

# PROTECTION DES SYSTÈMES D'INFORMATIONS DES ENTREPRISES D'EAU ET D'ASSAINISSEMENT



# AGENDA

1

Rappel /  
quelques  
définitions

2

Les tendances  
des cybers  
attaques contre  
les entreprises  
d'eau et  
d'assainissement

3

Les composantes  
clés d'un Système  
d'Information  
( SI) pour  
entreprise  
d'eau et  
d'assainissement

4

Les  
vulnérabilités  
possibles contre  
ce type de SI

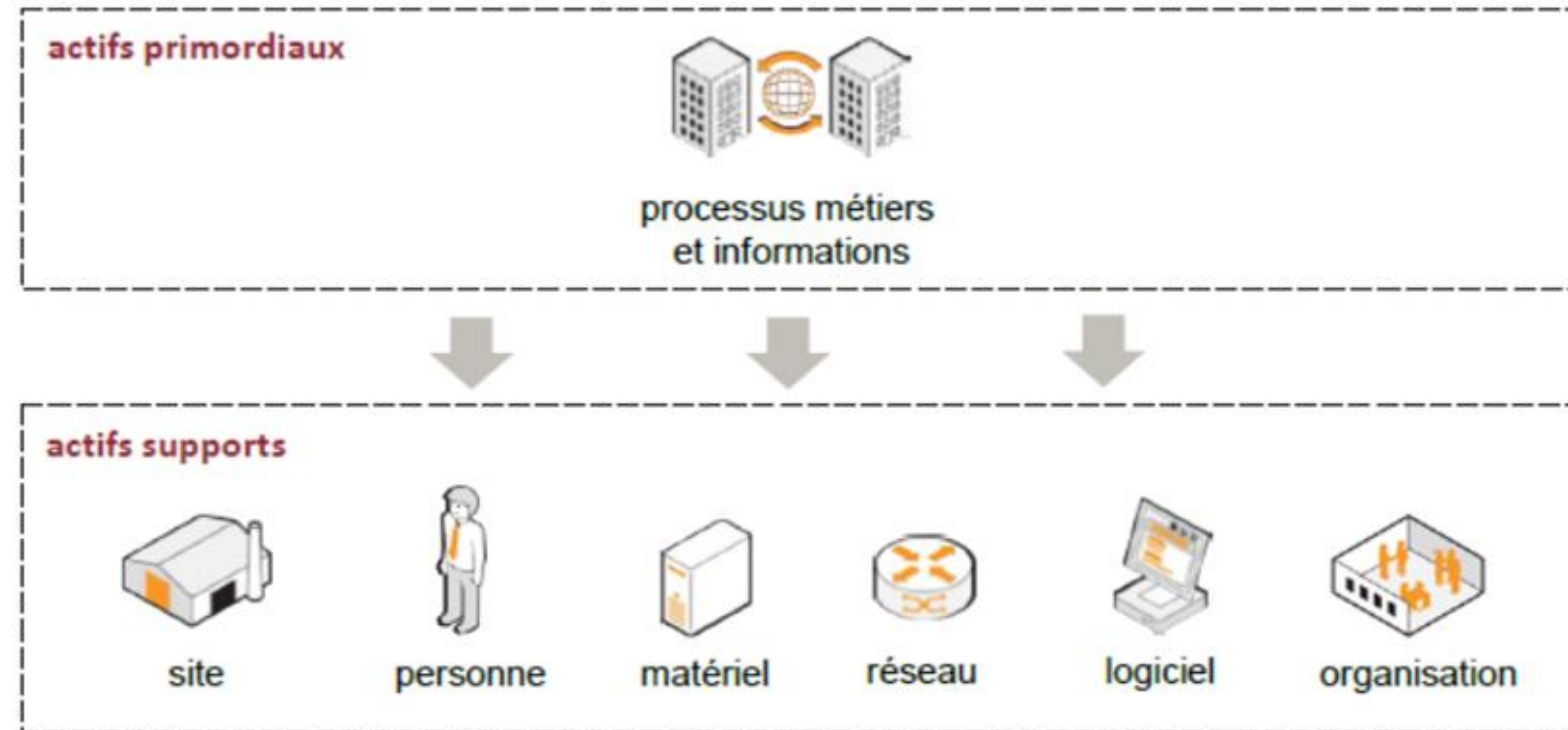
5

Quelques outils  
de protections

Systeme d'Information (S.I.): Ensemble des ressources destinées à **collecter, classier, stocker, gérer, diffuser** les informations au sein d'une organisation

**Le S.I. doit permettre et faciliter  
la mission de l'organisation**

- Le système d'information d'une organisation contient un ensemble d'actifs :



 ISO/IEC 27005:2008

**La sécurité du S.I. consiste donc à assurer la sécurité de l'ensemble de ces biens**

# Les enjeux de la sécurité

- ▶ La sécurité a pour objectif de réduire les risques pesant sur le système d'information, pour limiter leurs impacts sur le fonctionnement et les activités métiers des organisations...
- ▶ La gestion de la sécurité au sein d'un système d'information n'a pas pour objectif de faire de l'obstruction. Au contraire :
  - ▶ Elle contribue à la qualité de service que les utilisateurs sont en droit d'attendre
  - ▶ Elle garantit au personnel le niveau de protection qu'ils sont en droit d'attendre



Impacts financiers



Impacts sur l'image et la réputation

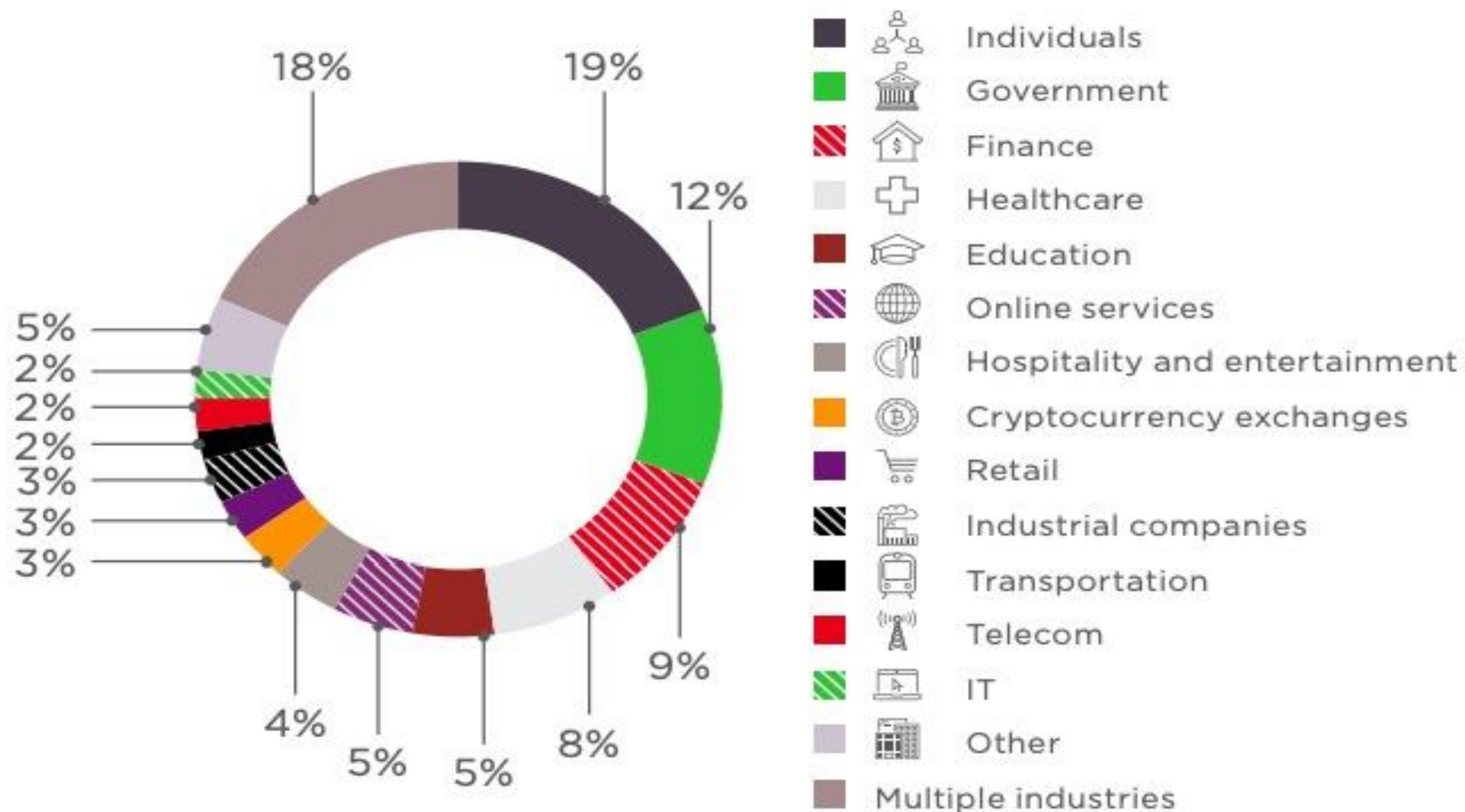
Sécurité des S.I.

Impacts juridiques et réglementaires

Impacts organisationnels



# Protégez votre SI : ça n'arrive pas qu'aux autres!

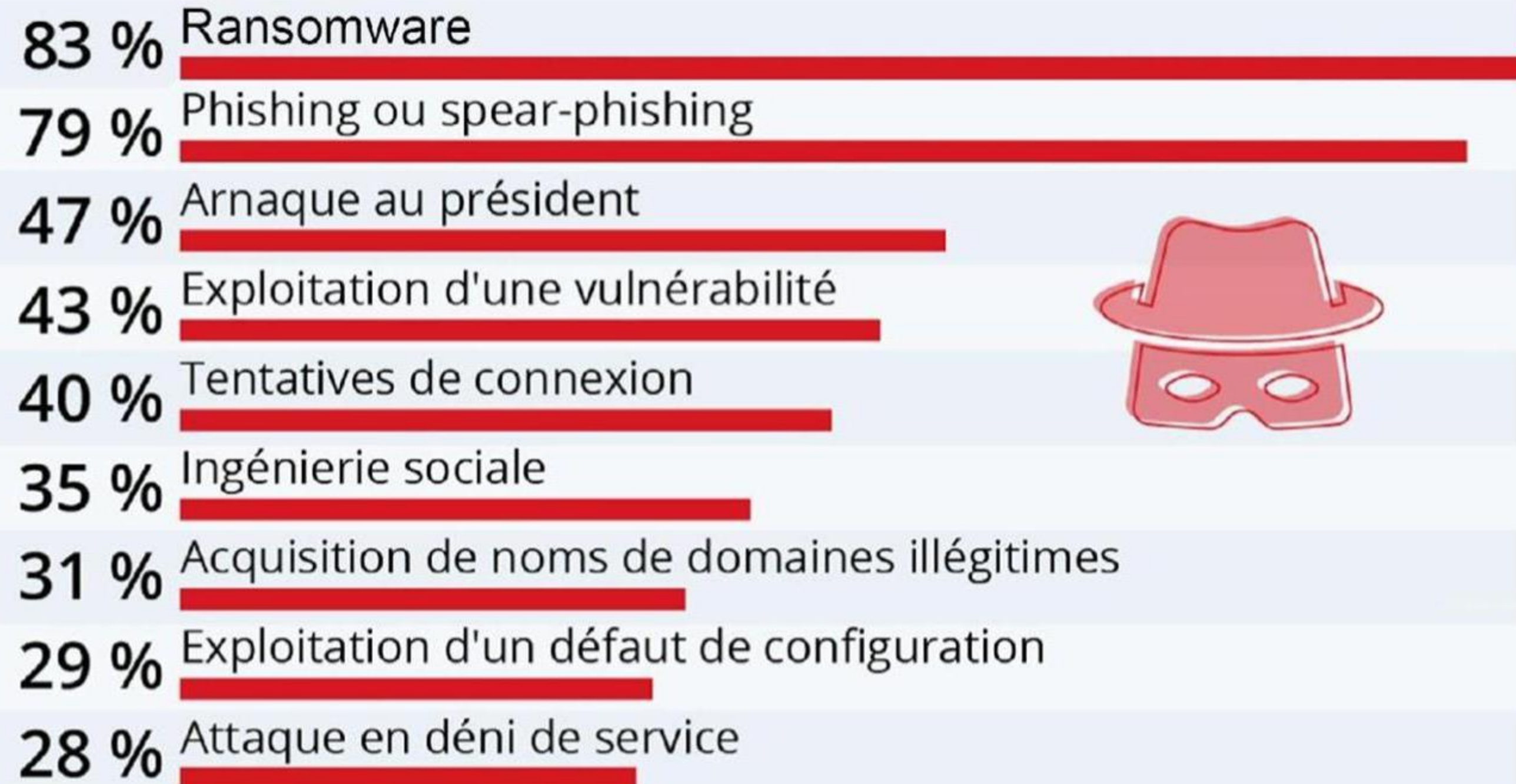


Ne le faites peut-être pas avec nous **MAIS FAITES LE POUR VOUS-MÊME SVP!!!**

Les industries les plus attaquées

# Les cyberattaques les plus courantes contre les entreprises

Types d'attaques les plus constatés par les entreprises en 2019 \*



\* Plusieurs réponses possibles, sélection des résultats supérieurs à 20 %.  
En moyenne : 3,9 types d'attaques constatés parmi les entreprises ayant subi au moins une attaque.

Sources : CESIN, OpinionWay





# Aperçu des cyberattaques qui ciblent les usines de traitement d'eau (ou les manufacturiers en général)

Chiffrement des systèmes critiques par un ransomware (paralyse du système d'approvisionnement en eau)

---

Hameçonnage (objectif = fraude financière)

---

DDOS (paralyse du système d'approvisionnement en eau)

---

Altération des quantités de produits chimiques utilisés pour traiter l'eau

---

(comme le cas du piratage de l'usine de traitement d'eau en Floride cette année) :  
mise en danger de vies humaines

Attentat : forte altération les qualités de produits chimiques afin de causer des décès massive :

---

risque non nul au regard de la situation actuelle du terrorisme au niveau mondial



**98% of .ci domains  
are vulnerable**



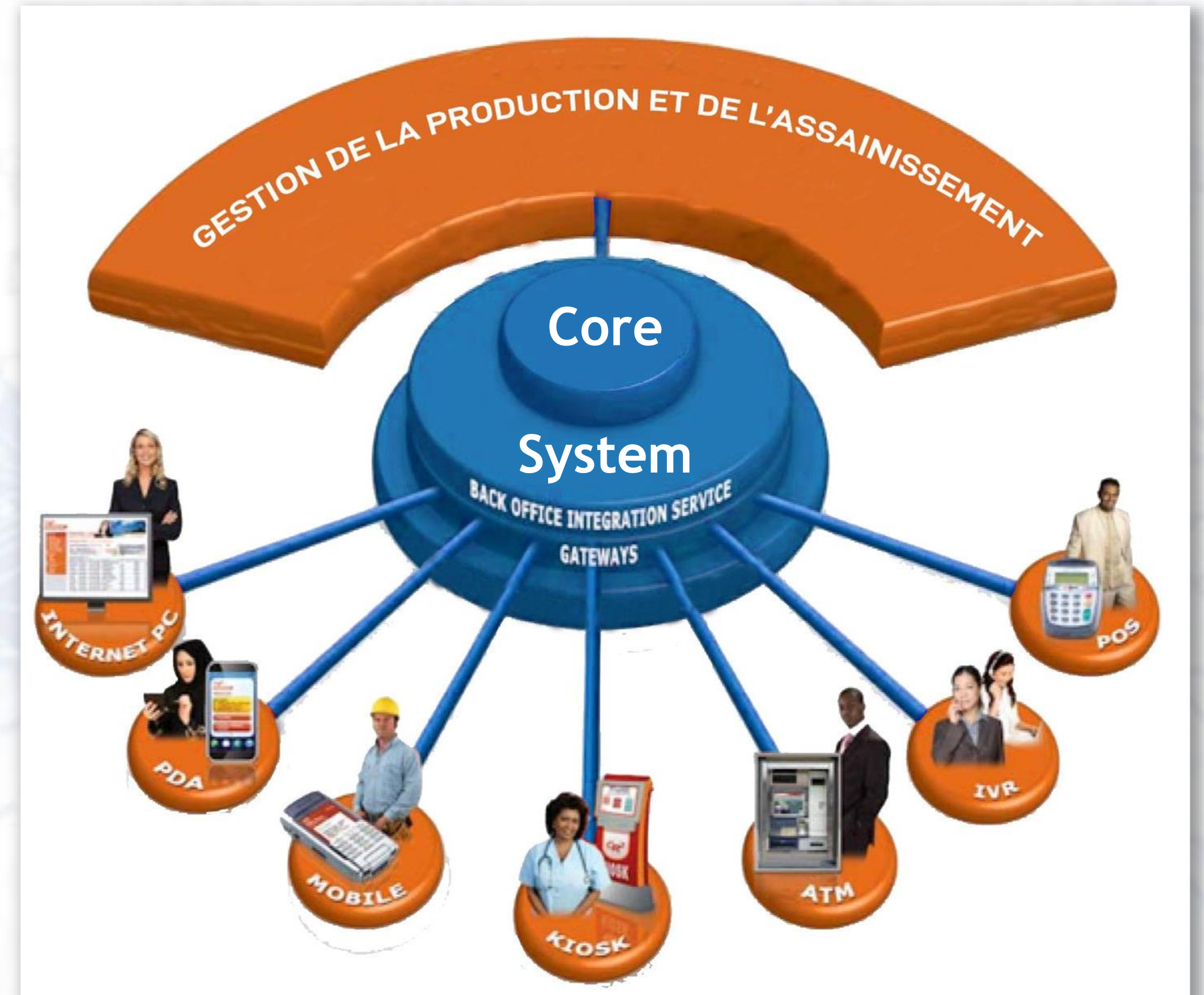
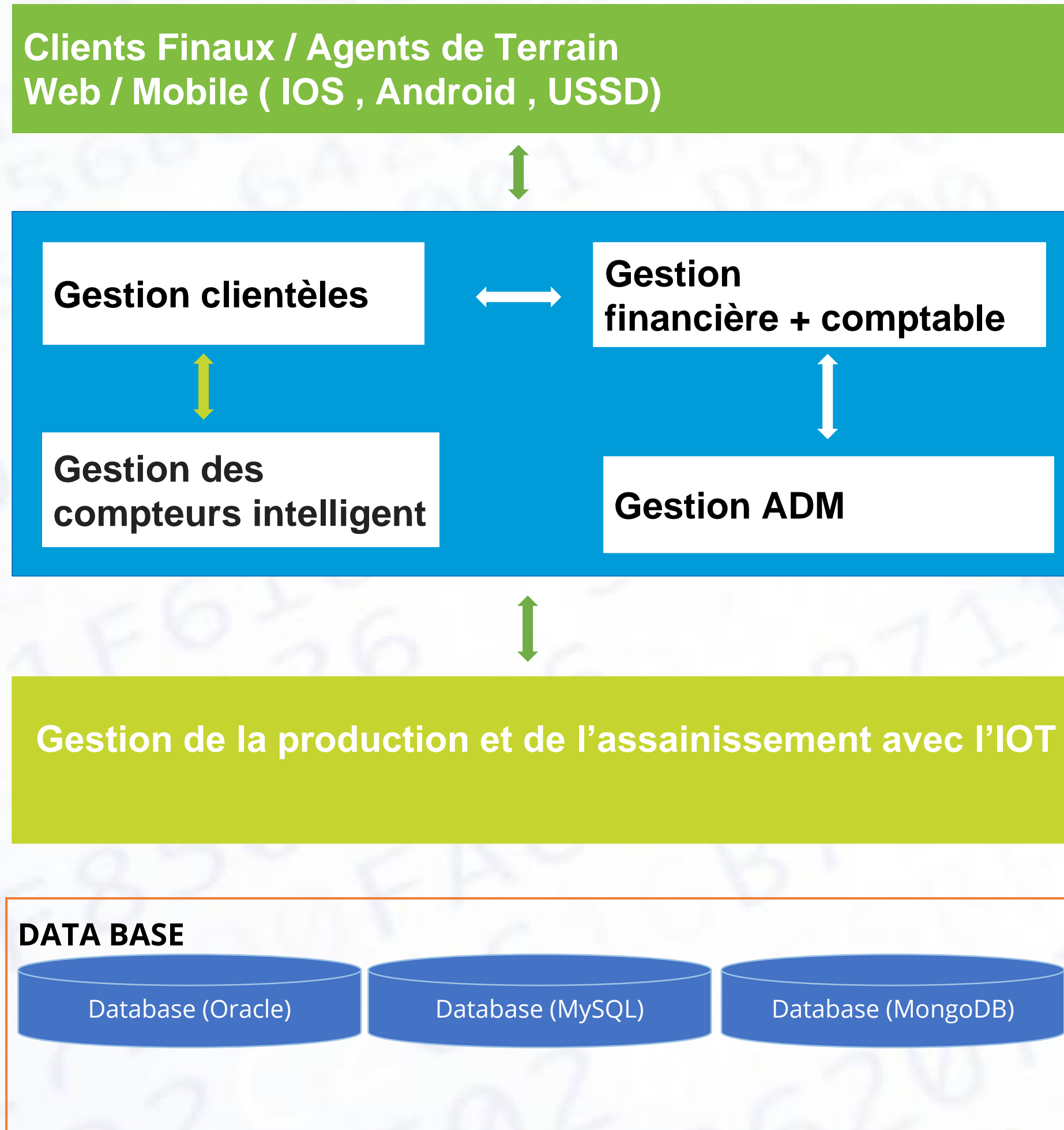
**89% of companies in  
West Africa are  
vulnerable to cyber  
attacks**

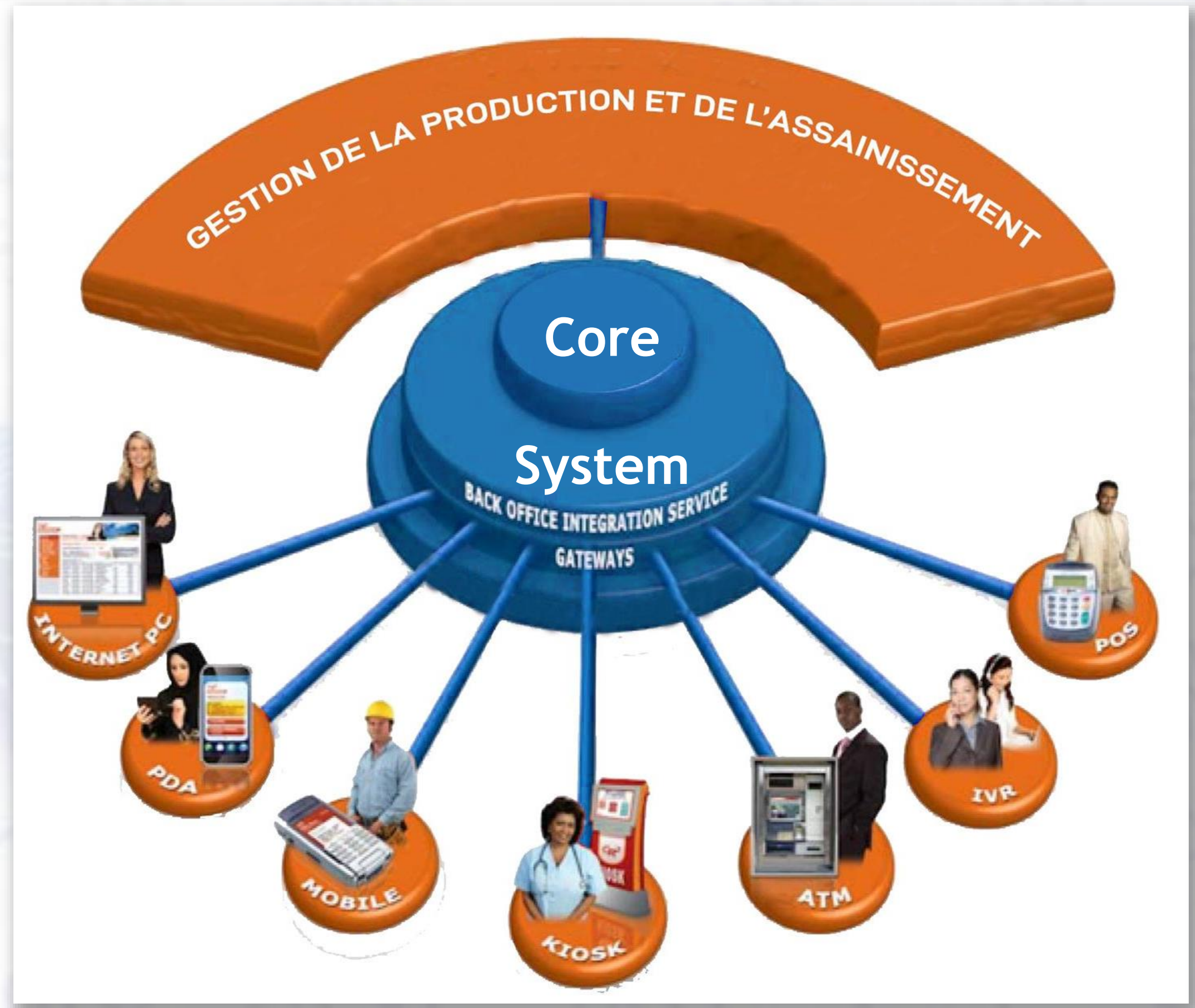
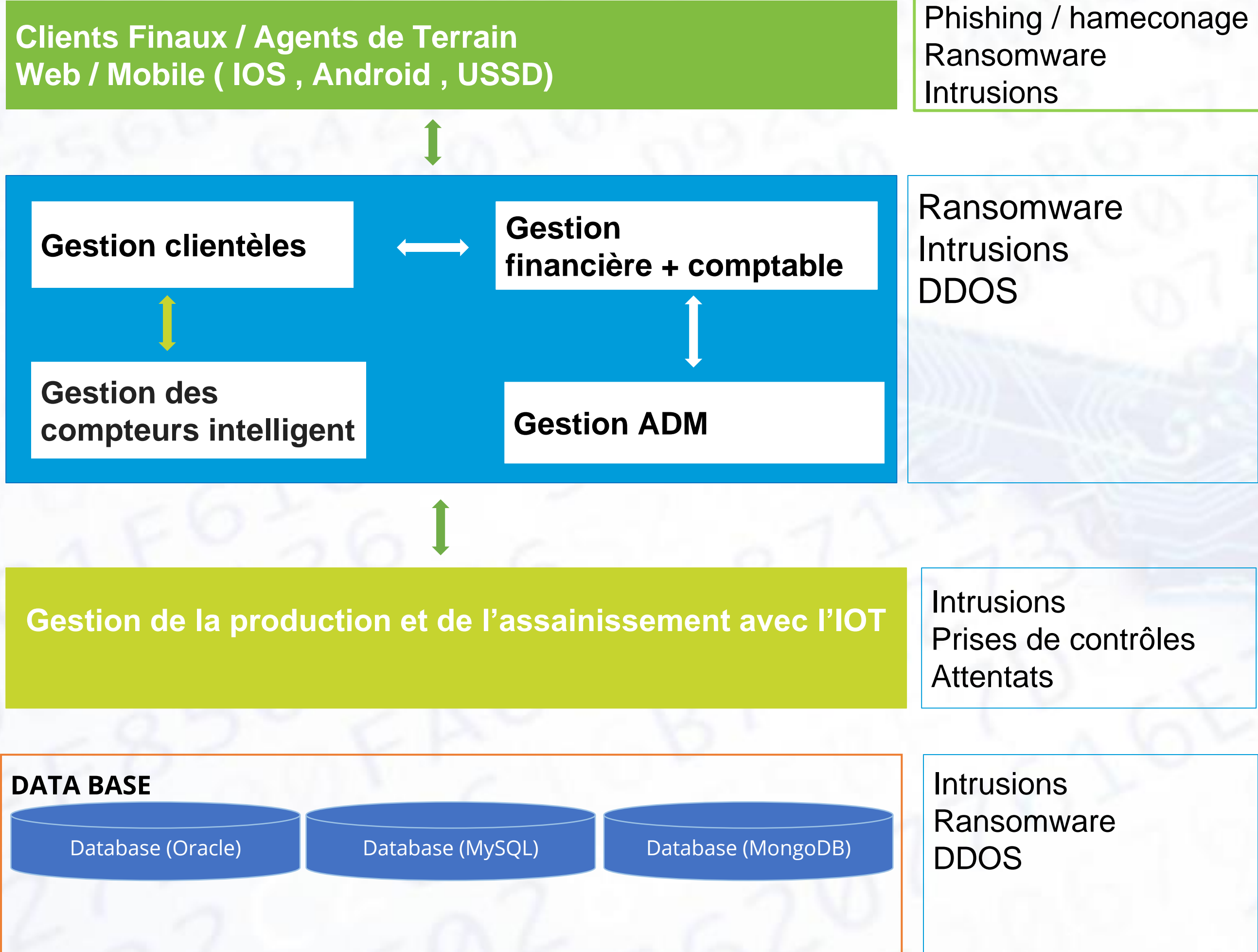


**69% des violations en Afrique ont eu un impact sur plus de la moitié des systèmes de l'entreprise**

**En 2019, 78% des entreprises en Afrique ont dû gérer une panne de plus de 5 heures en raison de cyberattaques**







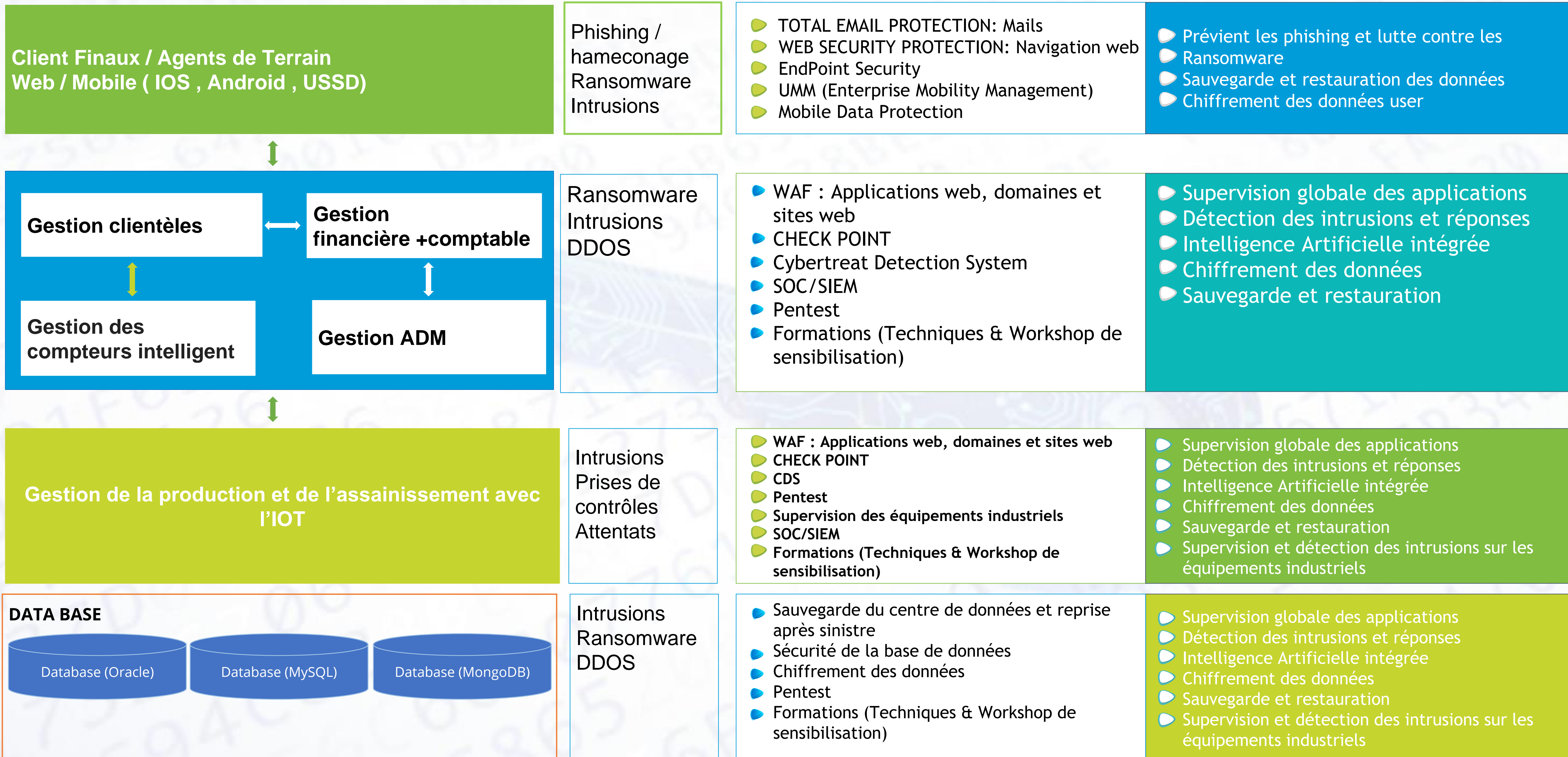
# Comment sécuriser les infrastructures de traitement d'eau (et des usines en général)

- ▶ Avoir la visibilité à 360 degrés de son parc informatique (IT, OT, IOT, Cloud, etc.) via un IDS/IPS
- ▶ Monitorer en continu la sécurité de son réseau (TI et OT/IOT) et prendre en charge tous les cas douteux/malicieux
- ▶ Gérer les vulnérabilités de sécurité
- ▶ Avoir une stratégie de cybersécurité proactive

- ▶ Support de la Haute direction
- ▶ Identifier ses principaux risques de sécurité et les traiter
- ▶ Faire des backups réguliers et les tester
- ▶ Définir un cadre de gouvernance de la sécurité
- ▶ Sensibiliser les utilisateurs
- ▶ Se préparer au pire : définir un plan de réponse aux incidents et le tester au moins 1 fois par année



# QUELQUES SOLUTIONS





Solutions / Services	Conditions	Prix FCFA	Les ++ de cette offre
<b>TESTS DE PÉNÉTRATION :</b> ➤ LES APPLICATIONS CRITIQUES  ➤ LES DOMAINES  ➤ LES SITES WEB	1 application critique	3 500 000  [3 - 5 jours]	➤ 1 workshop de sensibilisation offert pour les managers en ligne ➤ 1 POC pour le CDS (Déploiement online) ➤ 1 POC WAF
	3 applications critiques	5 000 000  [5 - 10 jours]	➤ 1 workshop de sensibilisation offert pour les managers ➤ 1 site web intégré ➤ 1 POC pour le CDS (Déploiement online) ➤ 1 POC WAF ➤ 1 POC TOTAL EMAIL PROTECTION ➤ 1 POC WEB SECURITY PROTECTION: Navigation web ➤ 1 POC pour les EndPoint Security
	1 Site web & 1 nom de domaine	3 000 000  [1 - 3 jours]	➤ 1 workshop de sensibilisation offert pour les managers ➤ 1 POC WAF : Applications web, domaines et sites web ➤ 1 POC pour le CDS (Déploiement online)

Validité de l'offre: 31/03/2021

► Services Cyber Sécurité de haut niveau et l'un des meilleurs au monde qui couvrent de bout en bout tous les aspects de la sécurité informatique: le conseil, la protection et la surveillance pour sécuriser votre entreprise

► En tant que Fournisseur de Services de Sécurité ou MSSP (Managed Security Service Provider), nous aidons les entreprise à :

- se protéger,
- détecter et à se défendre contre les cyber-intrusions.

Des services personnalisés pour répondre aux besoins de sécurité des clients

► Nous protégeons vos systèmes en partenariat avec les meilleures entreprises au monde grâce à nos solutions, nos services de Cyber Sécurité et les surveillons pour détecter et anticiper les cyberattaques.

## CYBER SECURITE ET GESTION DE RISQUES



Bilan de la  
Cyber Sécurité



Conseil  
en Cyber Sécurité  
et evaluation



Centre  
Opérationnel de  
Cyber Sécurité



Réseaux  
Sécurisés

La culture de la cyber sécurité en entreprise : « En matière de cybersécurité, l'humain est le principal point de vulnérabilité »

## La capacité défensive

- Specialists Analysts / SOC Analysts en support
- Centres d'entraînement

**Le management du risque:** accompagner les organisations à asseoir des règles et procédures de gestion permettant de minimiser le risque

