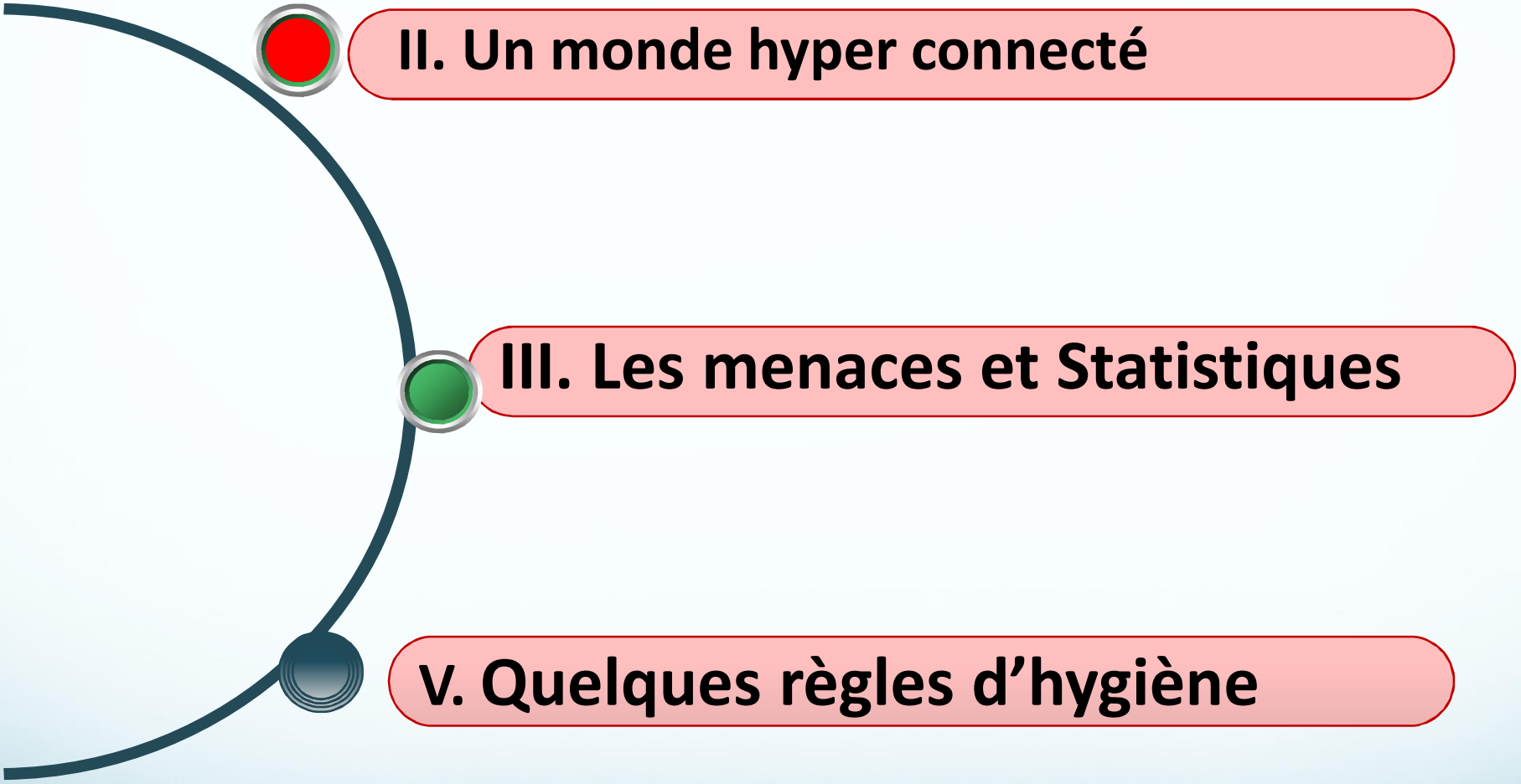
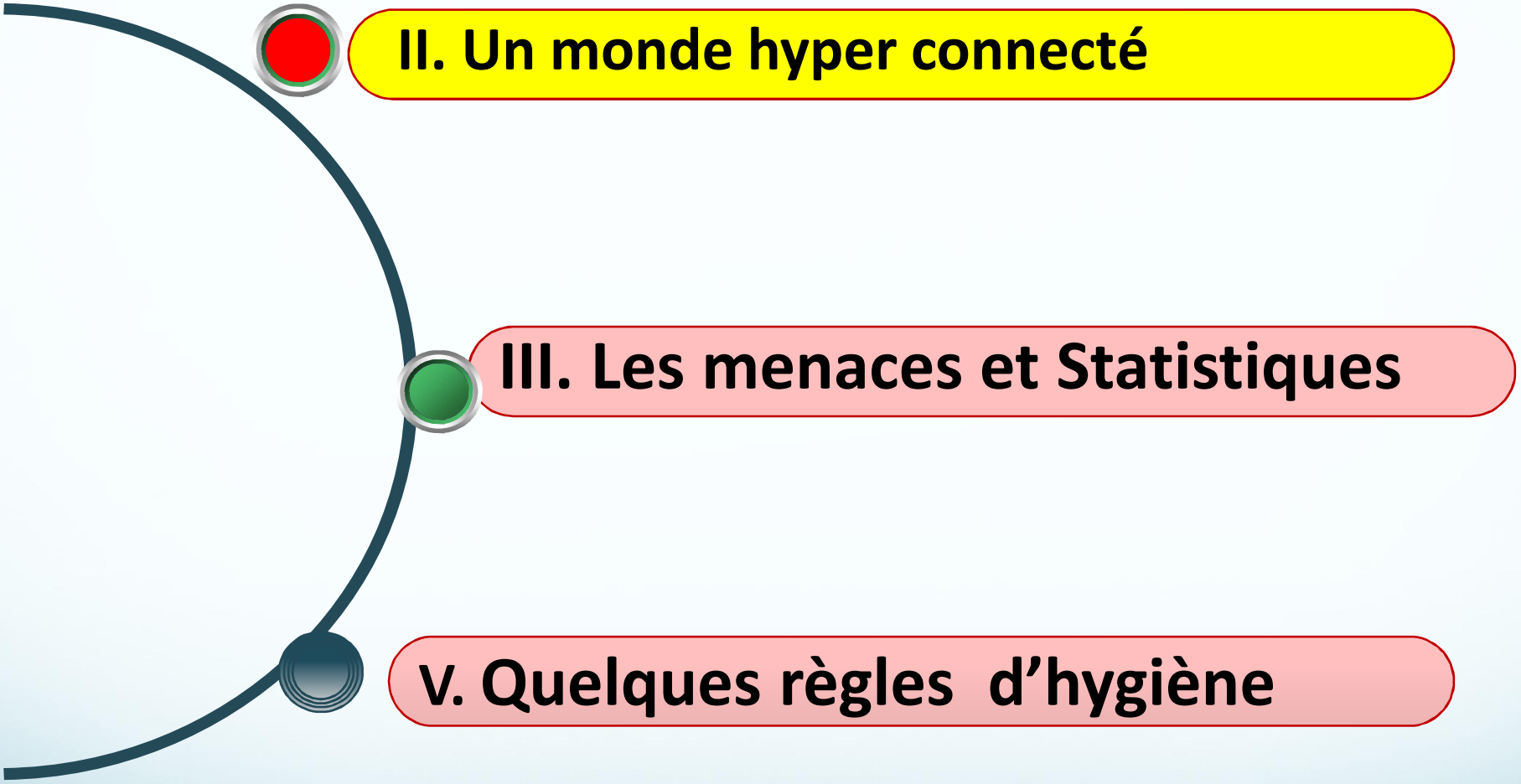

FFGI
2019

Beginingé

Michaël Guibougna Lawakiléa FOLANÉ
Directeur Général ANSSI/BF
michael.folane@anssi.bf


II. Un monde hyper connecté
III. Les menaces et Statistiques
V. Quelques règles d’hygiène


II. Un monde hyper connecté
III. Les menaces et Statistiques
V. Quelques règles d'hygiène

Le numérique :

- une révolution qui entraine
  - de **plus en plus** que nous soyons **connectés**
  - de **plus en plus** que nous soyons **adeptes de nouvel usage**
  - **…**

La **face noire et obscure** de ces questions :

- les **risques dâattaques**
- le **nombre de type dâagresseurs potentiels** (Des criminel, des organisation, des états,é)

Face à ces attaques chacun doit :

- Être **acteur**;

- **Comprendre** le numérique pour mieux se **protéger**


Dans les années 90 on assiste à la mise en place dôautoroute mondiale pour le transport de lôinformation par les société de télécom

La voie est alors toute tracée pour la plus grande des transformations

En **30 ans**, les choses ont **évoluées** et se sont **compliquées** davantage. Plus récemment ce sont les objets du quotidien qui sont à leur tout devenu des **objets connectés**

NB : plus il y a des objets connectés plus la surface d'attaques est augmentée

Les attaques informatiques utilisent le territoire virtuel que est le cyberespace pour atteindre leur cible.

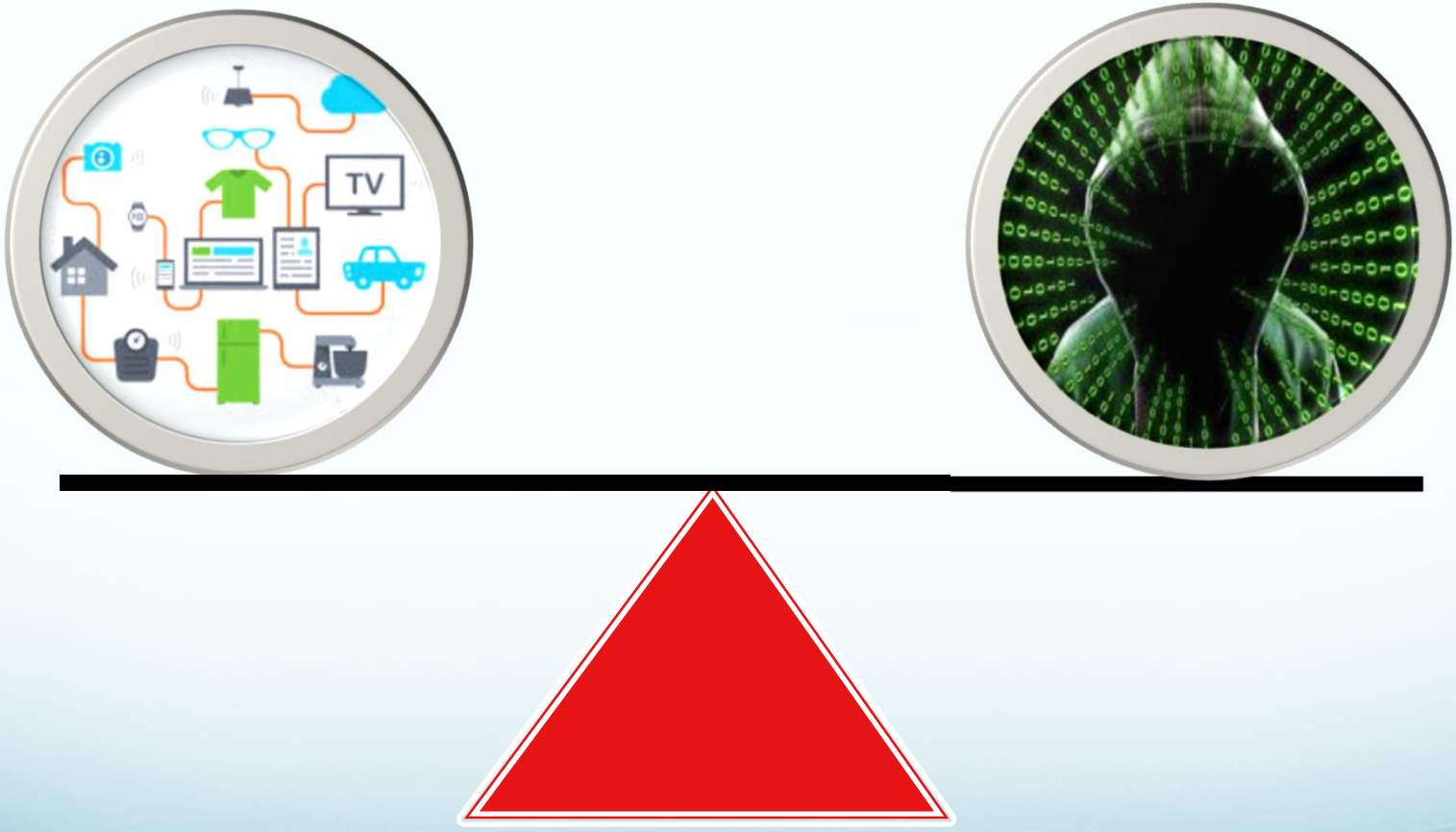
II. Un monde hyper connecté

III. Les menaces et Statistiques

V. Quelques règles d’hygiène

Menaces informatiques 2017/2018

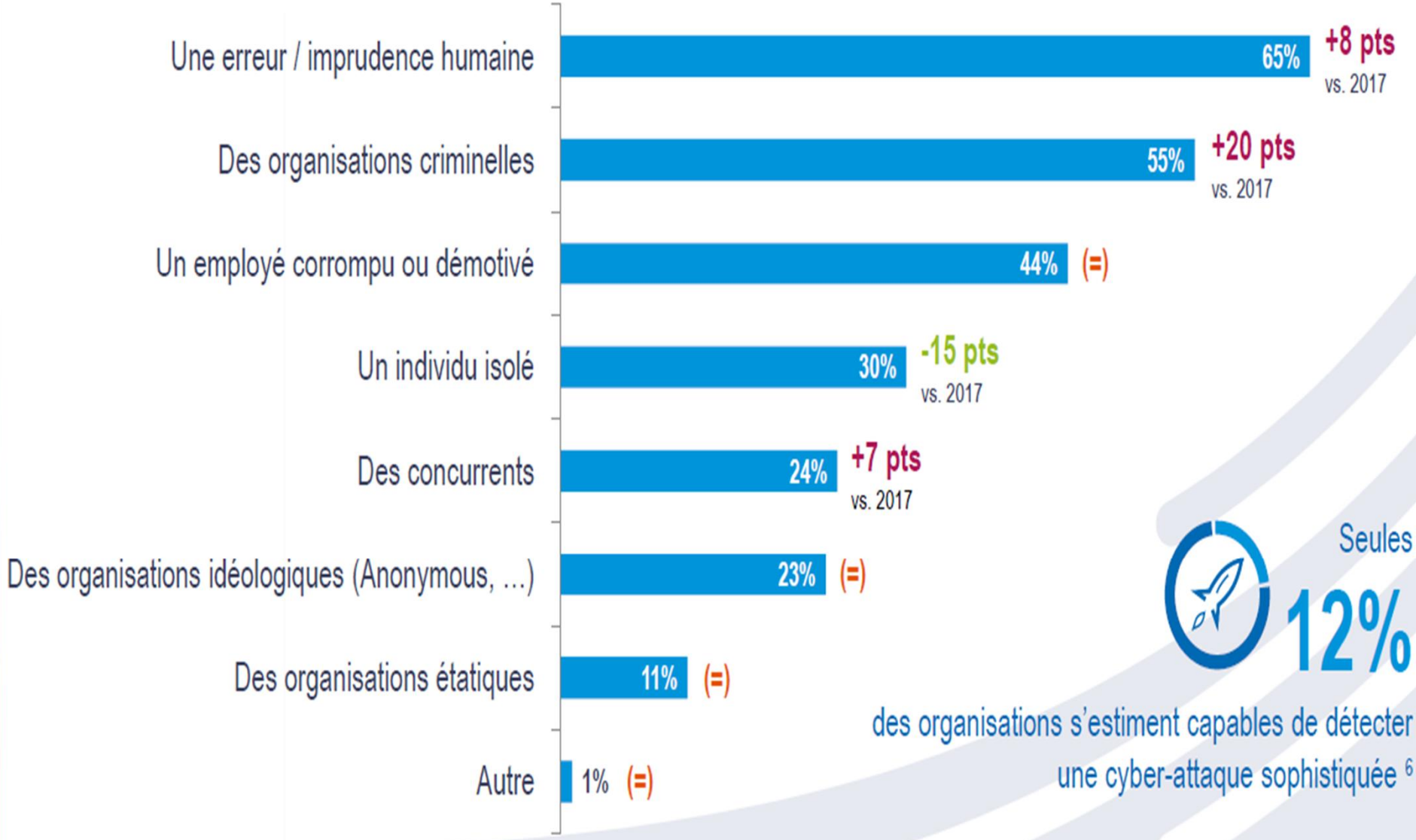
Plus la <u>technologie évolue</u>, plus les <u>menaces croissent</u> ?



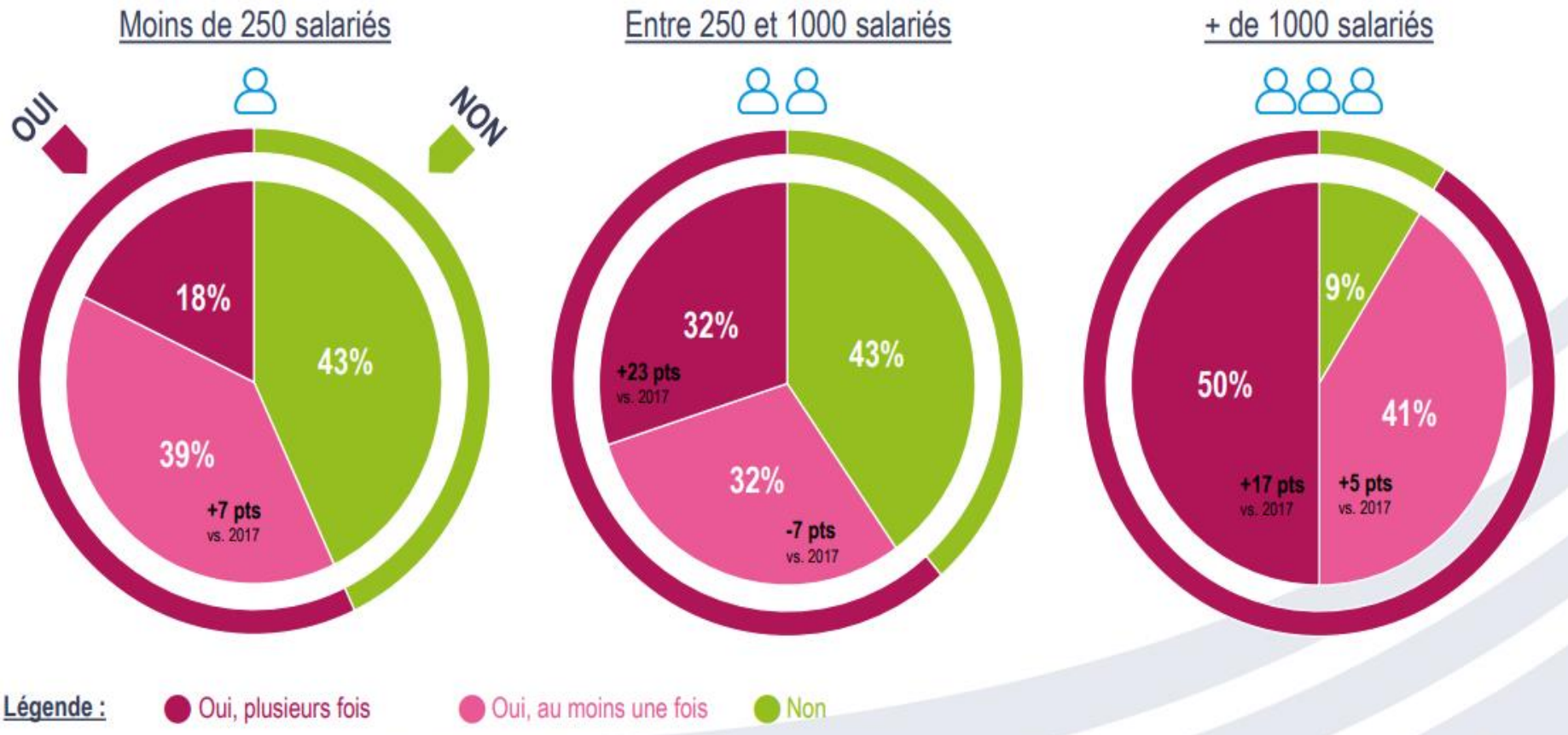
Rapport 2018

Sources : CFAO et CISCO

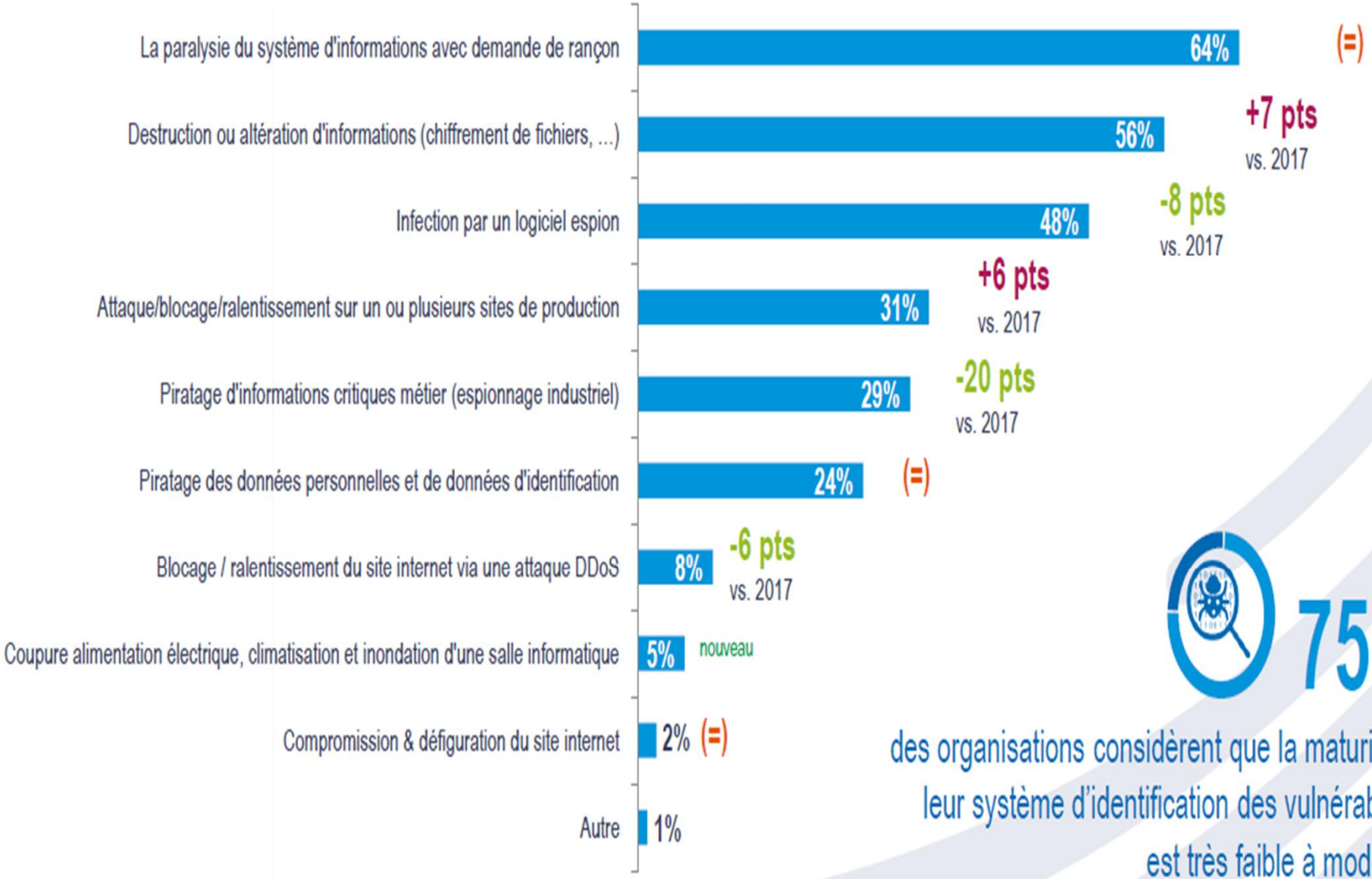
Les menaces potentielles des organisations



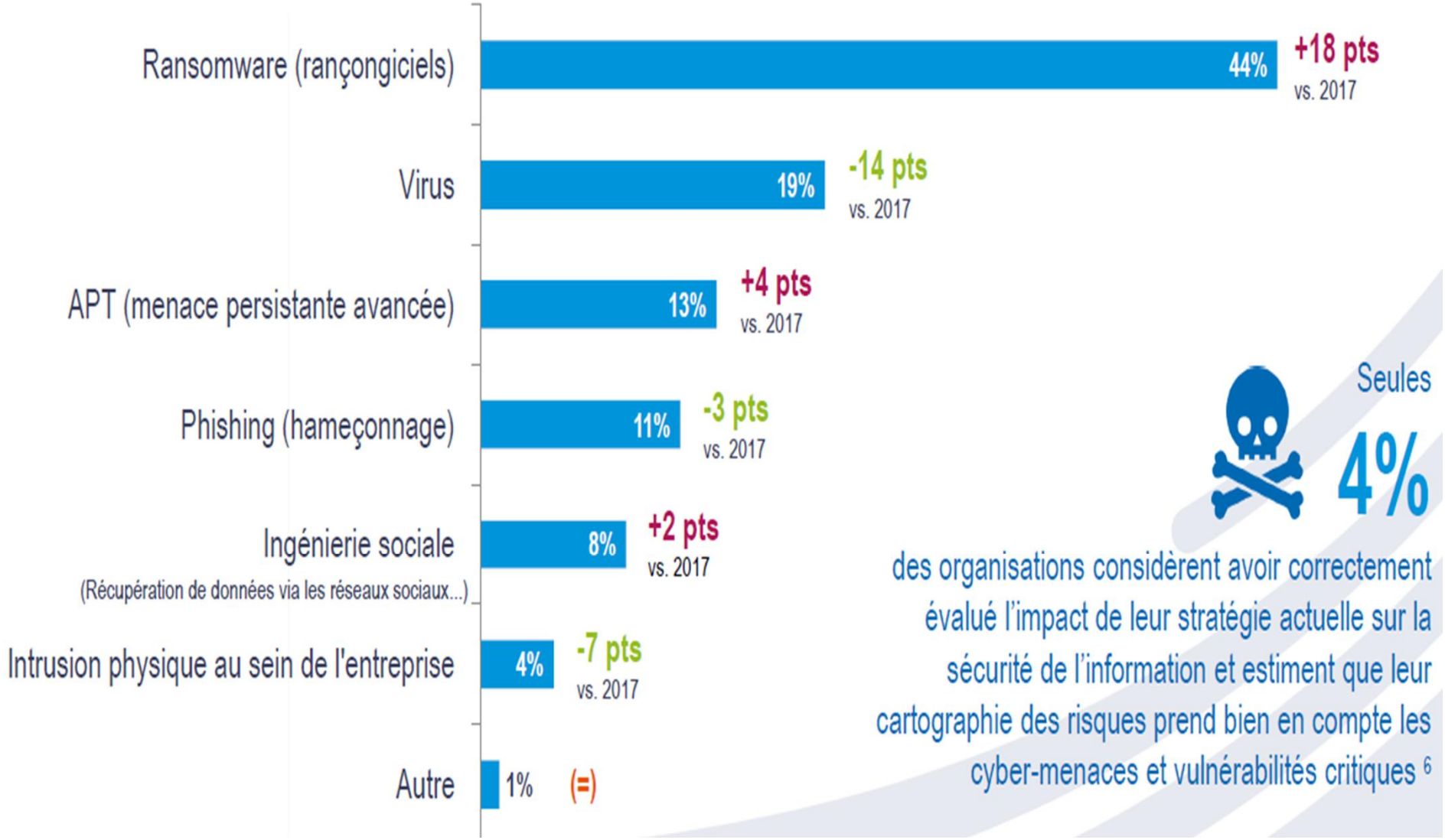
Taux d'employeur conscient que leur entreprise ait déjà été attaquée



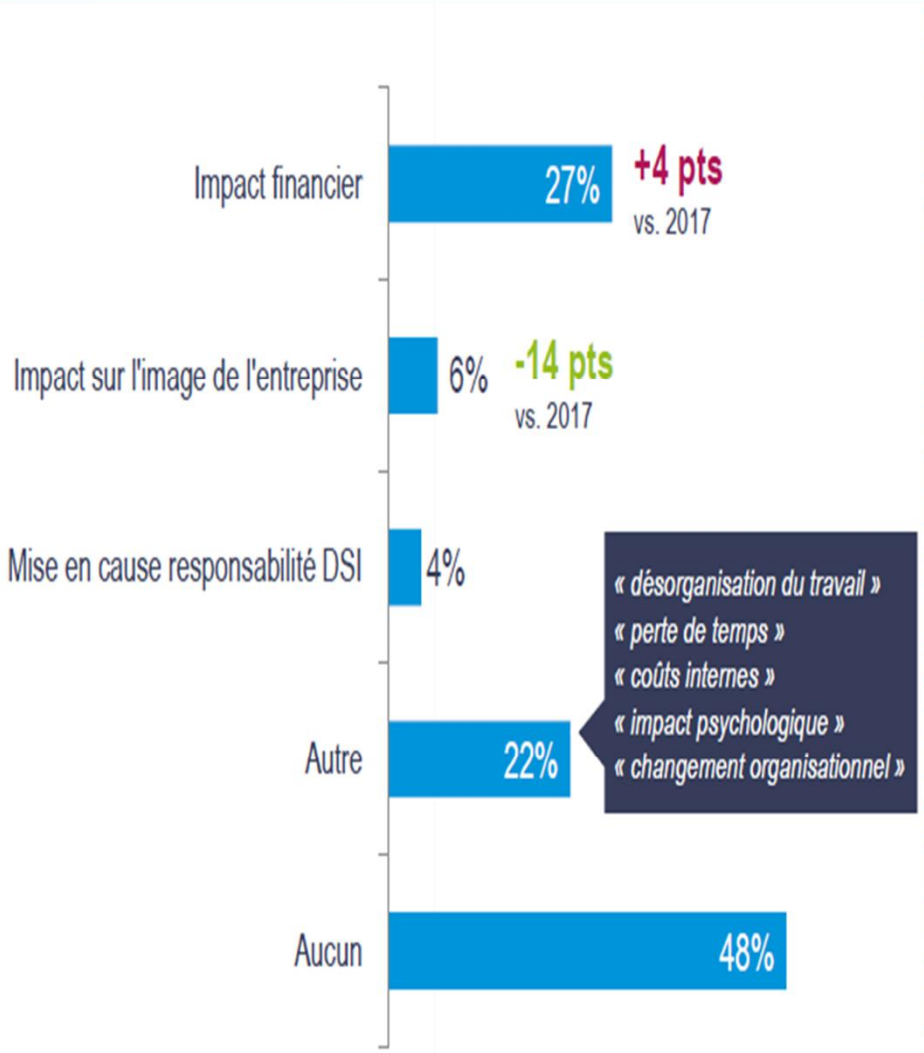
Attaques redoutées

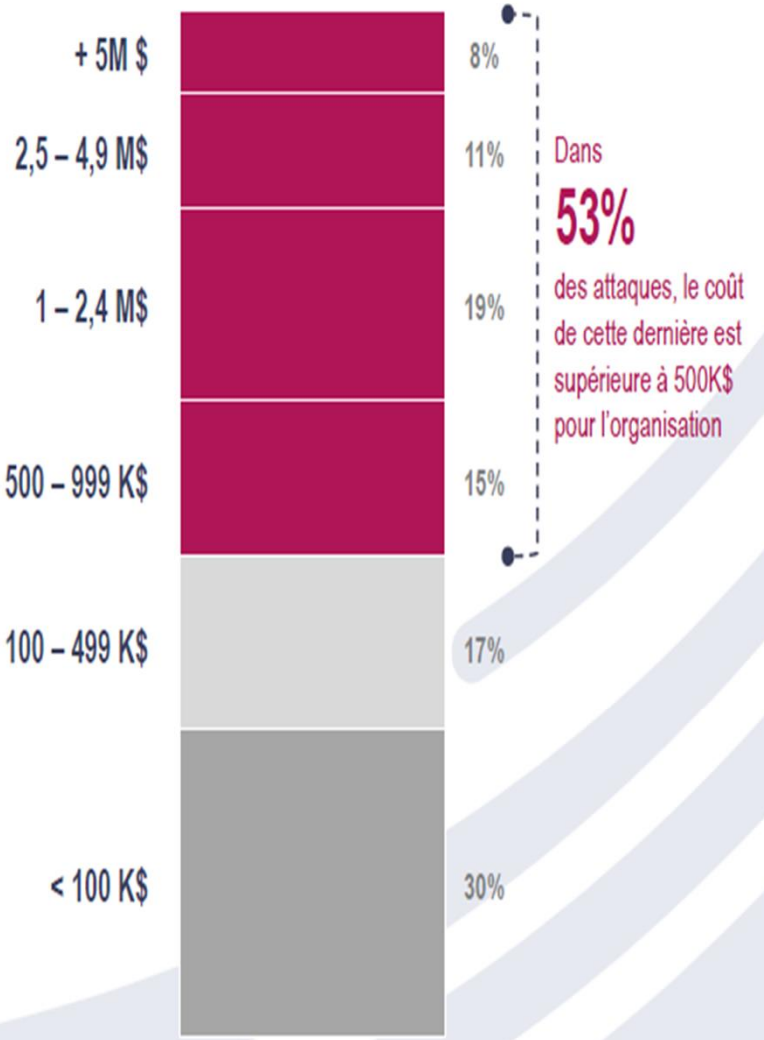


Menaces redoutées par les organisations

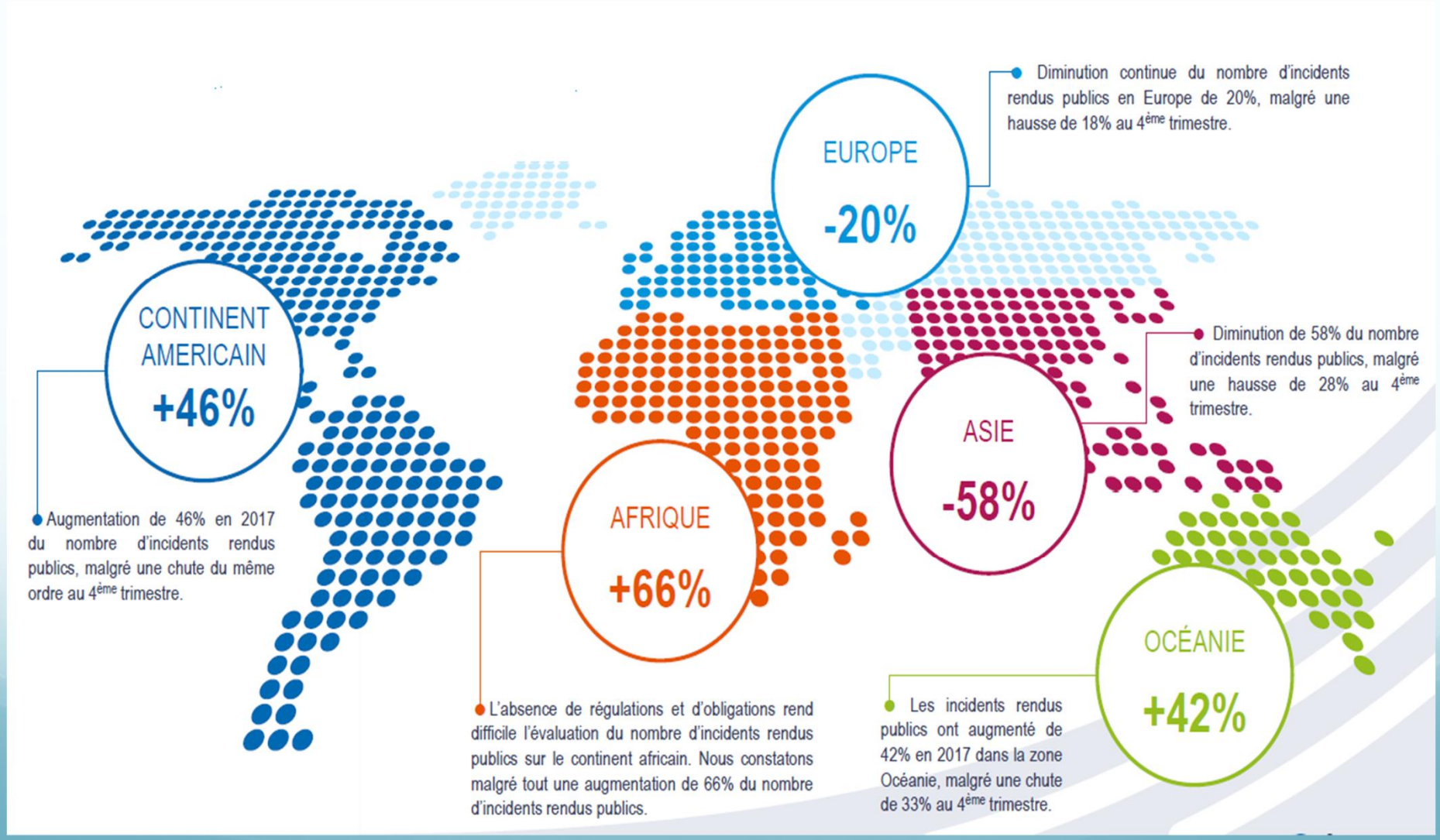


Impact des cyberattaques

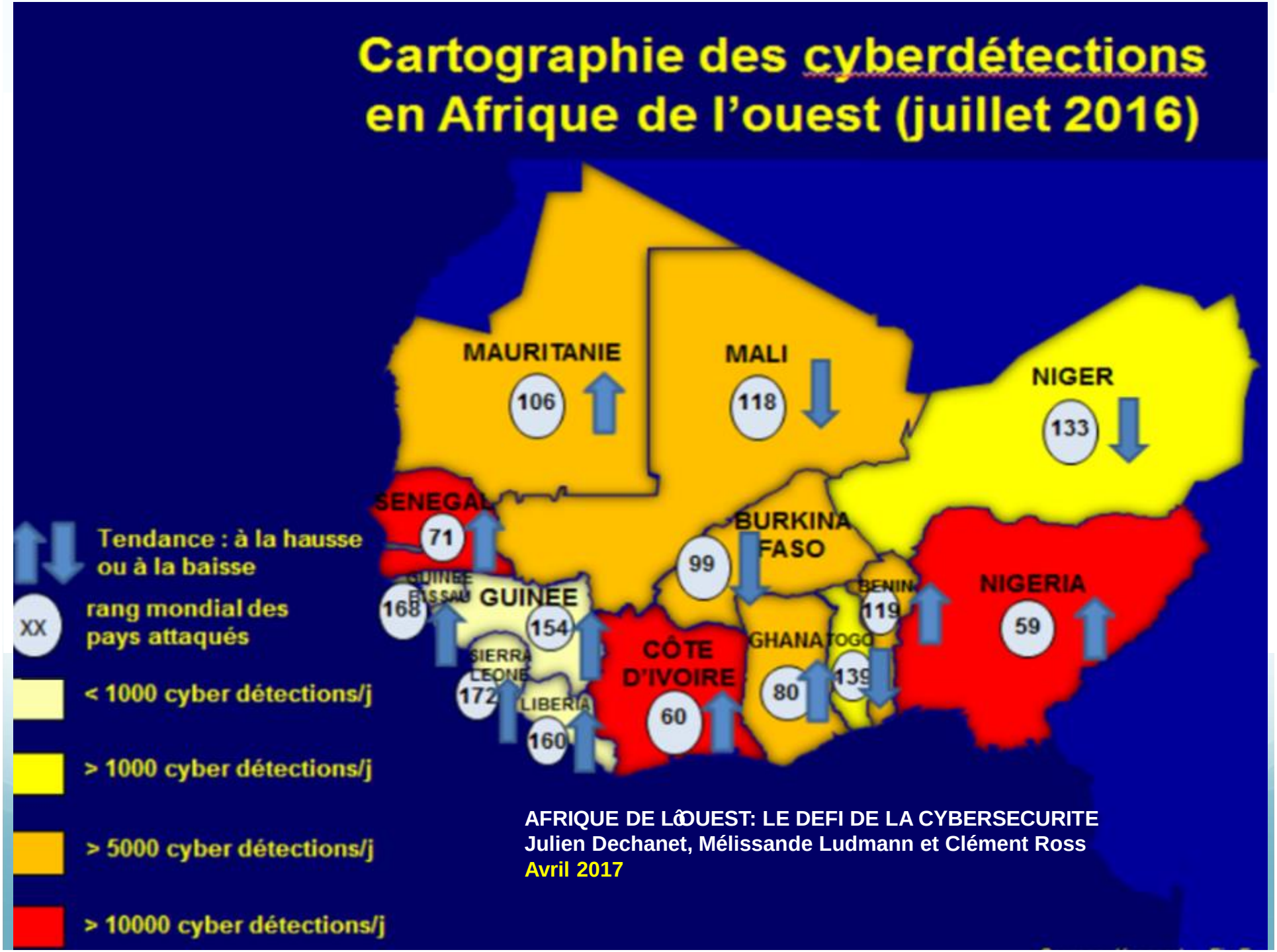




Cartographie des incidents par région



Sur l’Afrique de l’ouest


Cartographie des cyberdétections
en Afrique de l'ouest (juillet 2016)
MAURITANIE
106
MALI
118
NIGER
133
SENEGAL
71
BURKINA FASO
99
GUINEE
154
GUINEE BISSAU
168
SIERRA LEONE
172
LIBERIA
160
CÔTE D'IVOIRE
60
GHANA
80
TOGO
139
BENIN
119
NIGERIA
59
Tendance : à la hausse ou à la baisse
XX
rang mondial des pays attaqués
< 1000 cyber détections/j
> 1000 cyber détections/j
> 5000 cyber détections/j
> 10000 cyber détections/j
AFRIQUE DE LôOUEST: LE DEFI DE LA CYBERSECURITE
Julien Dechanet, Mélissande Ludmann et Clément Ross
Avril 2017

Cartographie des cyber-détections

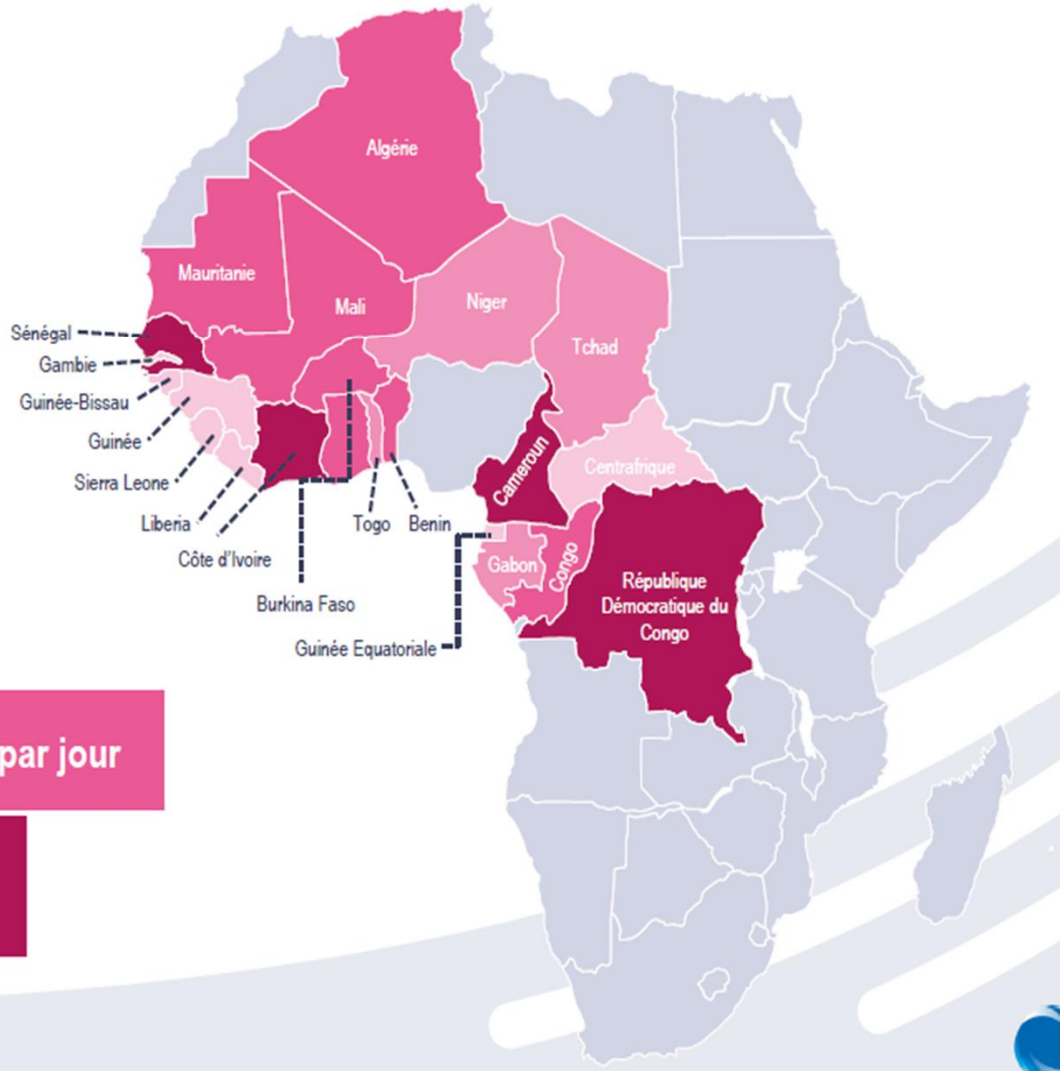
L'Afrique un continent exposé comme les autres. Longtemps l'Afrique a été considérée comme le berceau des cyber-criminels avec le Nigéria et l'Afrique du Sud comme principales bases des cyber-attaques qui ont touché des organisations, institutions et particuliers à travers le monde. Ce phénomène tend aujourd'hui à évoluer. Les organisations et institutions africaines évoluent pour accompagner l'essor des classes moyennes. Cette évolution s'accompagne par une transformation numérique de systèmes d'informations vieillissant voir obsolètes, peu sécurisés et administrés par des équipes ayant une faible maturité sur les sujets de la cyber-sécurité. Ces éléments expliquent l'intérêt grandissant et la recrudescence d'attaques auxquelles sont confrontées les organisations et institutions du continent Africain.

< 1000 cyber-détections par jour

> 1000 cyber-détections par jour

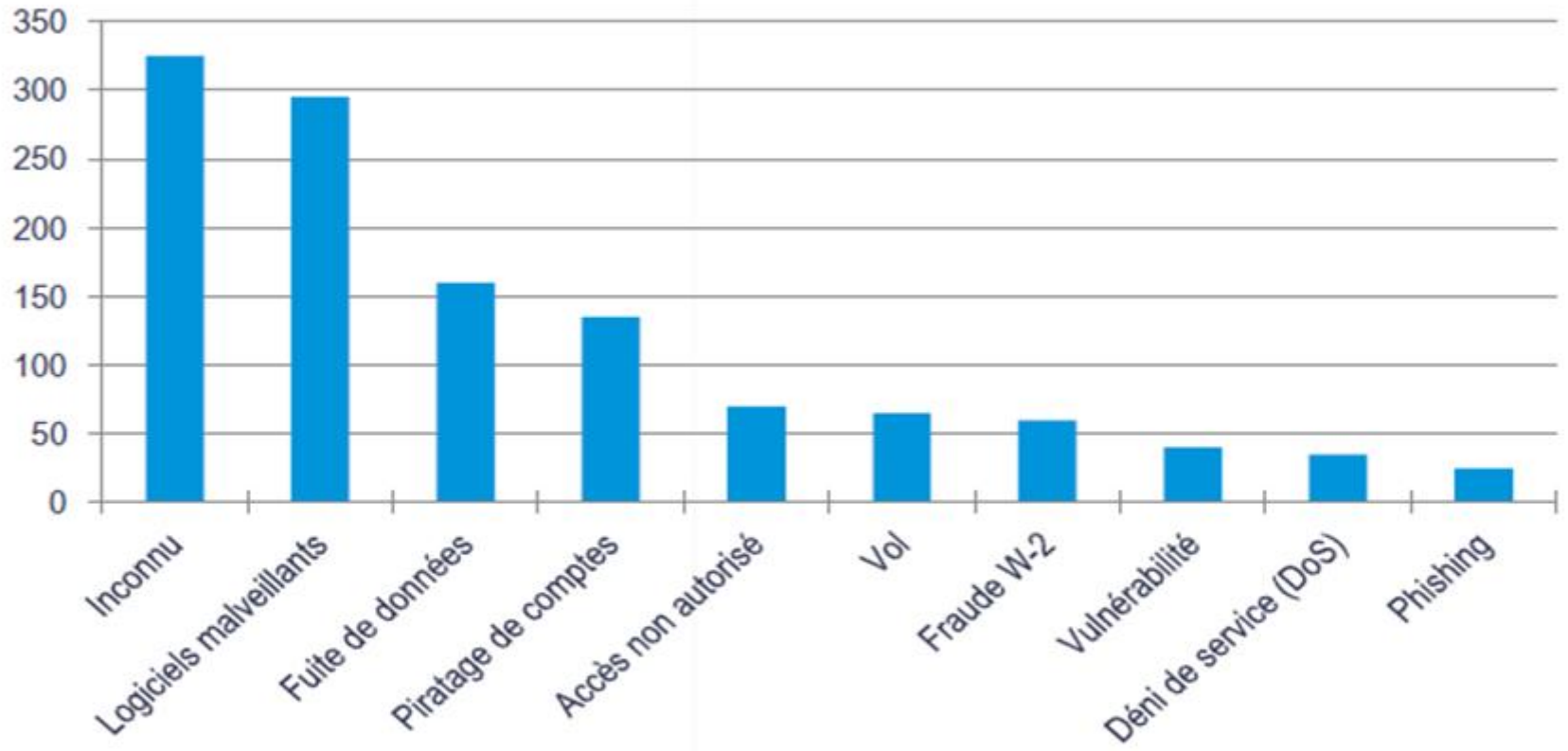
> 5000 cyber-détections par jour

> 10 000 cyber-détections par jour



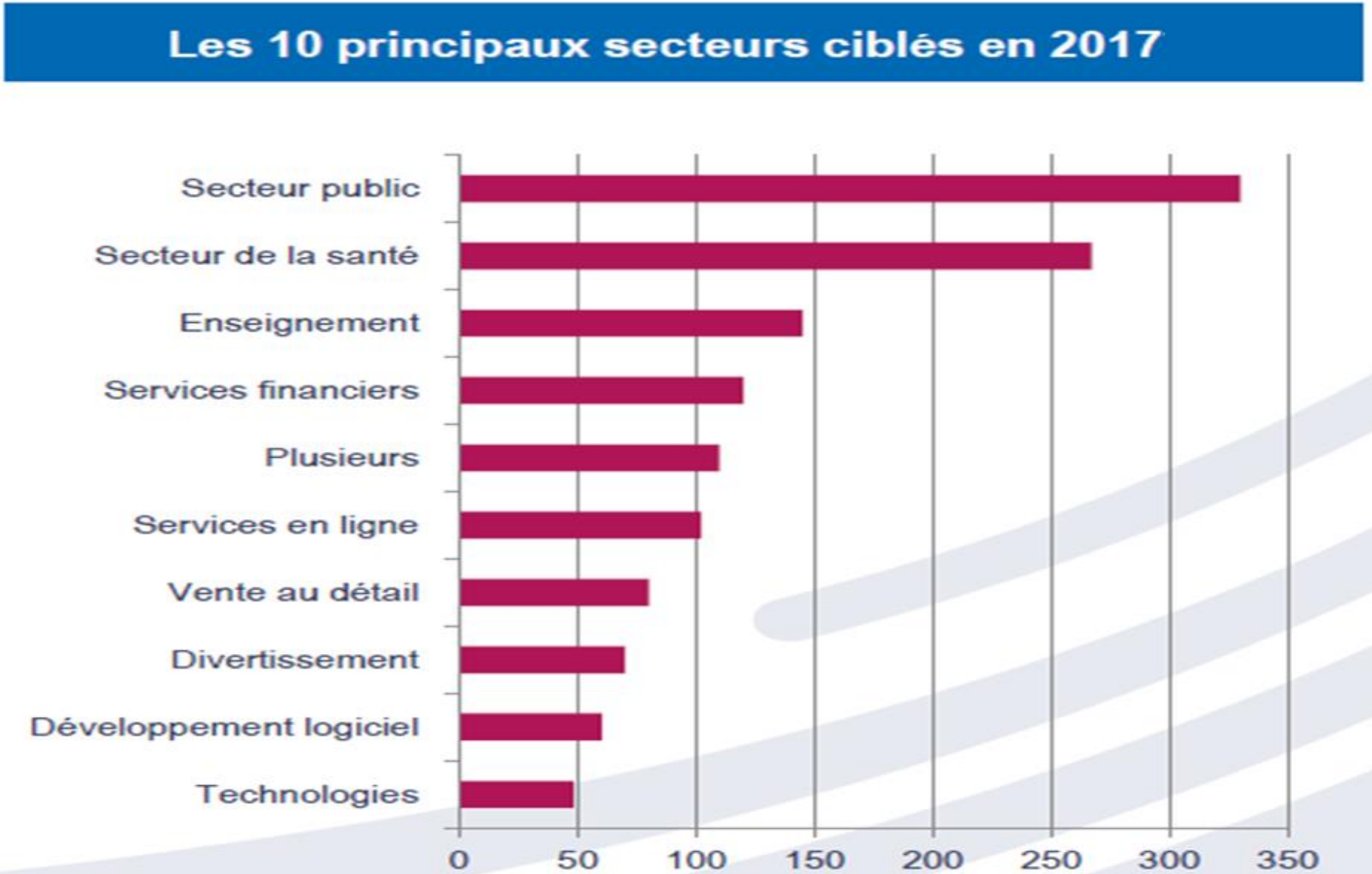
Vecteurs d'attaques et secteurs cibles

Les 10 principaux vecteurs d'attaques en 2017



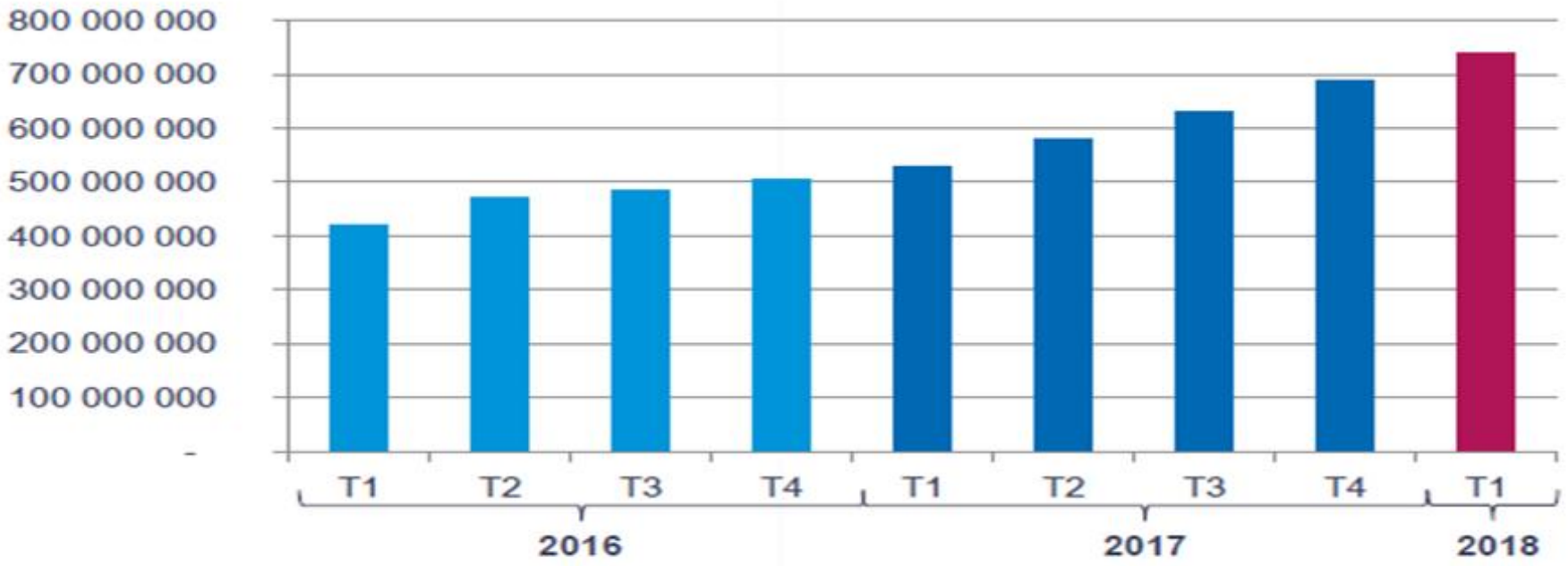
Pour la plupart, les vecteurs d'attaque sont inconnus ou n'ont pas encore été rendus publics. Cependant, on constate en 2017 une **augmentation de 29% des attaques déclarées par logiciels malveillants**, chiffre sensiblement proche du nombre de nouveaux logiciels malveillants référencés l'année passée (+36%). A l'inverse, les attaques par **déni de service (DoS)** et les **piratages de comptes ont diminué** respectivement de **-75% et -35%**. Les autres vecteurs d'attaques sont stables en terme de pourcentage sur les deux dernières années.

Vecteurs d'attaques et secteurs cibles



Statistiques des logiciels malveillants

Nombre total de logiciels malveillants (malwares) en T1 2018



L'année 2017 a confirmé le renforcement de l'arsenal informatique des cyber-criminels avec une **progression continue (+36%) sur l'année du nombre de nouveaux logiciels malveillants référencés**. Ces nombreux outils à disposition de cyber-criminels mieux organisés leur offre **plus d'agilité pour adopter de nouvelles stratégies et tactiques** de cyber-attaques. T2 et T3 2017 ont été émaillés par des attaques de rançongiciels, de compromission de base de données et fuites d'informations, tandis que le 4ème trimestre s'est caractérisé par le déploiement de nouveaux outils tels que les logiciels malveillants sans fichier (PowerShell) et le minage de cryptomonnaies en raison de la prise de valeur du bitcoin.

Les failles de sécurité de la Mobilité

Conseils pour la sécurité de la Mobilité

1. Sensibiliser vos collaborateurs

Sensibiliser les collaborateurs sur les caractéristiques et les conséquences des attaques par hameçonnage (phishing) et connexion à des points Wi-Fi non sécurisés, c'est anticiper une partie des menaces qui proviennent de l'interne (40%),

2. Définir la sensibilité au risque de l'organisation

Mettre en place des politiques d'identités et d'accès aux données basées sur une hiérarchisation des rôles, une classification des données par confidentialité et sensibilité au risque avec un suivi en temps réel des activités de données.

3. Renforcer la sécurité de base intégrée des appareils mobiles

Rendre obligatoire l'authentification à double facteur sur les mobiles : mot de passe et biométrie, s'assurer de l'application des mises à jour des OS, applications, correctifs et règles de sécurité, activer la localisation des terminaux et la suppression à distance des données.

4. Séparer les données personnelles et professionnelles

Créer des espaces de travail mobiles conteneurisés et sécurisés pour travailler, collaborer et partager tout en s'assurant que les données d'entreprise et personnelles restent privées et séparées. Ceci facilite l'encryptage des données et l'application des politiques de sécurité.

5. Mieux vaut prévenir que guérir

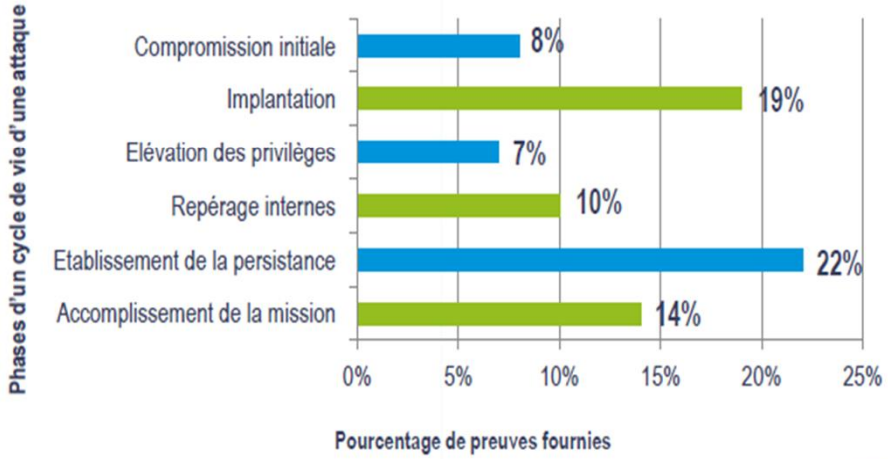
Intégrer la sécurité de la mobilité comme une composante à part entière de votre système d'informations et non pas une brique de sécurité externe.

Conséquences du manque de compétences

9 à 12

nombre minimum de salariés à plein temps nécessaires pour piloter un centre de cyber-défense opérationnel 24h/7j[14]

Il existe aujourd'hui une pénurie de spécialistes de la sécurité capables d'identifier une menace réelle dans un flot d'alertes constant, déficit d'autant plus criant au moment de la compromission initiale (8% de détection)



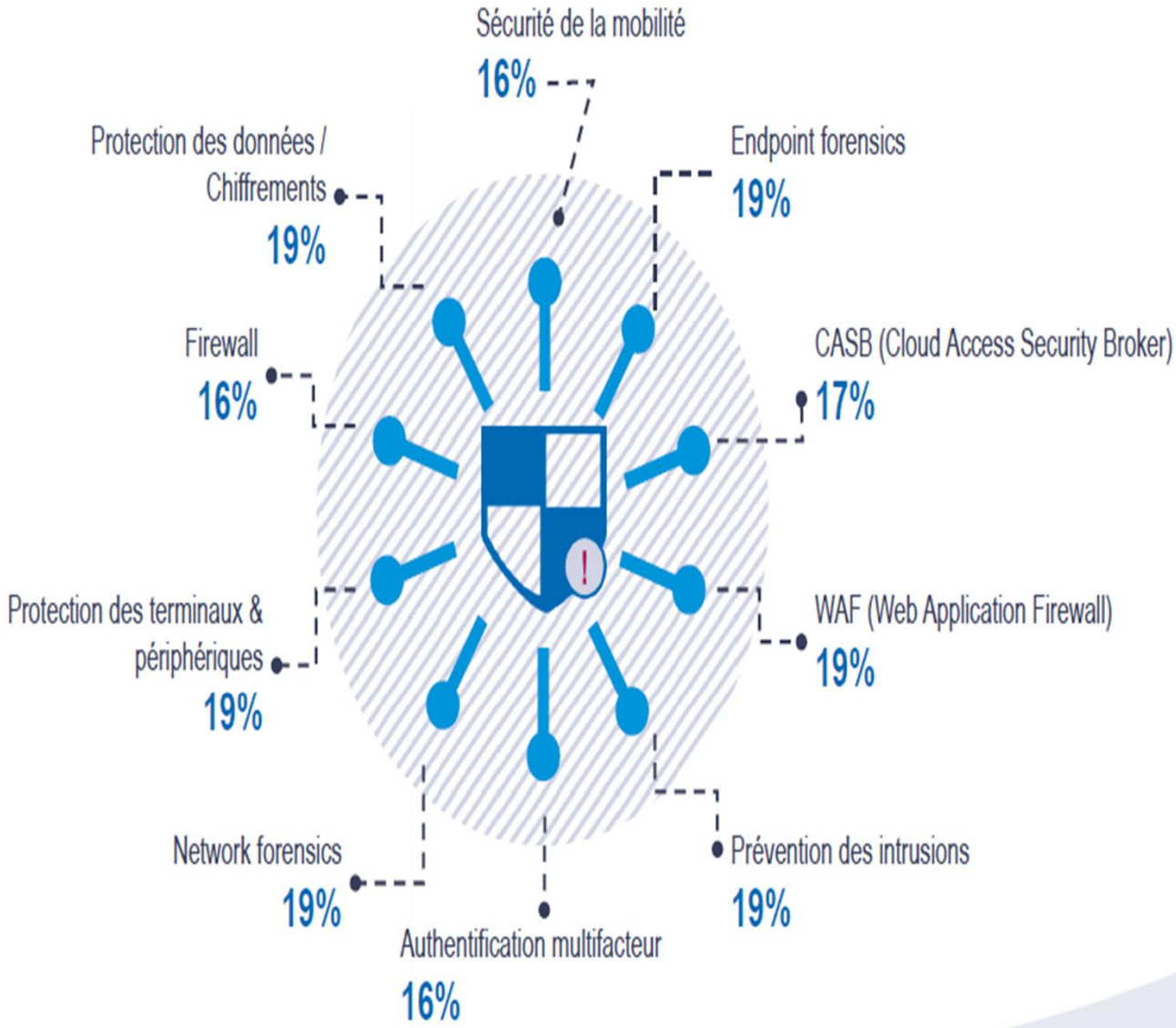
48% des organisations n'ont pas de centre de gestion des incidents (SOC - Security Operations Center)[6]

57% des organisations n'ont pas de programme de cyber-sécurité formel.[6]

VOICI LES QUESTIONS QUE TOUT PROFESSIONNEL DE LA SÉCURITÉ DOIT AUJOURD'HUI SE POSER :

- Quels outils utilisent nos salariés dans leur quotidien?
- Comment sécuriser leurs activités extra-professionnelles ?
- Comment les accompagner dans cette démarche ?
- Quelles politiques souhaitons-nous mettre en place ?
- Ces politiques sont-elles applicables dans la pratique ?

Axes de renforcement de la sécurité

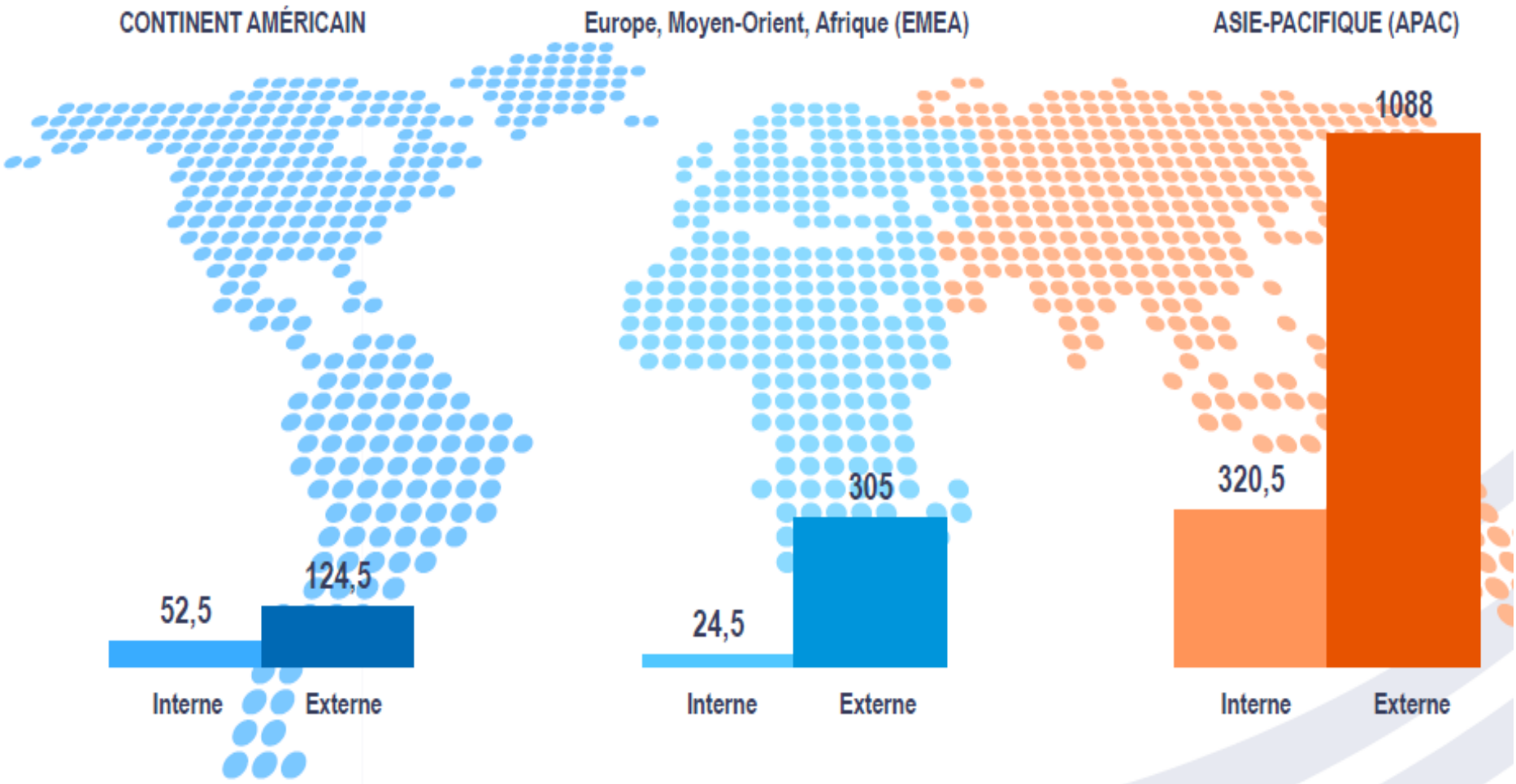


RECOMMANDATIONS :

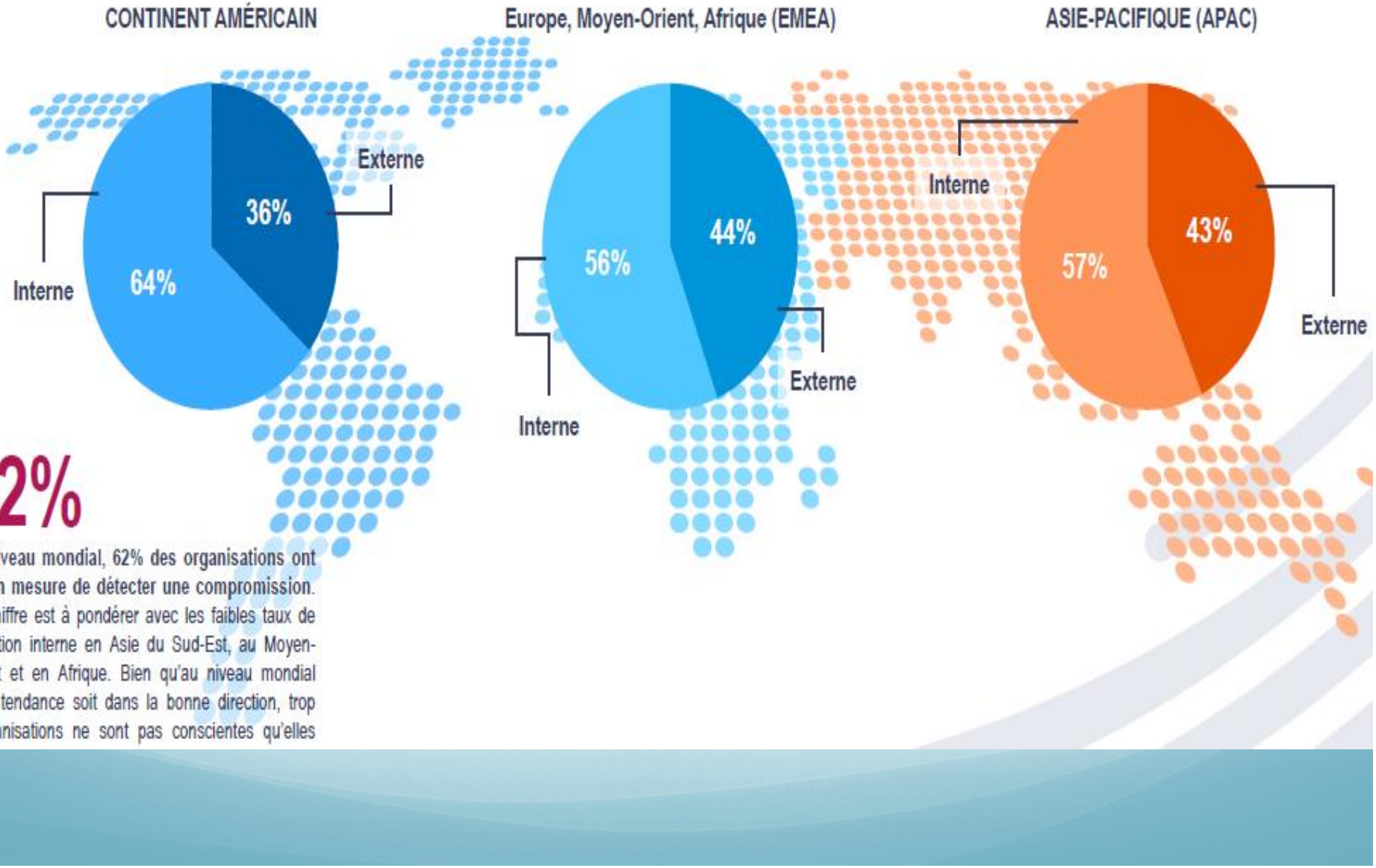
En complément de ces principaux axes pour renforcer la sécurité du S.I, les experts de CFAO Technology & Energy conseillent de prêter attention aux 3 axes suivants.

+ Audit de la politique globale de sécurité
+ Plan de réponse sur incident
+ Politique de gestion de la sauvegarde des données (backup)

NOMBRE MÉDIAN DE JOURS POUR DÉTECTER UNE CYBER-ATTAQUE SELON LA SOURCE DE DÉTECTION



SOURCE DE DÉTECTION DE LA CYBER-ATTAQUE



62%

Au niveau mondial, 62% des organisations ont été en mesure de détecter une compromission. Ce chiffre est à pondérer avec les faibles taux de détection interne en Asie du Sud-Est, au Moyen-Orient et en Afrique. Bien qu'au niveau mondial cette tendance soit dans la bonne direction, trop d'organisations ne sont pas conscientes qu'elles

CIBLE UN JOUR,
CIBLE TOUJOURS

Les entreprises victimes d'attaques ciblées ont de fortes chances de faire l'objet de récidives.

56%
des organisations ont subi une attaque en 2017

40%
ont été attaqués par plusieurs groupes .

C'est dans les vieux pots qu'on fait la meilleure soupe. En 2018, les bonnes vieilles méthodes seront toujours au rendez-vous : phishing et techniques d'ingénierie sociale pour la propagation des malwares. A ces artifices devraient s'ajouter les malvertising pour duper les utilisateurs, l'usage de logiciels de surveillance et une hausse du volume de vers et autres malwares à propagation rapide. Au regard de la conjoncture géopolitique actuelle, cet arsenal complet servira au vol de données qui restera l'un des principaux axes d'attaques des cyber-criminels.

Hausse des attaques de Phishing basées sur les domaines HTTPS avec une augmentation de 186% de la fréquence de ces attaques qui visent à compromettre des sites web légitimes, domaines récemment enregistrés ou encore des URL raccourcies pour rediriger l'utilisateur vers des sites de phishing **& Exploitation** des vulnérabilités dans les algorithmes et protocoles de cryptographie comme le SSL/TLS avec une forte augmentation du nombre de failles divulguées.

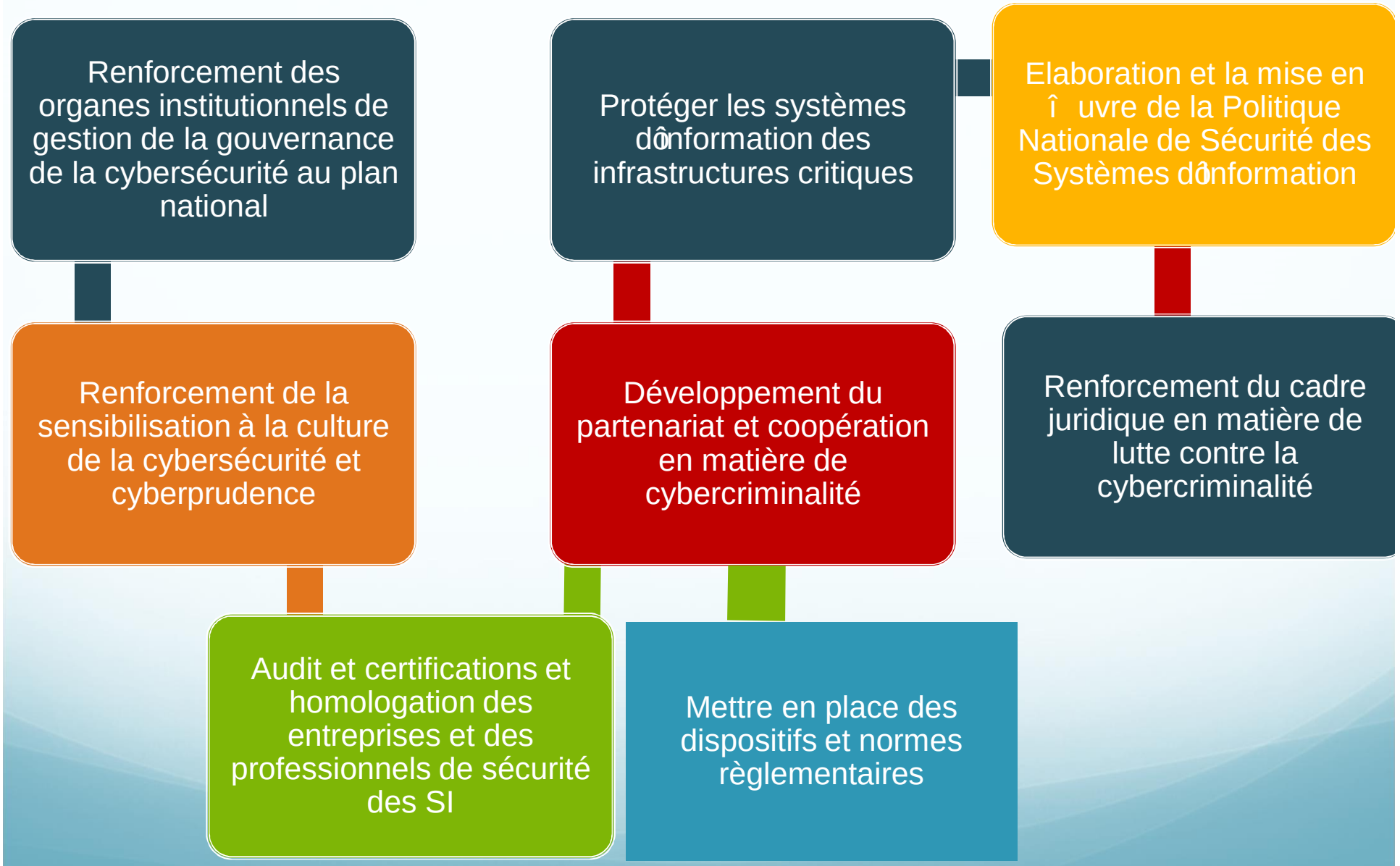
II. Un monde hyper connecté

III. Les menaces et statistiques

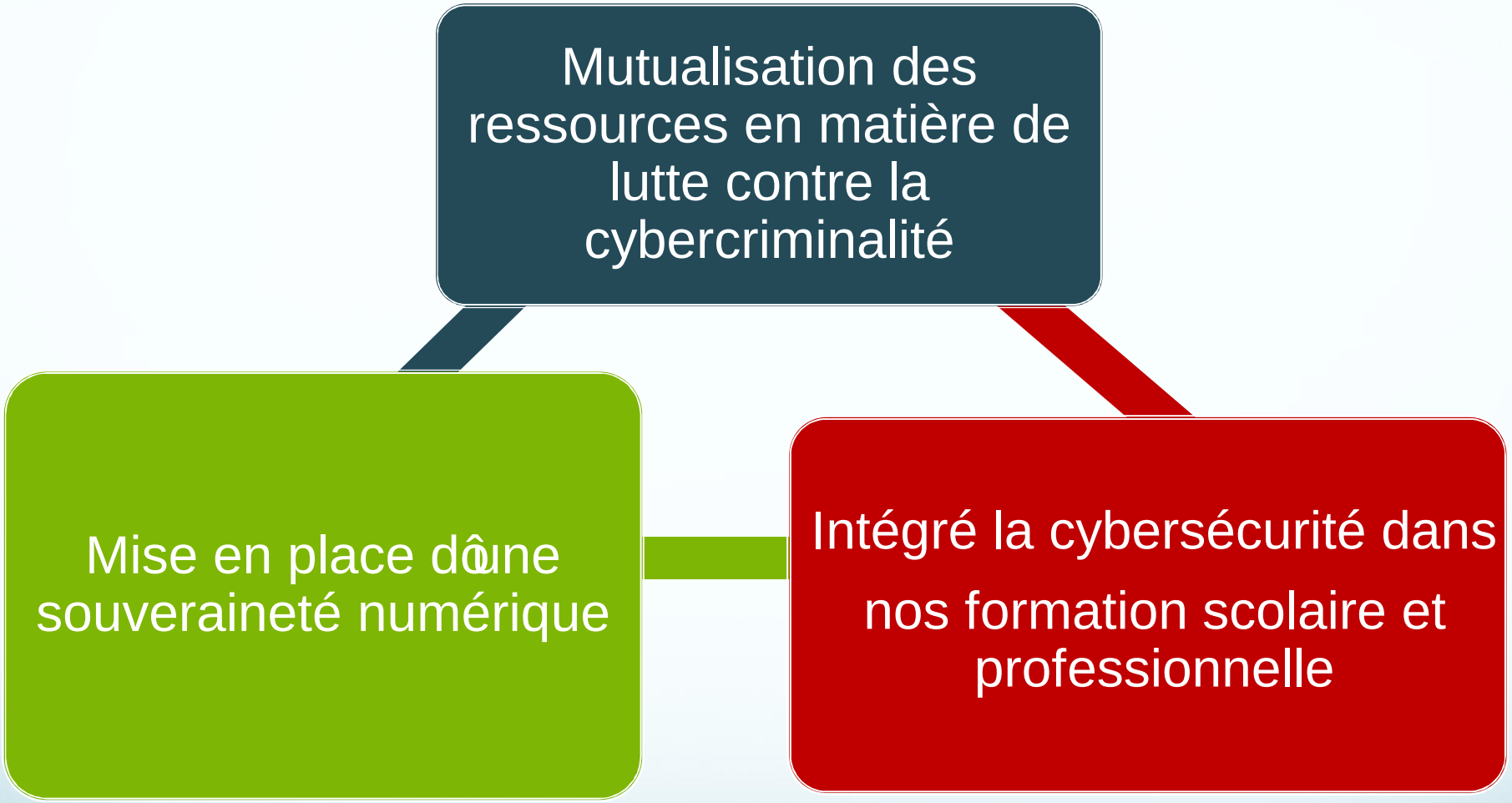
V. Quelques règles d'hygiène

Au niveau national

LES DEFIS DE LA CYBERSECURITE



Perspectives



Au niveau individuel

SE PROTÉGER DES ATTAQUES CIBLÉES

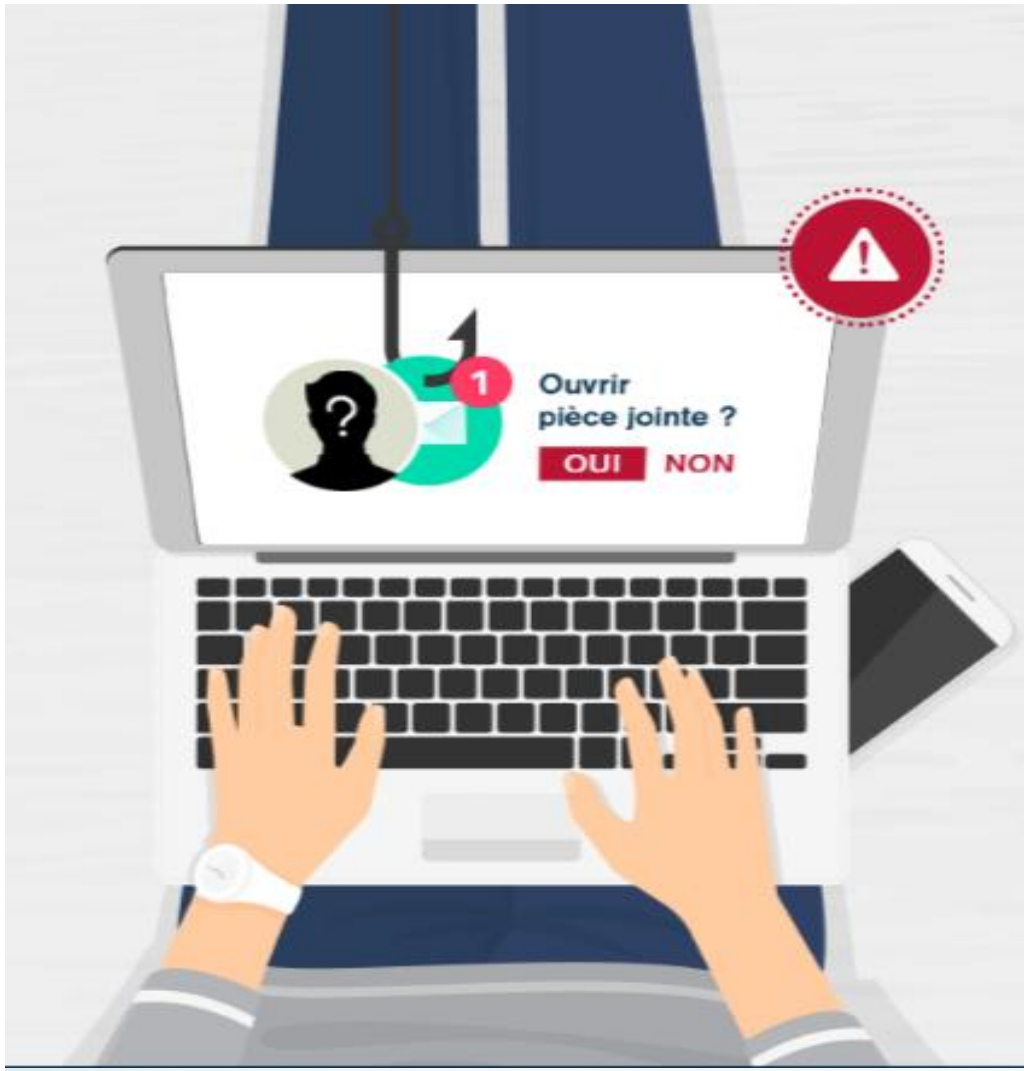
1

Détruire les messages non-sollicités sans répondre

SE PROTÉGER DES ATTAQUES CIBLÉES

2

Choisir des mots de passe sécurisés



SE PROTÉGER DES ATTAQUES CIBLÉES

3

Ne pas exécuter d'instructions venant d'un inconnu

SE PROTÉGER DES ATTAQUES CIBLÉES

4

Toujours effectuer les mises à jour

SE PROTÉGER DES ATTAQUES CIBLÉES

5

Ne pas diffuser d'informations personnelles et/ ou confidentielles sur Internet

Effectuer les sauvegardes régulières

En sommes adopter un comportement cyberprudent surtout sur les réseaux sociaux, lors des déplacement, lors des achats en ligneé

Seul on va vite,

mais ensemble on va loin…

é The End