégiera la proximité d'un pointd'échange interne pour implanter un Datacenter et bénéficier nexion avec un maxin ur un réseau Très Haut**




Lien direct

Service de peering

Source : http://www.internetexchangemap.com/

D'autres ressources sont également disponibles sur Internet :

- Euro-IX l'association Européenne des IXP : https://www.euro-ix.net/ixps/ixp-map/
- Wikipedia : https://en.wikipedia.org/wiki/List_of_Internet_exchange_points_by_size

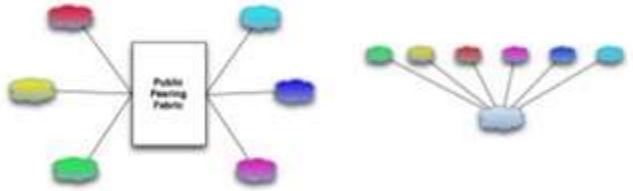
Le peering consiste à échanger du trafic qui a son origine sur le réseau de l'un des opérateurs (ou de ses clients) et aboutit sur le réseau de l'autre (ou de l'un de ses clients) et ne fait généralement pas l'objet d'une facturation de l'un à l'autre.

## Bénéfices des points d'échanges internet (IXP)

- Optimisation du trafic mondial
- Optimisation de la latence (exemple ville de montréal – shodan – tracert 104.20.15.35)
- Optimisation de la bande passante
- Optimisation du coût (facturation)

### Public and private peering

**Public Peering** is Internet Peering accross a shared peering fabric



**Private Peering** is Internet Peering accross transport with exactly two parties connected to it, usually a fiber cross connect or point to point circuit

*Politiche di peering* - 2010 NaMeX - 28

# Classement des datacenters

| | TIER 1 | TIER 2 | TIER 3 | TIER 4 |
|---|---|---|---|---|
| Niveau de redondance | N | N+1 | N+1 | 2 (N+1) |
| Équipements électriques, climatiseurs et générateurs | ✗ Sans redondance | ✓ Redondance des composants critiques | ✓ Doublés ou plus | ✓ Doublés ou plus |
| Réseaux d'alimentation (électricité, refroidissement, communication) | ✗ Uniques | ✗ Uniques | ✓ Doublés ou plus (actif / passif) | ✓ Doublés ou plus (actif / actif) |
| Indépendance physique des composants de secours et des réseaux d'alimentation | ✗ Non | ✗ Non | ✗ Non | ✓ Oui, nécessite deux distributeurs d'électricité indépendants |
| Double alimentation des composants | ✗ Non | ✗ Non | ✓ Oui | ✓ Oui |
| Refroidissement continu | ✗ Non | ✗ Non | ✗ Non | ✓ Oui |
| Réserve pour les générateurs de secours | 12 heures | 12 heures | 12 heures | 12 heures |
| Temps d'arrêt annuel<br>Taux de disponibilité | 28,8 h<br>99,67 % | 22 h<br>99,75 % | 1,6 h<br>99,982 % | 0,4 h<br>99,995 % |

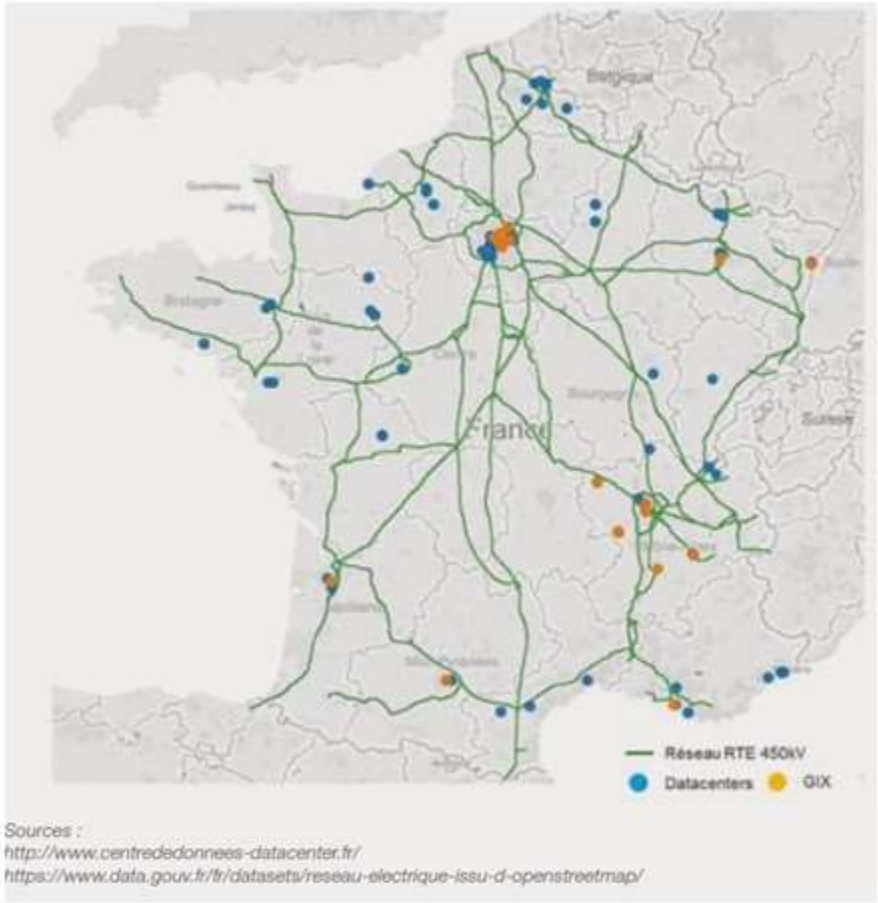
**Greenfield, Datacenter** privé de Crédit Agricole SA près de Chartres (TIER 4) ;

**DC3 d'Online**, filiale hébergement du groupe Iliad à Vitry-sur-Seine (TIER 3) ;

**Data Center Tours (DCT),** infrastructure privée de Gemalto, à Chambray-lès-Tours (TIER 3).

| Caractéristiques des Datacenters | TIER 2 | TIER 3 | TIER 3+ | TIER 4 | Non communiqué | TOTAL |
|---|---|---|---|---|---|---|
| Nombre de sites en France (Paris / Régions) | 5 | 56 | 21 | 8 | 47 | 137 |

# Implantation des datacenters conditionnés par le fournisseur RTE




*Sources :*
*http://www.centrededonnees-datacenter.fr/*
*https://www.data.gouv.fr/fr/datasets/reseau-electrique-issu-d-openstreetmap/*

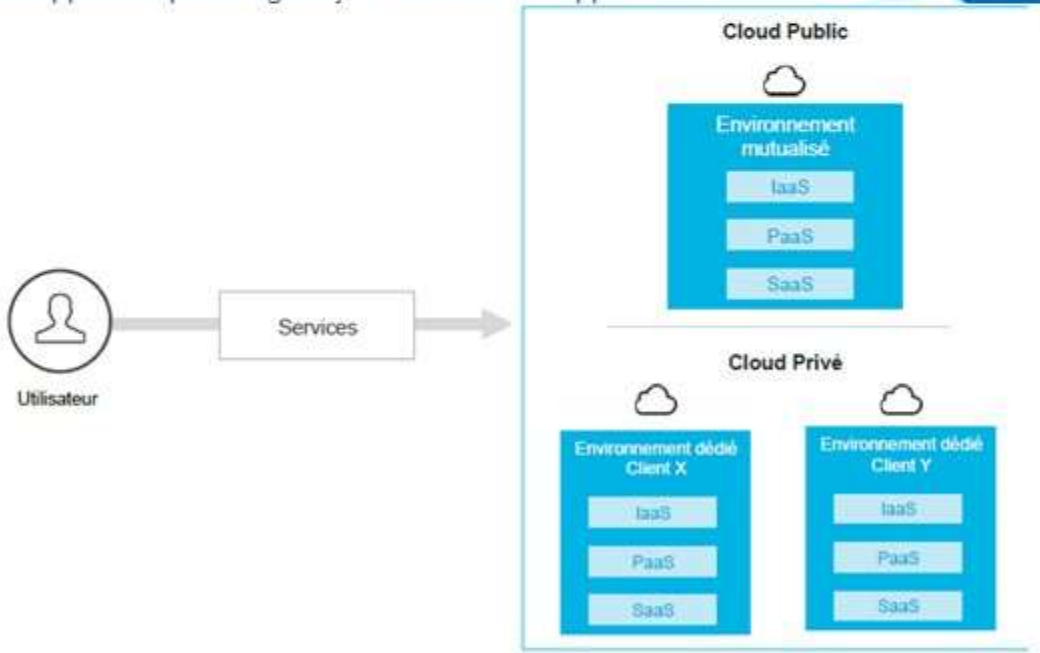
# Notre démarche

# Cloud computing – services hébergés dans des Datacenters

## Définition

Le Cloud computing est un modèle d'accès à travers le réseau internet à un ensemble de ressources numériques, pouvant être allouées et libérées à la demande et pour lesquelles le fournisseur du service assure l'ensemble des activités de maintenance, de support et d'exploitation

Ce modèle offre des services de différentes natures, allant des services d'infrastructure (location de capacités de stockage ou de calcul), des services de plateforme (location d'environnements de développement préconfigurés) ou de services d'applications (location d'applicatio

# Cloud Computing – fourniture de ressources informatiques

**une large accessibilité via le réseau** : les services sont accessibles en ligne et sur tout type de support (ordinateur de bureau, portable, smartphone, tablette

**mesurabilité du service :** l'utilisation du service par le client est supervisée et mesurée afin de pouvoir suivre le niveau de performance et facturer le client en fonction de sa consommation réelle

**une solution multitenant ou multiclient :** une même instance d'un logiciel est partagée par l'ensemble des clients de façon transparente et indépendante. Tous les clients utilisent la même version du logiciel et bénéficient instantanément des dernières mises à jour. Chaque client dispose d'un paramétrage utilisateur qui lui est propre

**une disponibilité à la demande** : le service peut être souscrit rapidement et rendu opérationnel automatiquement avec un minimum d'interaction avec le fournisseur

**l'élasticité immédiate des ressources :** des ressources supplémentaires peuvent être allouées au service pour assurer la continuité du service en cas de pic de charge, et être bien réallouées à un autre service dans le cas inverse ;

# IaaS, PaaS et SaaS :

IaaS : Infrastructure as a Service

PaaS : Platform as a Service

SaaS : Software as a Service

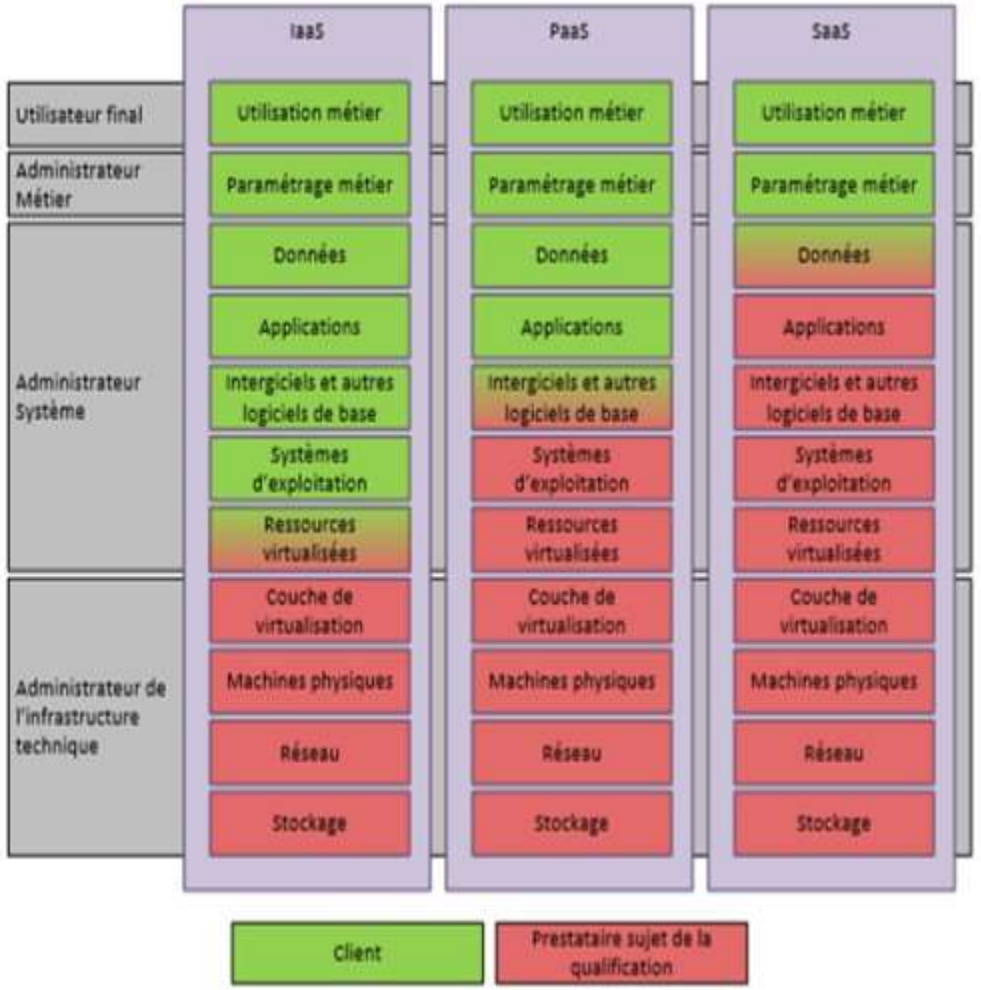



**Figure 1 - Répartition des responsabilités par type de service**

# IaaS Infrastructure as a service – des serveurs virtuels à la demande

**Location de capacité de calcul et de stockage**

**Mise à disposition par le fournisseur de ressources matérielles virtualisées** comprenant :

- la puissance de calcul ;
- les unités de stockage des données ;
- les réseaux ;
- les couches de virtualisation

**A charge du client les systèmes d'exploitation**

Le client prend en charge la gestion et l'exploitation de toutes les couches supérieures, *middlewares*,

bases de données, applications.

La souscription à une offre *IaaS* permet au client d'externaliser son parc matériel serveur et de

s'affranchir des compétences de conception et d'exploitation des infrastructures techniques

## Offre intermédiaire

# PaaS – Platform as a Service, des plateformes de développement prêtes à l'emploi

**Mise à à disposition une plateforme middleware opérationnelle**, incluant des serveurs d'applications, des bases de données et les outils permettant au client de développer et de déployer ces propres applications

### Client – pour disposer de plateformes de développement

Cette configuration est très employée pour disposer de plateformes de développement ou de

tests disposant de l'ensemble des outils et middleware nécessaires, en évitant ainsi les taches

de construction et de maintenance de ces plateformes non critiques. Elle se destine donc naturellement

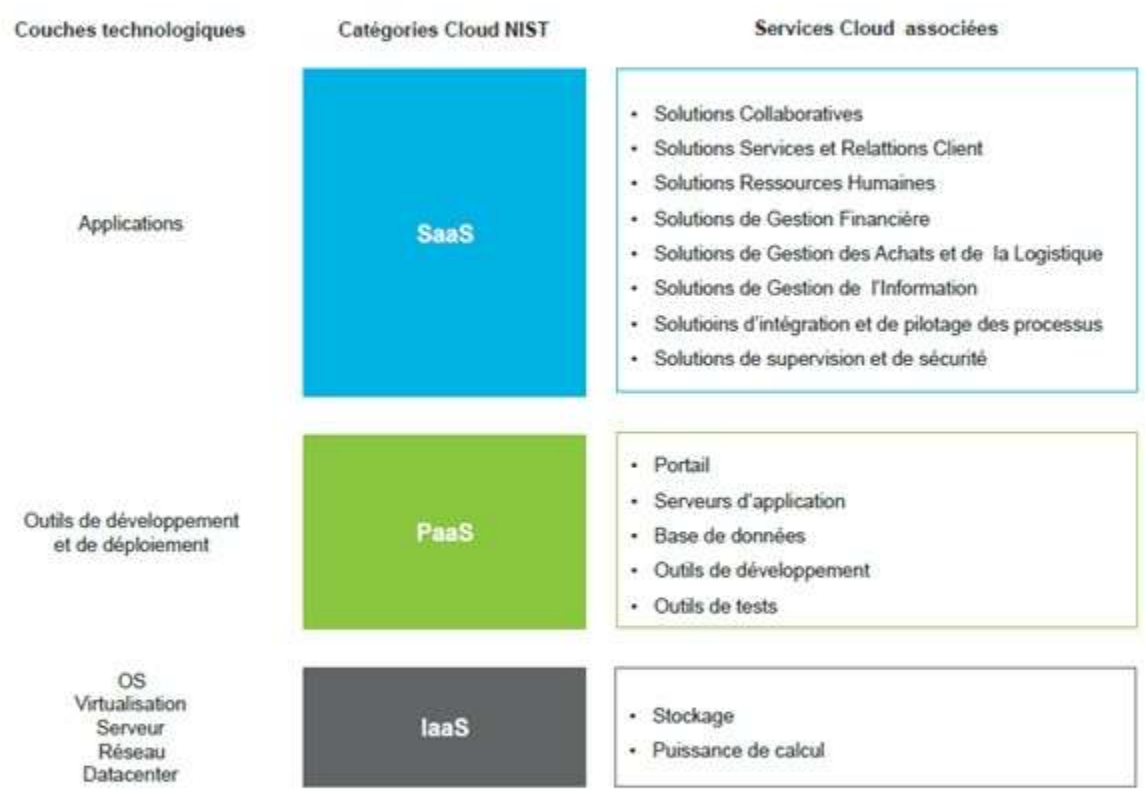
avant tout aux développeurs

# SaaS – Software as a Service, des services métiers à la demande

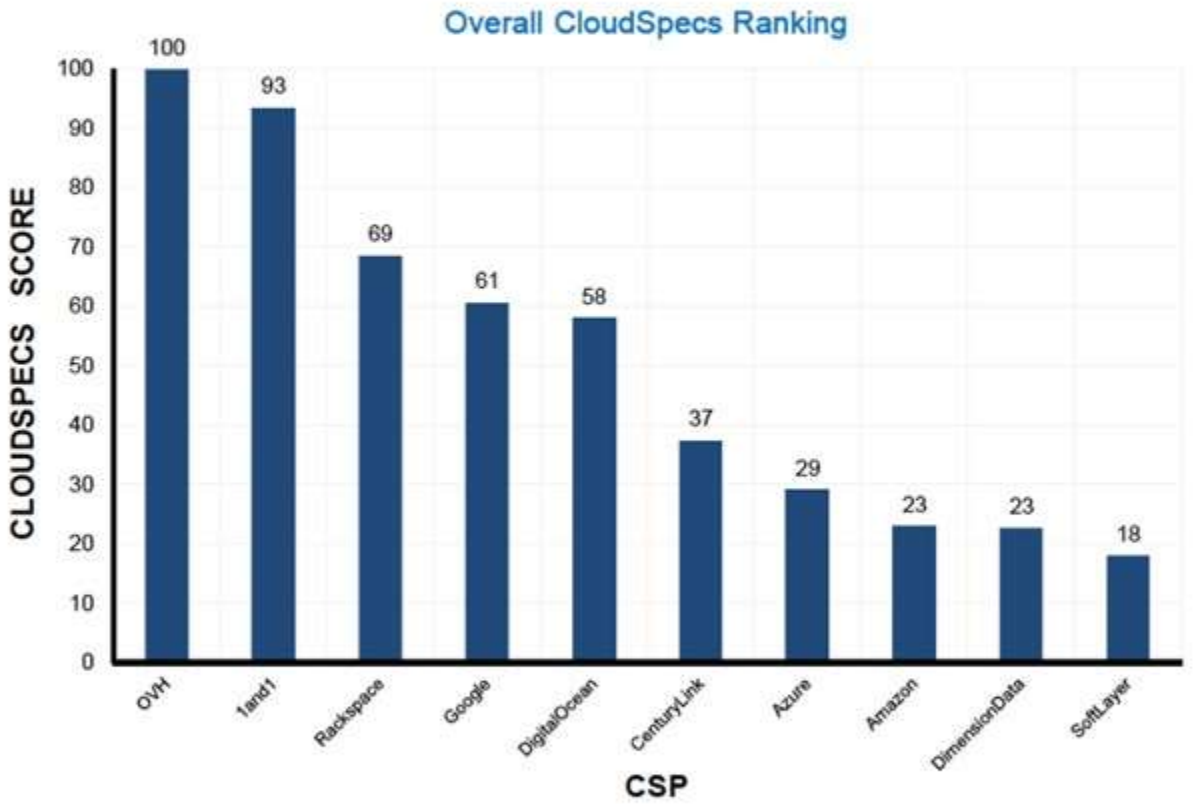
**Offre tout compris**

Le prestataire met à disposition une application qu'il administre et configure en majeure partie. Le client externalise ainsi ses applications (logiciels métiers ou solutions techniques à destination des DSI), auxquelles il accède à la demande.

Il paie à l'usage, selon le nombre d'utilisateurs et/ou le temps d'utilisation du logiciel.



# IaaS, PaaS et SaaS : des offres de services à valeur ajoutée


CSP CloudSpecs Price

# Cloud privé  Cloud public

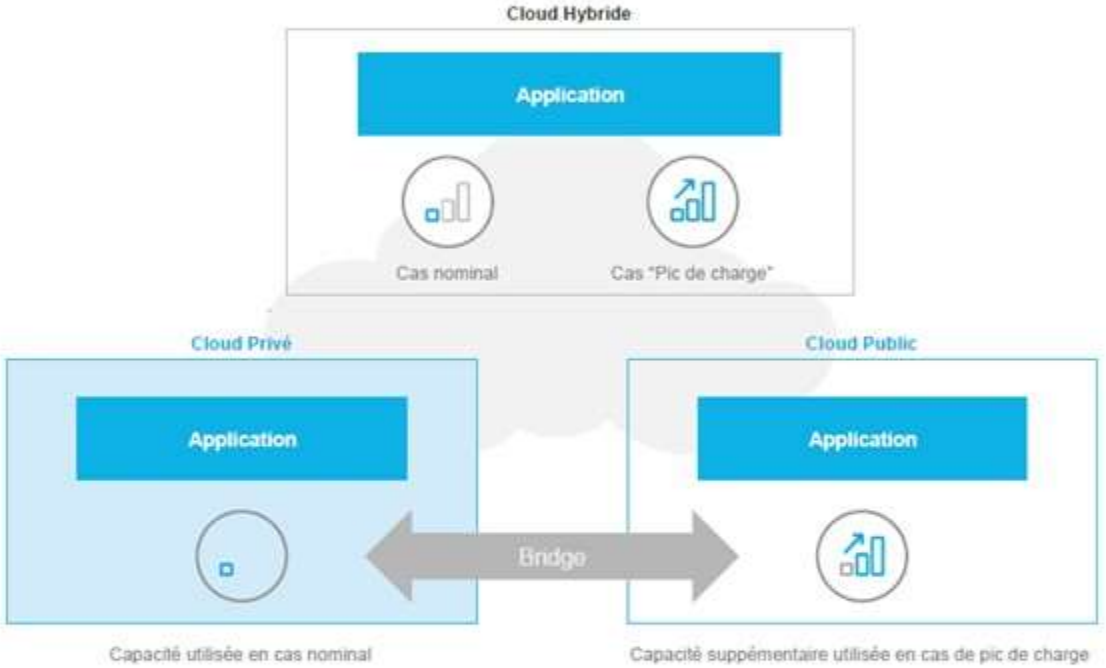
Selon le degré de mutualisation des ressources, on distingue plusieurs modes de déploiement, garantissant une réservation plus ou moins exclusive au client utilisateur des capacités physiques qui lui sont allouées. Dans tous ces modes, l'étanchéité entre les ressources allouées à chaque client est toujours
garantie.

Principales différences entre *Cloud* public et *Cloud* privé

| | ***Cloud* public** | ***Cloud* privé** |
|---|---|---|
| **Type d'infrastructure** | Environnement externe multilocatif | Environnement interne ou externe dédié au client |
| **Élasticité / disponibilité en capacité** | Illimitée (en théorie) | Limitée |
| **Allocation de ressources** | Immédiate | Immédiate dans la limite des capacités disponibles |
| **Localisation des données** | Dépend des partenaires du tiers fournissant le service en *Cloud* public | Définie par contrat |
| **Sécurité et niveaux de services** | Identiques pour tous les clients | Les niveaux d'exigences peuvent être définis de façon spécifique en fonction des besoins du client |
| **Coût à long terme** | Inférieur au coût d'un *Cloud* privé | Élevé en raison des niveaux de services spécifiques |

# Architecture hybride

*Figure 8 - Les architectures hybrides*




Le terme d'**Architecture hybride** s'applique également pour désigner les environnements hétérogènes mixant des ressources hébergées sur un environnement interne (ou parle de ressource on-premise ou à demeure) et un *Cloud* public ou plusieurs environnements *Cloud* public.

# Notre démarche

# Externalisation des systèmes d'information – gestion des risques

# Objectifs du guide

Faire prendre conscience aux décideurs informatiques des risques en matière de sécurité des systèmes d'information (SSI) liés à toute opération d'externalisation

Fournir une démarche cohérente de prise en compte des aspects SSI lors de la rédaction du cahier des charges d'une opération d'externalisation

Fournir un ensemble de clauses types ainsi qu'une base d'exigences de sécurité, à adapter et personnaliser en fonction du contexte particulier de chaque projet d'externalisation.

**Les publications de l'ANSSI sont diffusées sur son site Internet : http://www.ssi.gouv.fr/publications/**

# Risques liés à la perte de maîtrise de son SI

- **Risques liés à la sous-traitance** au sein d'un groupement d'entreprises répondant à un appel d'offres (co-traitance solidaire, sous-traitances déclarées)

- **Risques liés à la localisation des données (CID)**

  - **Réglementation RGPD** , autres obligations légales et réglementaires (Opérateurs d'importance vitale, santé publique)

  - **Obligations de sécurité physique et cyber sécurité**

  - **Localisation des données (infrastructures réparties) non maîtrisée**
    - difficulté à exercer un droit de regard et de contrôle sur les personnels du prestataire
    - difficulté à effectuer un audit de sécurité de l'infrastructure sous-jacente
    - difficulté à répondre à d'éventuelles injonctions de la justice, pour des raisons fiscales par exemple, ou d'autres raisons d'ordre juridique

# Risques liés à la perte de maîtrise de son SI

- **Risques liés aux données à caractère personnel**
  - **Responsabilité du titulaire des données** avec obligations de contrôle vis-à-vis du fournisseur
  - En effet, il faut garder à l'esprit que le donneur d'ordres, en tant que responsable de traitement, encourt des sanctions pénales en cas de non-respect des dispositions de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés

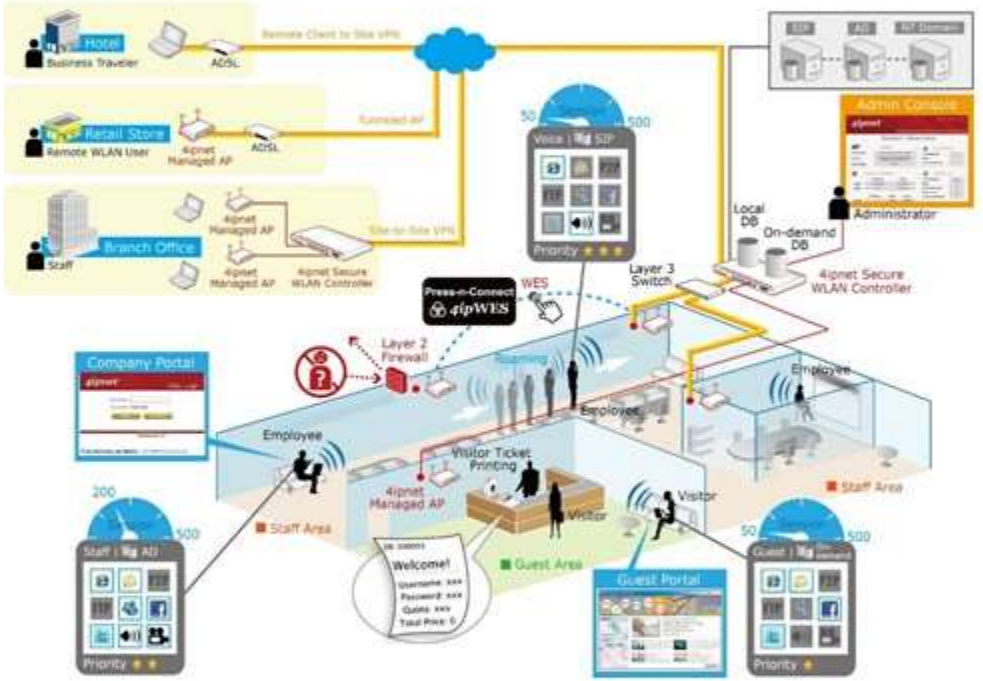
- **Risques liés aux choix techniques du prestataire**
  - Pour des raisons économiques d'où nécessité de valider les solutions proposées par le prestataire
  - Interopérabilité et format standard pour réversibilité, portabilté

# Risques liés aux accès à distance

**le télédiagnostic** : supervision d'équipements réseau et sécurité, diagnostic d'anomalies sur une application, etc.

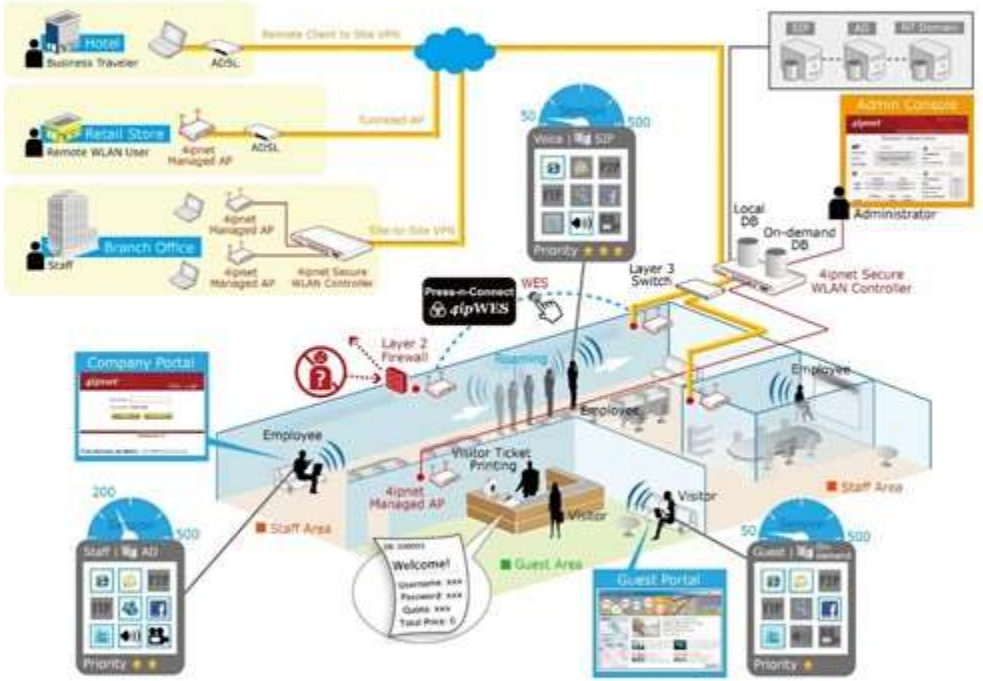
**la télémaintenance** : réalisation, après le diagnostic, des opérations à distance sur le dispositif

**la télédistribution** : mise à jour d'une application à distance



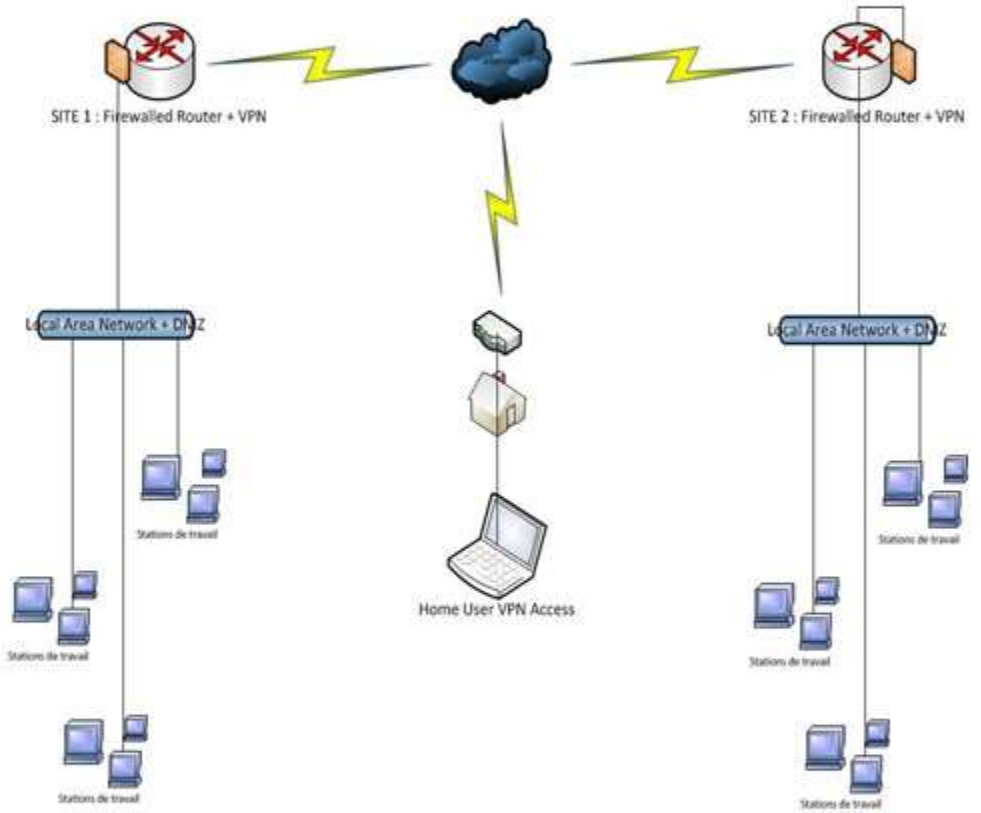
# Risques liés aux accès à distance

- **liaison établie de façon permanente** avec l'extérieur
- **mots de passe par défaut** (connus dans le monde entier) ou faibles
- **présence de failles** dans les interfaces d'accès
- **systèmes d'exploitation** des dispositifs non tenus à jour
- **absence de traçabilité** des actions
- **personnels responsables** de ces dispositifs non conscients des problèmes de sécurité ou mal formés
-
- **interconnexion de systèmes sécurisés** de confiance à des systèmes de niveau faible (internet par exemple).



# Mise en œuvre d'une solution sécurisée

- **authentifier** la machine distante et la personne en charge du support
- mettre en place une **politique de gestion des accès rigoureuses**
- **prévenir l'exploitation de vulnérabilités** ou de portes dérobées sur le dispositif de télémaintenance ;
- **garantir la confidentialité et l'intégrité des données** sur le SI
- assurer une **traçabilité de confiance des actions effectuées par le technicien du centre de support**
- **garantir l'innocuité de la fonction de télémaintenance** vis-à-vis du système faisant l'objet du télédiagnostic ainsi que des systèmes connexes
- **garantir l'absence de fuite d'informations** vers l'extérieur



# Risques inhérents à l'hébergement mutualisé

- **Perte de disponibilité : DDOS**
  - Problèmes si plusieurs services sont hébergés sur le même serveur (effets collatéraux)
  - Problème matériel côté héherbeur (cas d'une mise à jour par exemple , panne matérielle)

- **Perte d'intégrité**
  - Vulnérabilités (Spectre et Meldown) aboutissant à l'installation d'une porte dérobée, défiguration de site web, vol d'informations, rebond d'attaques  cryptomining
  - Changement d'un logiciel (voulu ou non) ayant une répercussion indirecte sur un service hébergé

- **Perte de confidentialité**
  - Partage de services dans un même environnement physique peut aboutit à des croisements d'information (contenu des fichiers clients de plusieurs sites dans la même base de données  ex ants –immatriculation)
  - Contrôle des accès par du personnel du fournisseur

## Prestataires de services d'informatique en nuage (SecNumCloud)
## Synthèse du référentiel d'exigences – niveau Essentiel

L'approche consistant à contractualiser au cas par cas la sécurité dans chaque projet de mise en nuage montre ses limites, les offres étant le plus souvent packagées ; de plus, il est également illusoire d'inciter chaque client à procéder à des audits réguliers des services offerts.

Une approche unifiée autour d'un référentiel a été préférée, favorisant ainsi l'émergence et la promotion d'offres qualifiées, les offreurs disposant d'un cadre stable dans lequel s'inscrire pour aller vers la qualification et les usagers pouvant baser leur confiance sur cette qualification.

Le référentiel de qualification de prestataires proposant une offre de services en nuage couvre les trois types d'activité (SaaS, PaaS et IaaS).

Les exigences, déclinées en 19 chapitres, sont relatives au prestataire et portent notamment sur le contrôle d'accès et gestion des identités, la cryptologie, la sécurité liée à l'exploitation et la gestion des incidents liés à la sécurité de l'information. Ces exigences seront vérifiées par une évaluation documentaire, organisationnelle, physique et technique des processus, infrastructures et lieux liés à la prestation visée par la qualification.

# Contrôle d'accès et gestion des identités

- **Politique et gestion d'accès** (cloisonnement, droit à en connaître, procédures entrant / sortants)

- **Enregistrement et désinscription des utilisateurs** (procédure via une interface de gestion des comptes et des droits d'accès)

- **Revue et contrôle planifié des droits d'accès utilisateurs**

- **Gestion des authentifications des utilisateurs**
  - la gestion des moyens d'authentification (émission et réinitialisation de mot de passe, mise à jour des CRL et import des certificats racines en cas d'utilisation de certificats, etc.). - > authentification à multiples facteurs
  - la mise en place des moyens permettant une authentification à multiples facteurs afin de répondre aux différents cas d'usage du référentiel
  - les systèmes qui génèrent des mots de passe ou vérifient leur robustesse, lorsqu'une authentification par mot de passe est utilisée. Ils doivent suivre les recommandations de [NT_MDP]. b) Tout mécanisme d'authentification doit prévoir le blocage d'un compte après un nombre limité de tentatives infructueuses.

# Sécurité de l'information – fonction, formation, communication

- **Documentation à jour** sur l'organisation interne (RACI)
  - Un responsable de la sécurité des systèmes d'information
  - Un responsable de la sécurité physique

- **Procédures claires pour coopération avec les autorités**
  - Sécurité de l'information
  - Protection des données à caractère personnel

- **Sécurité des ressources humaines**
  - Embauche (casier judiciaire, signature charte éthique, respect charte informatique)
  - Sensibilisation, apprentissage et formation à la sécurité de l'information (plan de formation adapté aux besoins)
  - Processus disciplinaire en cas d'infraction aux règles (connues et respectées)
  - Rupture, terme ou modification du contrat de travail
    - Gestion des arrivées et départ ( messagerie, mots de passe, accès distants, etc)

# Gestion des actifs

- **Inventaire et propriétés des actifs à jour**
  - les informations d'identification de l'équipement (nom, adresse IP, adresse MAC, etc.) ;
  - la fonction de l'équipement ;
  - le modèle de l'équipement ;
  - la localisation de l'équipement ;
  - le propriétaire de l'équipement ;
  - le besoin de sécurité des informations
  -
- **Restitution des actifs en fin de contrat (réversibilité)**

Le prestataire doit documenter et mettre en œuvre une procédure de restitution des actifs permettant de s'assurer que chaque personne impliquée dans la fourniture du service restitue l'ensemble des actifs en sa possession à la fin de sa période d'emploi ou de son contrat

- Prise en compte des besoins en sécurité (cas d'information sensible de l'entreprise : hôpital, PI)

# Cryptologie

- **Chiffrement des données stockées**
  - Protection de récupération des données clients en cas de réallocation d'une ressource physique ou de remplacement de cette dernière
  - Chiffrement suivant les recommandations de l'ANSSI

- Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr

- **Chiffrement des flux**
  - **Protocole TLS** : Le protocole TLS1 est une des solutions les plus répandues pour la protection des flux réseau. Dans ce modèle client–serveur, les données applicatives sont encapsulées de manière à assurer la confidentialité et l'intégrité des échanges. Le serveur est nécessairement authentifié, et des fonctions additionnelles permettent l'authentification du client lorsqu'un tel besoin a été identifié.

  - **Protocole IPSEC** : IPsec est une suite de protocoles de communication sécurisée permettant la protection des flux réseau. Elle est éprouvée, mais souvent mal maîtrisée et reste encore trop peu ou mal employée.

  - **Protocole SSH**,ou Secure SHell,est unprotocole applicatif(couche7dumodèledel'OSI)qui vise à corrigerles déficiences connue s dans les protocoles FTP, RSH, RCP et TELNET

# Cloud et RGPD

L'entrée en vigueur du nouveau Règlement Général de Protection des Données (RGPD) , prévue en 2017 par la Commission Européenne, amènera à une revue des contrats cloud. Traitant notamment de la confidentialité des données dans le cloud, cette directive engage les DSI qui se doivent de vérifier la localisation de celles-ci et la réglementation applicable au cas par cas avec tous leurs fournisseurs

## Services cloud, sécurité et confidentialité

Nécessité de vérifier que toutes les obligations réglementaires et les pratiques de sécurité appliquées dans l'organisation sont appliquées à l'identique par ses fournisseurs. Des garanties supplémentaires et des contrôles sont requis pour assurer la protection du patrimoine de données qui est remis entre les mains de ces parties tierces.

## Evaluations des risques spécifiques aux services du cloud

Liste des parties impliquées, rôles et responsabilités (entreprise- fournisseur)

Localisation des datacenters où sont stockées les données ou fournis les services

Engagements contractuels entre le contrôleur de l'entreprise cliente et le fournisseur de traitement dans le cloud

# Cloud et RGPD

En raison des implications figurant dans le nouveau Règlement Général de la Protection des Données (RGPD), la plupart des organisations globales utilisant des services cloud devront suivre d'une façon ou d'une autre les recommandations de cette loi. La conséquence la plus directe de son application est que **autant les clients que les fournisseurs auront des responsabilités accrues dans l'accomplissement de leurs obligations, quoi que, d'après l'art. 22, les entreprises clientes resteront les seules finalement responsables et devront vérifier que les activités de traitement numérique sont effectuées en accord avec la réglementation.**

# Références

- Guide sur le Cloud Computing et les Datacenters à l'attention des collectivités locales DGE – Caisse des Dépôts – cget
- Prestataires de services d'informatique en nuage (SecNumCloud) référentiel d'exigences – niveau Essentiel

Version 3.0 du 8 décembre 2016


Risques numériques
MRT de sécurisation
Sécurisation des architectures SI et ICS
Datacenter et Cloud Computing
RGPD

https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes

# RGPD

Règlement Général sur la protection des données
Applicable mai 2018

Protection des données à caractère personnel et données sensibles

## LA RÉFORME DE LA PROTECTION DES DONNÉES POURSUIT TROIS OBJECTIFS :

1. **Renforcer les droits des personnes**, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures ;
2. **Responsabiliser les acteurs traitant des données** (responsables de traitement et sous-traitants) ;
3. **Crédibiliser la régulation** grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux et des sanctions renforcées.

**Renforcer les droits des personnes**

# Des données à emporter !

**Je peux récupérer les données que j'ai communiquées à une plate-forme et les transmettre à une autre (réseau social, fournisseur d'accès à internet, site de streaming, etc.)**

## Plus de transparence


**Je bénéficie de plus de lisibilité sur ce qui est fait de mes données et j'exerce mes droits plus facilement (droit d'accès, droit de rectification).**

## Protection des mineurs

**Les services en ligne doivent obtenir le consentement des parents des mineurs de moins de 16 ans avant leur inscription.**

## Guichet unique

**En cas de problème, je m'adresse à l'autorité de protection des données de mon pays, quelque soit le lieu d'implantation de l'entreprise qui traite mes données.**

# Sanctions renforcées

**En cas de violation de mes droits, l'entreprise responsable encourt une sanction pouvant s'élever à 4% de son chiffre d'affaires mondial.**

# Consécration du droit à l'oubli

**Je peux demander à ce qu'un lien soit déréférencé d'un moteur de recherche ou qu'une information soit supprimée s'ils portent atteinte à ma vie privée**

# LE **RGPD** EN UN COUP D'ŒIL

## PORTÉE

Toutes les entreprises du **MONDE** traitant
les données personnelles de citoyens européens

## OBLIGATIONS


Les entreprises doivent notifier les violations de données
**DANS UN DÉLAI DE 72 HEURES**

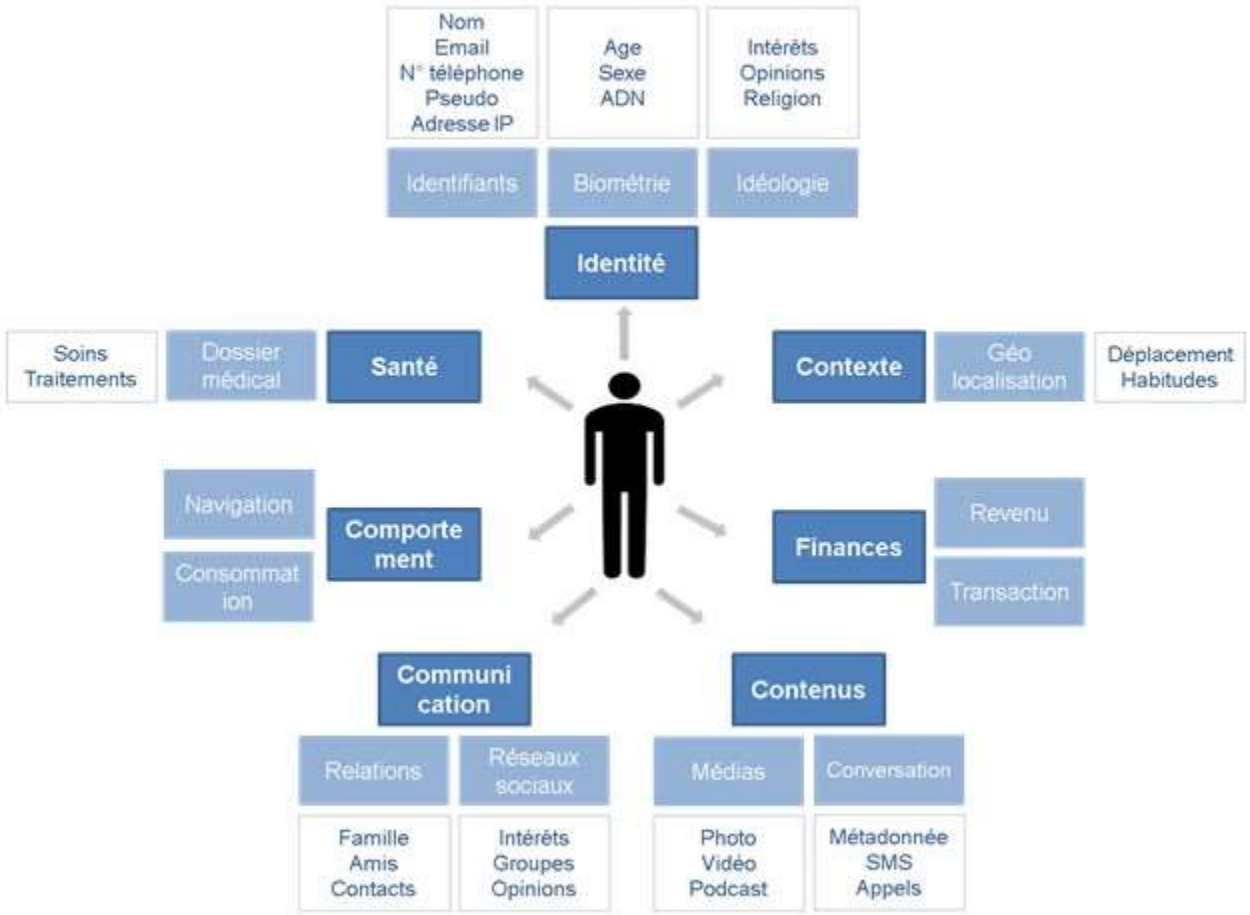
## SANCTIONS


JUSQU'À DU CHIFFRE D'AFFAIRES **MONDIAL**

## CALENDRIER


Promulgation par les États membres de l'UE

# Champ d'application : données à caractère personnel



# Données sensibles (RGPD)

**Traitements communs à la plupart des entreprises**

- Fichiers clients (entreprises) / usagers (administrations)
- Fichiers fournisseurs
- Annuaire interne
- Contrôle d'accès (badges)
- Cantine
- Fichiers des mauvais payeurs
- Site internet
- E-commerce
- Logs des serveurs

# Champ d'application du RGPD

- **Traitement de données**

Quelques exemples d'opérations considérées comme des traitements : Collecte, enregistrement, organisation, structuration, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission, diffusion, mise à disposition, rapprochement, interconnexion, limitation, effacement, destruction, etc.

- **Traitements communs à la plupart des entreprises**
  - Fichiers clients (entreprises) / usagers (administrations)
  - Fichiers fournisseurs
  - Annuaire interne
  - Contrôle d'accès (badges)
  - Cantine
  - Fichiers des mauvais payeurs
  - Site internet
  - E-commerce
  - Logs des serveurs

# Responsabilisation des entreprises

### ◆ Un champ d'application étendu

Le règlement s'applique dès lors que le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union européenne ou que le responsable de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services aux résidents européens ou à les « cibler » (en anglais monitor).

En pratique, le droit européen s'appliquera donc chaque fois qu'un résident européen sera directement visé par un traitement de données, y compris par Internet.

### ◆ Responsabilité des sous-traitants

Par ailleurs, alors que le droit de la protection des données actuel concerne essentiellement les « responsables de traitements », c'est-à-dire les organismes qui déterminent les finalités et les modalités de traitement de données personnelles, le règlement étend aux sous-traitants une large partie des obligations imposées aux responsables de traitement.

### CNIL : guichet unique

**Par exemple**, dans le cas d'une entreprise dont l'établissement principal est en France, la CNIL sera le guichet unique de cette entreprise et lui notifiera les décisions adoptées dans le cadre de ce mécanisme de cohérence. Ses décisions seront ensuite, si elles sont défavorables, susceptibles de recours devant le Conseil d'État.

# Exemple d'inventaire

| Pourquoi | Qui | Quoi | | | QUAND | | | | Où | Confidentialité |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Type | Source | Base juridique | Origine | Mise à jour | Période de conservat | Conformité légale | | |
| GESTION du personnel | Employés | Nom | | | | | | | Dossier papier RH | Confidentiel |
| | | Adresse | Individuel | | | | | | Fichier excel sur serveur x | |
| | | Détails de contact | | contrat salarial | Entrée dans la socié | Sur demande | 6 ans après avoir | gov fr | | |
| | | Santé | | | | | quitté l'entreprise | | portable Dir RH | |
| | | CV | | | Pré-embauche | Non | | code de bonne | portable resp activités | |
| | | Références | Tiers | | Pré-embauche | Non | | pratiques | | |
| | | Données bancaires | Individuel | | | ? | | | | |
| | | Passeport -ou ID | Individuel | conformité légale ? | | | | | | |
| | | | | | | | | | | |
| | | Permis de travail | Individu /Tiers | | ? | ? | | | | |
| | | | | | | | | | | |
| | | Salaire | Individuel | | contrat de travail | rev annuelle | | | Fichiers des salaires | |
| | | | | | | | | | A éclaircir | |
| | | Congés | Individuel | | sur demande | | | | | |
| | | | | | | | | | | |
| | | Discipline | Individuel | | ADTR | | | | | |
| | | | | | | | | | | |
| | | Pensions | Individuel | | contrat de travail | | | | | |
| | | | | | | | | | | |
| | | Evaluation | Individuel | | Annuel | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| Marketing Direct | Clients existants | Nom | | | | | | | | Restreint |
| | | Adresses | Individuel | Consentement | 1ere prise de contac | sur demande | consentement mutue | LRGPD | | |
| | | Email | | | | | | | | |
| | | Mobile | | | | | | | | |
| | | Téléphone | | | | | | | | |
| | | | | | | | | | | |
| | Clients potenteils | Nom | Listing / Interne | A trouver | ?? | sur demande | N/A | N/A | | Public |
| | | Email | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

# Evaluation des menaces et des risques

| Données - services | C | I | D | A | Mesures fonctionnelles | Mesures techniques |
|---|---|---|---|---|---|---|
| 001 -RH | Confidentiel | Oui | 6 h | Audit ADTR | Plan accès management – sponsor RH<br>Formation personnel RH Contrôle des procédures de sécurité – sponsor gestionnaire des risques | Messagerie chiffrée<br>Sauvegarde chiffrée<br>Temps de restauration respecté => budget – renfort personnel<br>Contrat sous-traitant validé et conforme aux exigences du RGPD |
| 002 - Clients | | | | | | |
| 003- Vacataires | | | | | | |
| 004- Sous-traitants | | | | | | |
| | | | | | | |

# Registre des traitements

| Identification du traitement | | | | Acteurs | Finalité du traitement | Transferts hors UE ? | Données sensibles ? |
|---|---|---|---|---|---|---|---|
| Nom / sigle | N° / REF | Date de création | Dernière mise à jour | Responsable du traitement | Finalité principale | Oui /non | Oui/non |
| Gestion RH | ref-001 | 31/10/2017 | | Dir RH | Salaire -carrière - licenciment | Non | Oui |
| Gestion Clients | ref-002 | 31/10/2017 | | Dir Commercial | Prospect - devis - facturation | Non | Non |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

# Mesures de sécurité

- **Organisation** : DPO et des responsables de traitements par départements / activités
- **Procédures documentées** : cycle de gestion de vie des données , les personnes autorisées à y accéder et à les utiliser , le contrôle du respect des obligations par les sous-traitants en charge d'un traitement particulier, les procédures de notification et de gestion des incidents etc.
- **Contrats juridiques** avec les sous-traitants avec délégation d'une partie des responsabilités
- **Moyens de sécurisation informatique** :
  - sécurisation du réseau informatique, des postes de travail, smartphones, tablettes
  - Sécurisation des moyens de transmission de données sensibles (messagerie, documents sensibles envoyés, vpn)
  - Sécurisation des données stockées en interne ou externe (chiffrement)
  - Sécurisation physique des locaux
- **Revue régulière de la documentation obligatoire**
- **Plan de formation des personnes manipulant ces données**

# Processus de notification de failles de sécurité (autorités, clients)

**72 heures**
**-> Clients**
**-> CNIL**

**Une obligation de sécurité et de notification des violations de données personnelles pour tous les responsables de traitements**

Les données personnelles doivent être traitées de manière à garantir une sécurité et une confidentialité appropriées. Lorsqu'il constate une violation de données à caractère personnel, le responsable de traitement doit notifier à l'autorité de protection des données la violation dans les 72 heures. L'information des personnes concernées est requise si cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne.

# Les documents règlementaires à produire

- **Inventaire des données  et des traitements**
- **L'analyse des risques** : études d'impact sur la vie privée
- **La tenue d'un registre des traitements**
- **Les Procédures de  notification et de gestion de failles de sécurité** (aux autorités et personnes concernées)
- **La  certification de traitements** : aspects contractuel avec sous-traitants
- **La fiche de tâche du correspondant CNIL DPO** (délégué à la protection des données) ou équivalent