Orientations stratégiques pour une meilleure cyber-résilience

Pr. Chérif DIALLO

PhD, CISSP, CCNP, CCDP

Professeur Titulaire en Informatique

UFR SAT, UGB



PLAN

I. Introduction

II. Contexte & Problématique

III. Cycle stratégique pour une meilleure cyber-résilience

IV. Conclusion



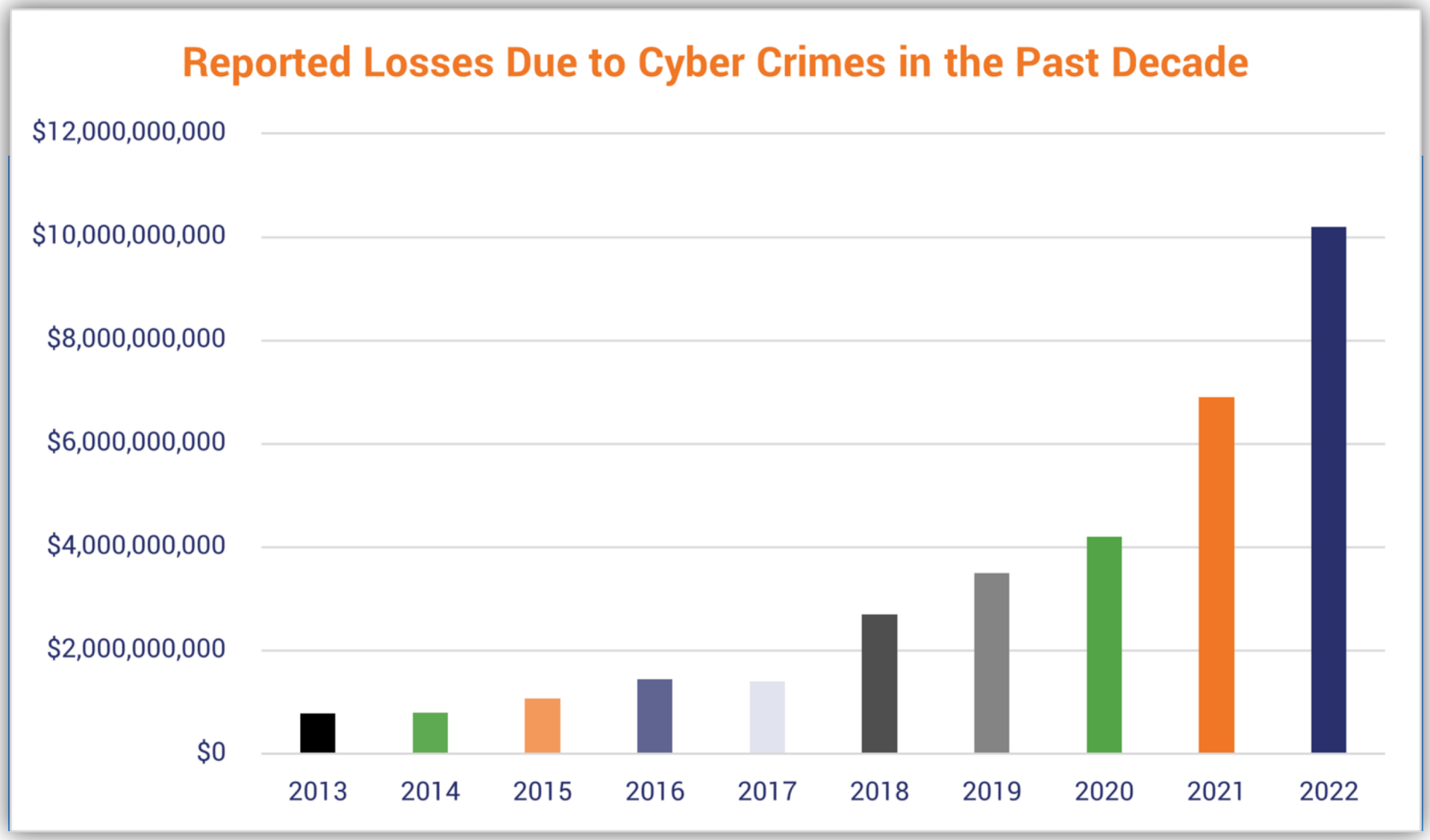
Introduction

- La cyber-résilience est la capacité à se préparer, à résister et à se remettre d'une cyberattaque, d'une menace ou d'une perturbation.
- Les cybermenaces continuant d'évoluer et de se développer, il est essentiel que les organisations élaborent une stratégie de cyber-résilience afin de protéger leur infrastructure informatique, leurs données, leurs clients et leurs opérations.

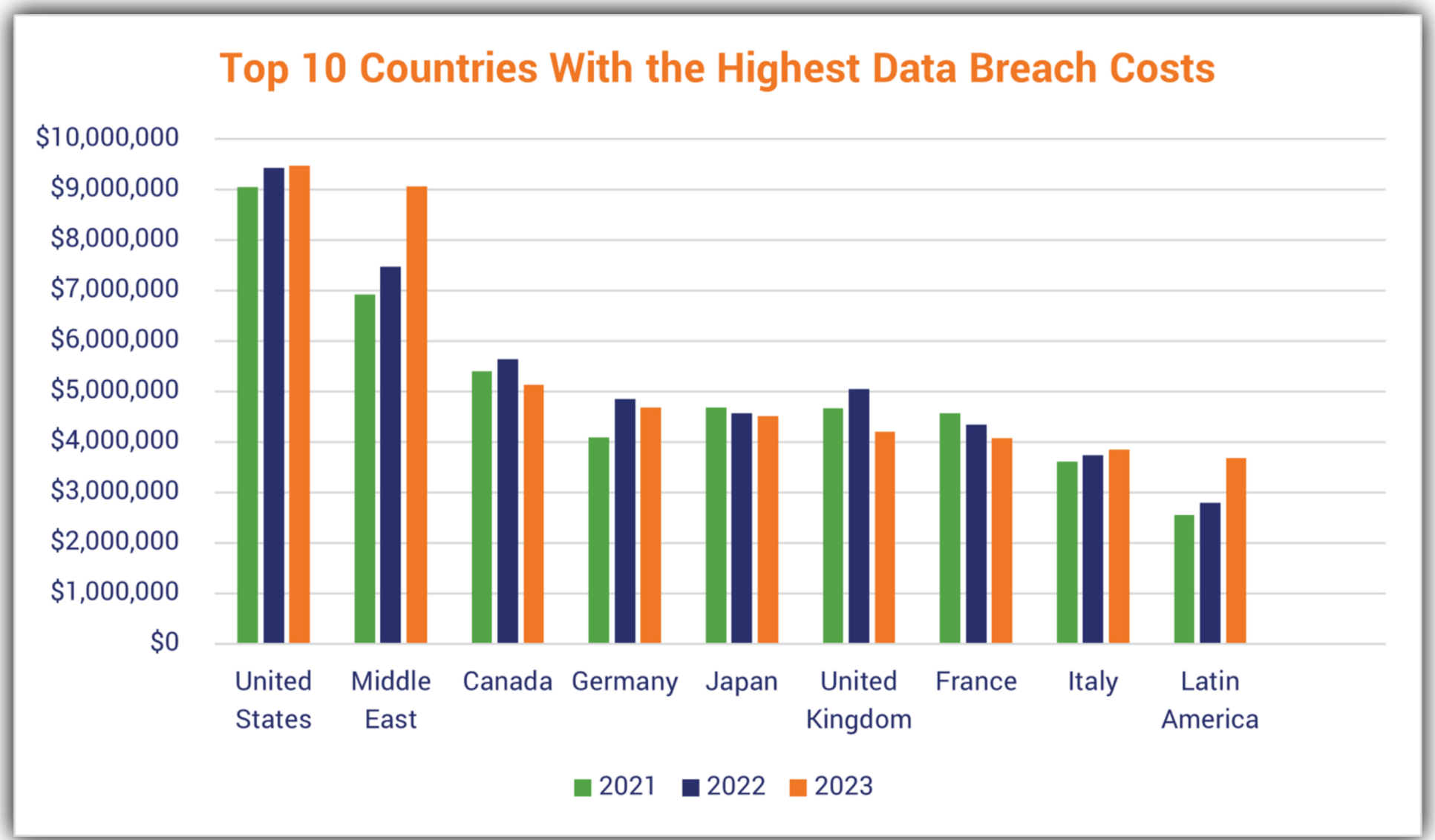
Contexte & Problématique

Quelques statistiques (Fr, en 2023)

- Le coût moyen d'une violation de données pour une PME s'élève à 130 000 €.
- 41 % des PME ne parviennent pas à récupérer leurs données après une violation.
- 94 % des malwares sont distribués par le biais de courriers électroniques.
- Un tiers des entreprises ayant versé une rançon a été confronté à une nouvelle attaque.
- On recense 330 000 attaques réussies contre les PME au cours de l'année 2023.

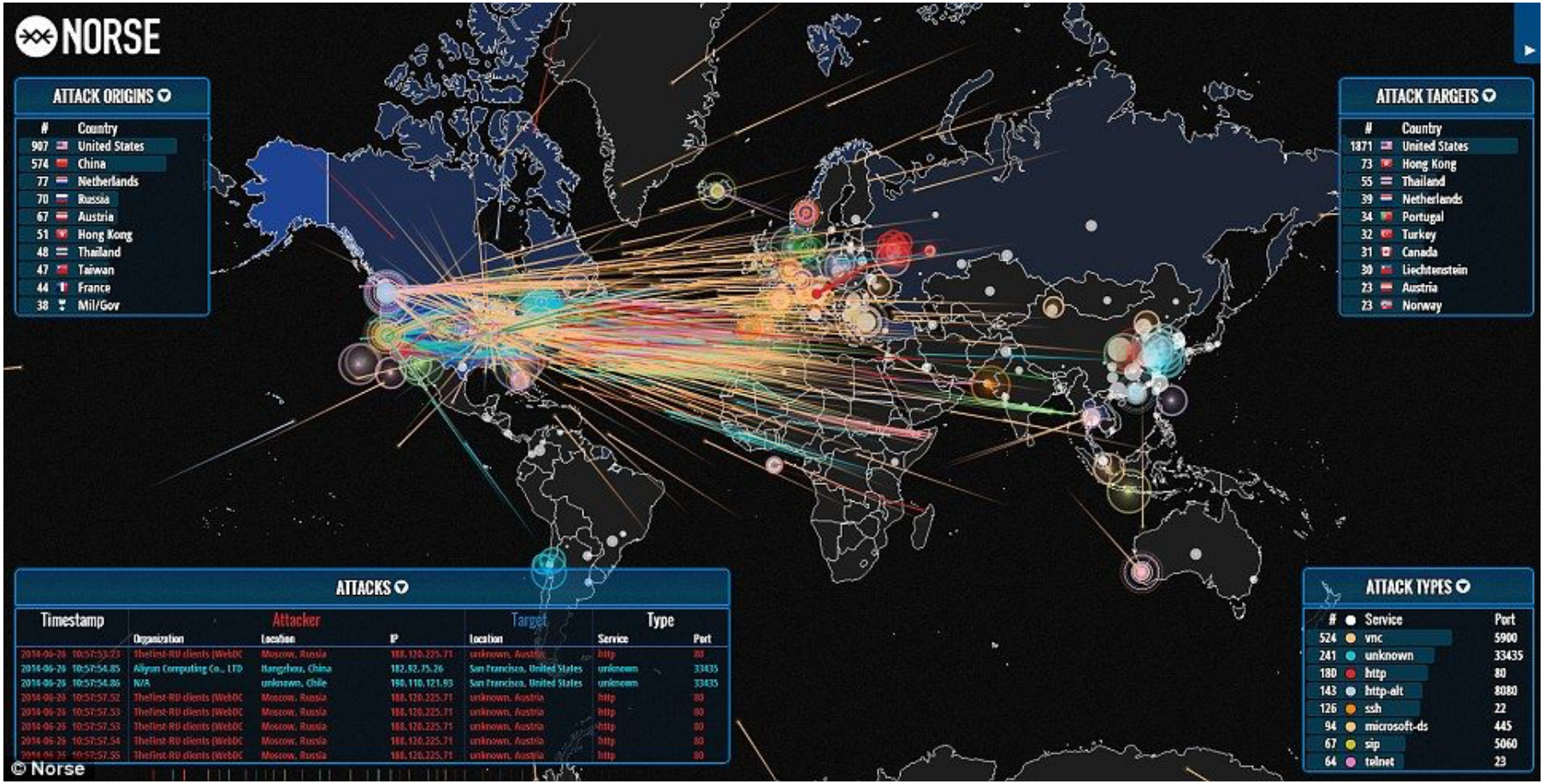


Data sources: FBI Internet Crime Complaint Center Internet Crime Reports for 2018, 2021 and 2022



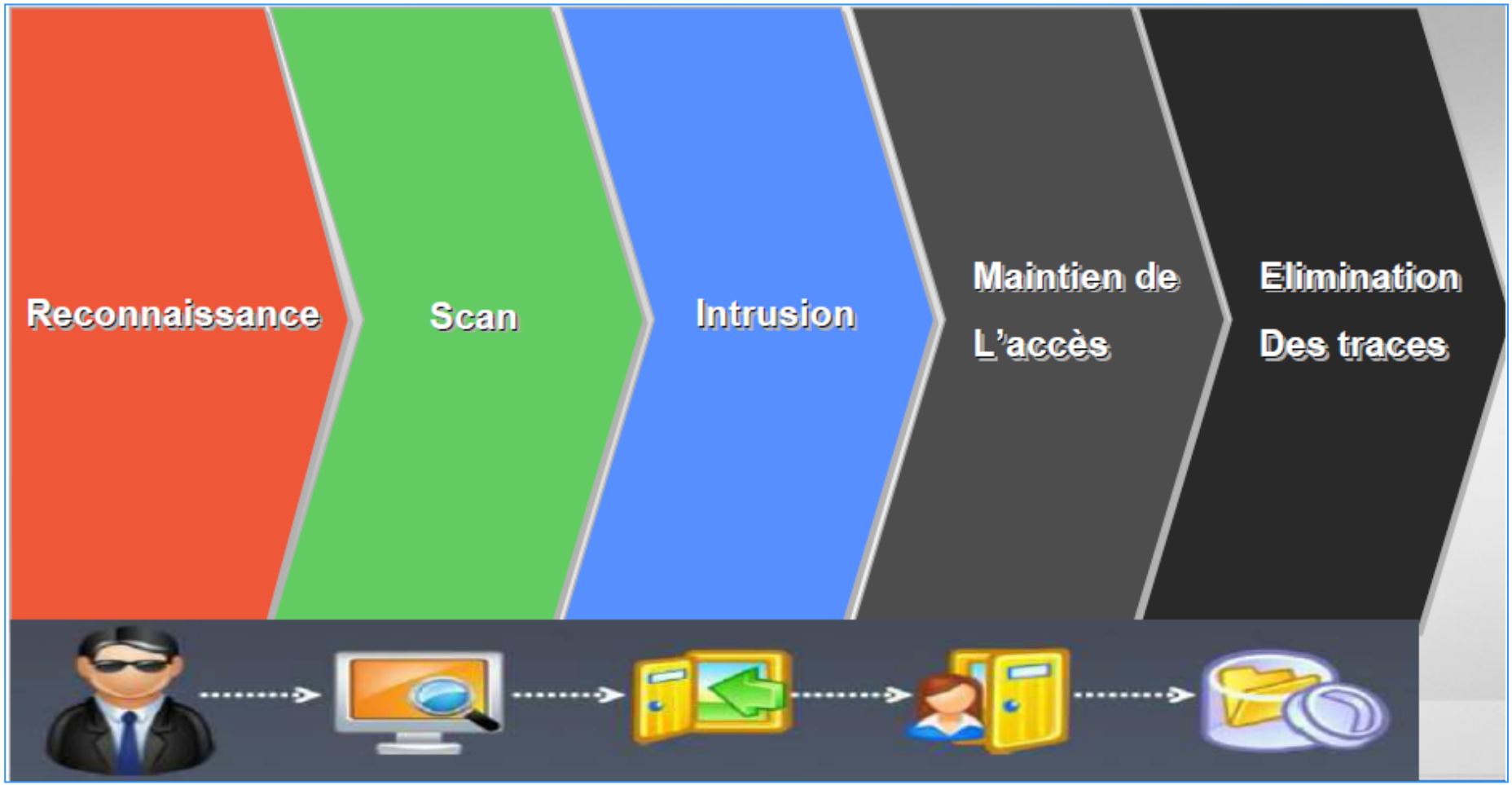
Data source: IBM's Cost of a Data Breach 2022 and 2023 reports. This chart serves as an overview of the growing costs of data breaches over the past three years.

Attaques en temps réel dans le monde



Contexte & Problématique

- Les étapes d'une attaque cyber

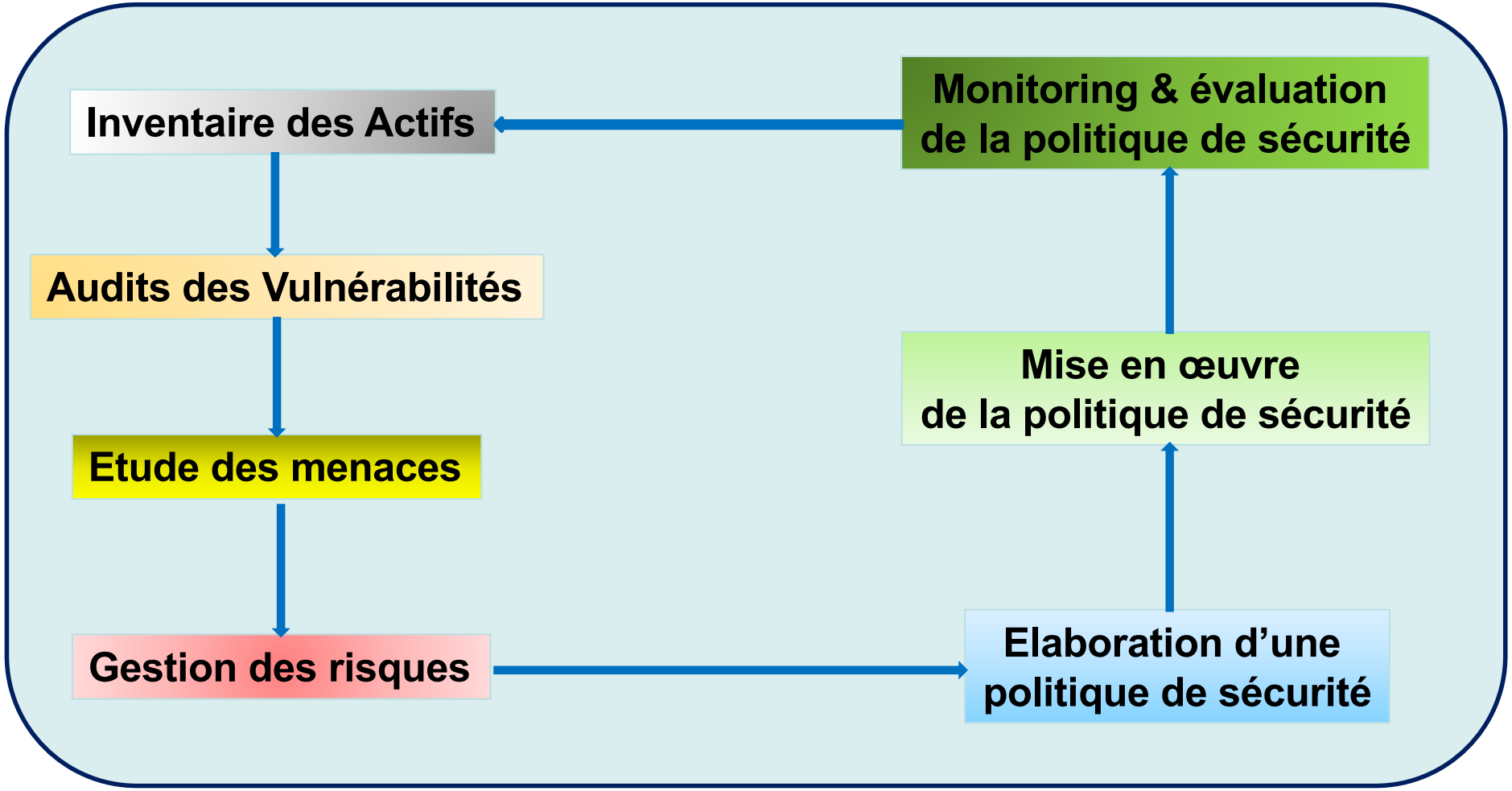


Conséquences des menaces → Risques

- Panne/Arrêt
- Diminution de la qualité de service
- Perturbation interne de l'entreprise
- Perte d'image
- Retard de la mise sur le marché d'un produit
- Fuite de technologie
- Pertes financières
- Sanctions pénales
- ...

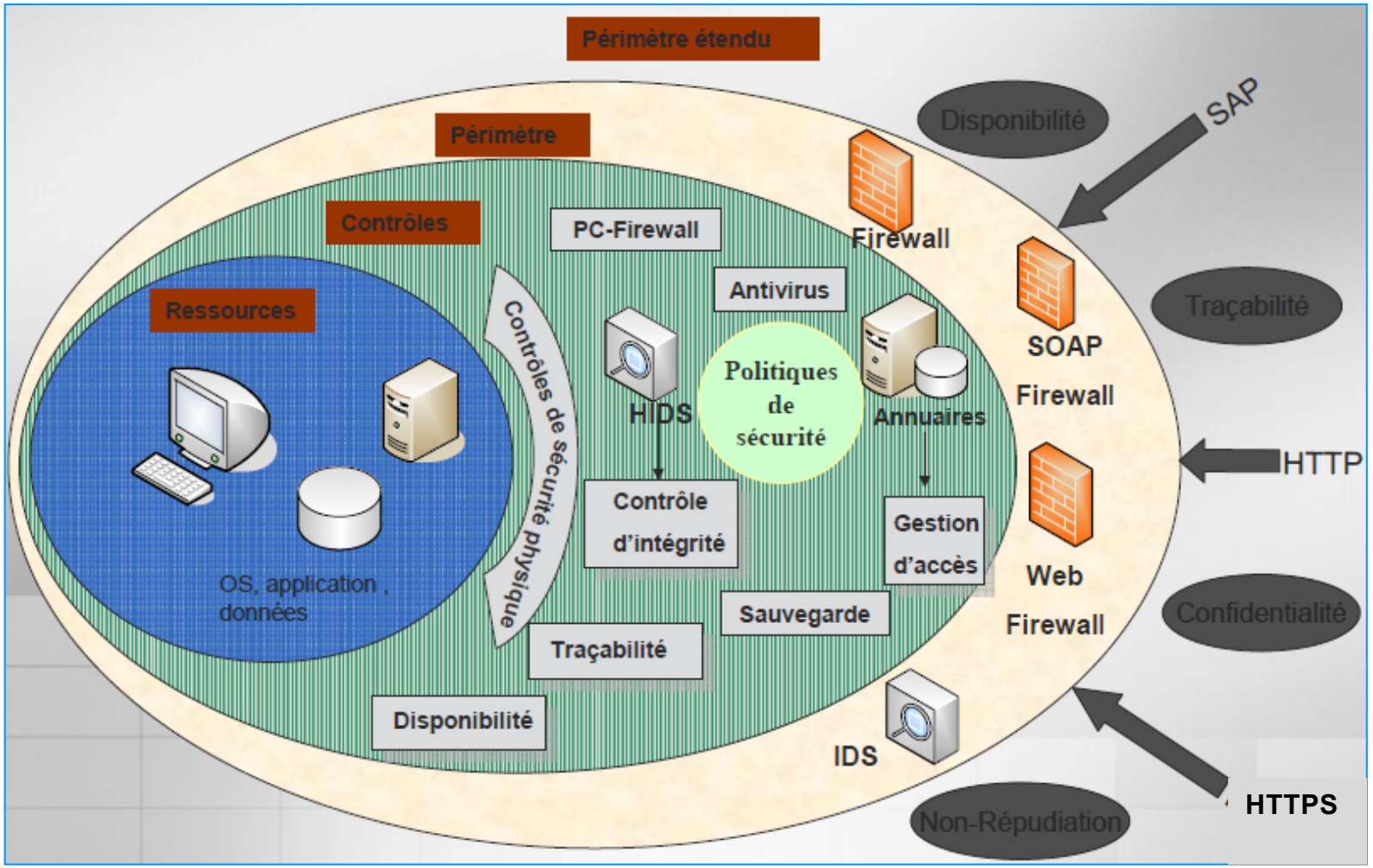
En route vers la cyber-resilience

Cycle stratégique pour la cyber-résilience



Audit régulier d'inventaire des actifs

➢ Identification des actifs et des ressources :



Audit régulier d'inventaire des actifs

- Réaliser un inventaire complet de tous les actifs, données et systèmes informatiques, applications, projets, savoir faire, etc.
- Classer par ordre de priorité les actifs qui ont le plus besoin d'être protégés.
- Utilisez un outil de gestion de l'inventaire des actifs informatiques
- Un outil de gestion des actifs informatiques est utilisé pour assurer le suivi de tous les actifs matériels et logiciels qui se trouvent dans votre environnement informatique.
- Il aide également à réduire les coûts de maintenance informatique.
- En gérant tous les actifs informatiques qui se connectent à votre réseau, vous pouvez contribuer à soutenir vos actifs pendant toute leur durée de vie et à renforcer votre sécurité informatique globale.
- **Outils ➔ NinjaOne, Timly, WhatsUp, ManageEngine AssetExplorer, Planon asset & maintenance management, SolarWinds Network Performance Monitor, etc.**

Audits des Vulnérabilités

Vulnerability Assessment (VA)

- **Audit des Vulnérabilités i.e. Vulnerability Assessment (VA) :**
  - Activité d'audit où l'auditeur va scanner le système cible (serveur, application, équipement réseau, etc.) à la recherche de vulnérabilités. Et par la suite quantifier et donner des priorités pour chaque vulnérabilité découverte.
  - VA peut être caractérisée par :
    - Les tests de VA peuvent être réalisés depuis l'intérieur ou l'extérieur du réseau.
    - Pas d'exploitation de vulnérabilités.
    - Pas d'attaques dangereuses tels que DOS ou BUFFER OVER FLOW qui peuvent perturber le système cible.
    - **Utilisation des outils de scan automatiques tels que Snort, Suricata, Nessus, OpenVas, Qualys, Acunetix, Retina, GFI Languard, etc.**

Etude des menaces

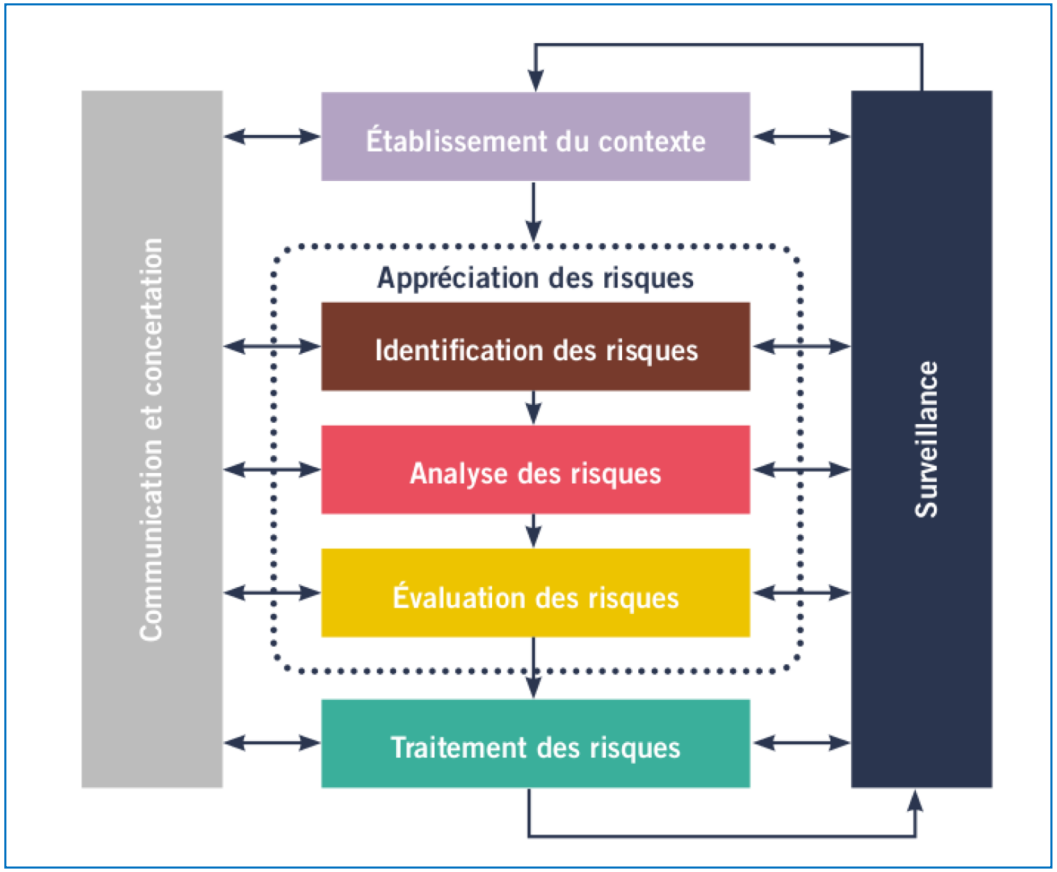
Etude des menaces

- L’ Institut national des normes et de la technologie (NIST) définit l'analyse de la menace comme « *le processus d'évaluation formelle du décret de menace pour un système d'information ou une entreprise et décrivant la nature de la menace* ».
- Identifier les faiblesses de sécurité actuelles, issues des vulnérabilités (par exemple, les informations d'identification compromises).
- Passer en revue les contrôles de sécurité actuels, comme la segmentation des réseaux ou l'exigence d'une authentification multi facteur.
- Déterminer si la menace présente un risque pour le SI ou une partie du SI.
- **Définir un système de notation qui permet de communiquer l'importance accordée à une menace :**
  - **Gravité**
  - **Analyse**
  - **Impact potentiel.**

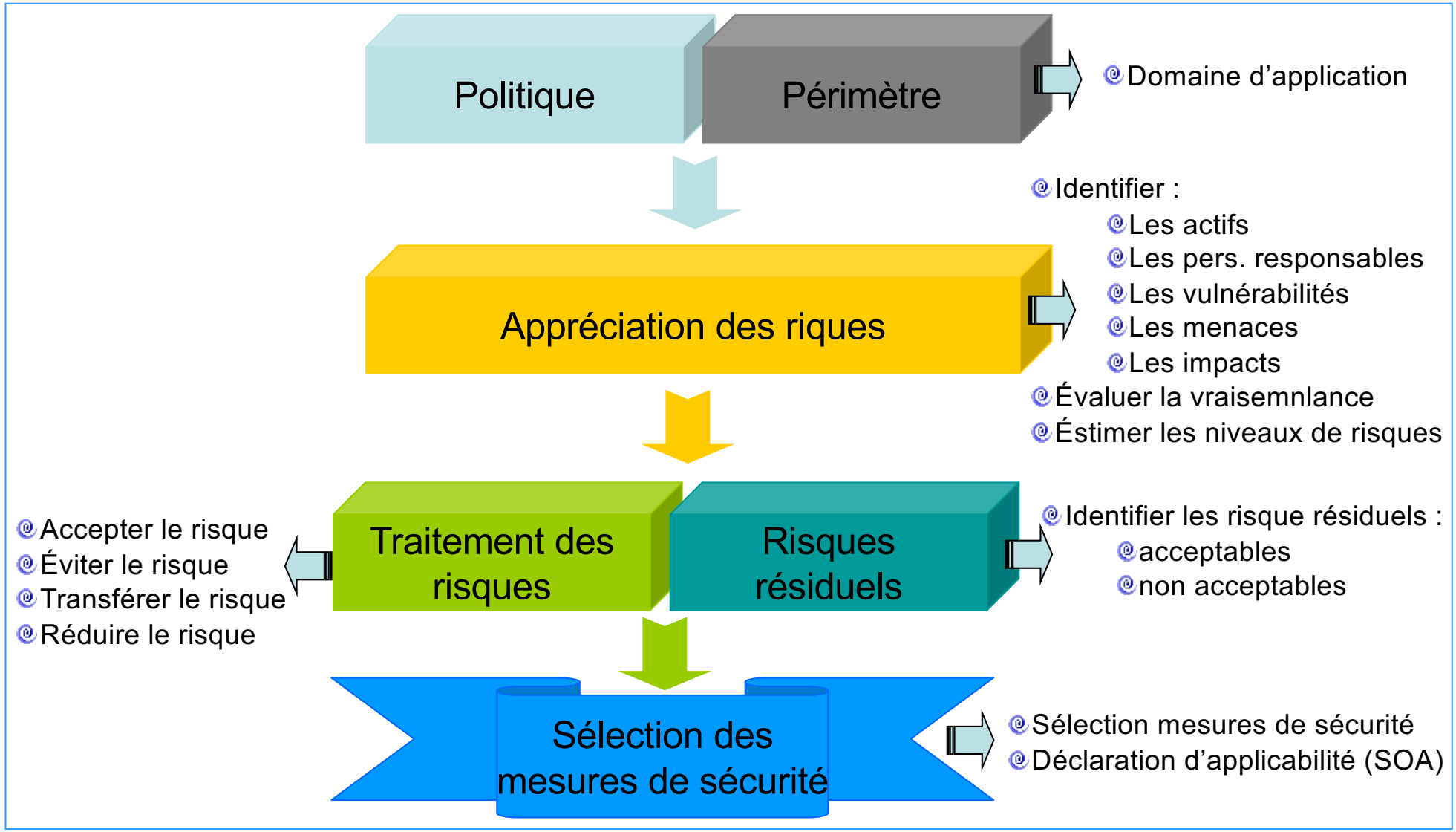
Identification & Gestion des Risques

Gestion des risques

- La gestion des risques consiste à classer les risques en fonction de leur probabilité d'occurrence et de la gravité de leur impact potentiel ainsi qu'à les traiter en cherchant à les limiter.



Gestion des risques avec ISO 27001



Politique de Sécurité

Politique de sécurité

- La mise en œuvre des **moyens de protection** exige la définition préalable d'une **politique de sécurité** élaborée au niveau de la direction générale et qui concerne tous les acteurs de l'entreprise.
- Il est nécessaire de définir dans un premier temps une **politique de sécurité**, dont la mise en œuvre se fait selon les quatre étapes suivantes :
  - **Identifier les besoins** en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences ;
  - **Elaborer des règles** et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés ;
  - **Surveiller et détecter** les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;
  - **Définir les actions** à entreprendre et les personnes à contacter en cas de détection d'une menace ;
- La **politique de sécurité** est donc l'ensemble des orientations suivies par une organisation (à prendre au sens large) en terme de sécurité ➔➔➔➔

Mettre en œuvre des mesures et des contrôles de sécurité solides

- Mettre en place des mesures de sécurité telles que l'authentification multifactorielle, la protection des points d'extrémité, les pare-feu, le chiffrement et les systèmes de sauvegarde des données.
- Protection antivirus, anti spam, détection des rootkits & des backdoors.
- IDS/IPS, Analyse & Corrélation des événements.
- Effectuer régulièrement des tests de vulnérabilités et des audits de sécurité avec des tests de pénétration.
- Former les employés aux meilleures pratiques en matière de cybersécurité et les sensibiliser à ce sujet.

Élaborer des plans d'intervention en cas d'incident

- Élaborer des procédures sur la manière de réagir en cas de cyberattaque ou de violation.
- Mettre en place des processus de confinement, d'éradication et de récupération en cas d'incident.
- Disposer de sites de backup et de reprise.
- Désigner les rôles et les responsabilités.
- Préparer des plans de communication pour informer les clients, les partenaires et les autorités de réglementation.

Définir les plans BCP/BRP et les tester régulièrement

- La planification de la reprise des activités ou BRP concerne la restauration des fonctions après un incident.
- Bien que le BRP soit similaire au BCP, le BRP manque généralement de procédures pour garantir la continuité des fonctions critiques tout au long d'une urgence ou d'une perturbation.
- Effectuer des simulations, des exercices sur table et des entraînements pour tester les plans d'intervention en cas d'incident et l'état de préparation des employés.
- Apporter des mises à jour et des améliorations si nécessaire.
- Des tests réguliers permettent de s'assurer que les plans restent efficaces et que les équipes restent préparées.

Intégrer la cyber-résilience dans la culture de l'organisation

- Intégrer la cyber-résilience dans la stratégie, les politiques, les procédures et les activités quotidiennes.
- Favoriser une culture de sensibilisation à la sécurité dans l'ensemble de l'organisation.
- Les hauts responsables doivent démontrer leur engagement en faveur de la cybersécurité et de la résilience.

Évaluation de la politique de sécurité

- Moyen de contrôle dont le but est de s'assurer en permanence :
  - L'efficacité de la politique de sécurité
  - La conformité de son implémentation par rapport aux spécifications
- 3 outils permettent de répondre à cette exigence :
  - **Les audits internes**
  - Le contrôle interne
  - Les revues
    - Résultats des audits internes
    - Retour des parties prenantes
    - État des lieux sur les actions en cours
      - Préventives
      - Correctives
    - Menaces mal appréhendées lors de l'appréciation des risques
    - Interprétation des indicateurs
    - Nouvelles priorités
    - Changements survenus dans l'entreprise (réorganisations, fusions, acquisitions, cessions, etc.)

Pour finir

Conclusion

- En conclusion, une stratégie de cyber-résilience à multiples facettes qui intègre les personnes, les processus et la technologie est essentielle pour atténuer les risques et minimiser les perturbations causées par les cyber-menaces.
- Avec une planification, une formation, des tests et des ressources appropriés, les organisations peuvent développer la résilience nécessaire pour résister aux cyberattaques et rebondir rapidement.

Merci de votre attention !



cherif.diallo@ugb.edu.sn