15ème FORUM DES COURTIERS 2025

LABEL CYBER SAFE

Cyberattaques, la nouvelle criminalité du XXIe siècle

Etat de la menace

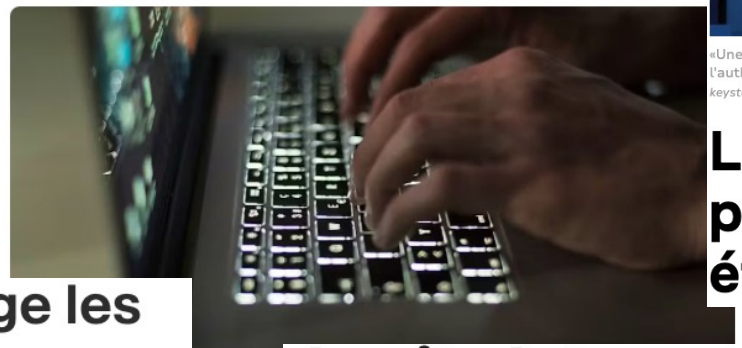
Les filiales Spar et les magasins TopCC ont été victimes d'une cyberattaque

L'entreprise annonce s'efforcer de rétablir le plus rapidement possible son activité, après une attaque survenue dans la nuit de jeudi à vendredi. Une plainte a été déposée

Cyberattaque

Radiologie: le Groupe 3R victime d'une cyberattaque

Le Groupe 3R (Réseau Radiologique Romand) a été victime d'une cyberattaque lors de laquelle des données de patients ont été dérobées. I appelle les patients de ses centres d'imagerie romands à se méfier de tou contact suspect.



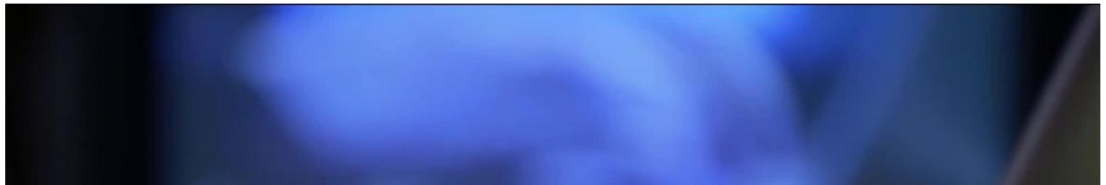
«Une soixantaine de caisses de pension pourraient être concernées, avec environ 13 000 destinataires qui utilisent l'authentification par SMS.»
keystone / dr

La caisse de pension de plusieurs milliers de Suisses a été piratée

La cyberattaque de Vidymed plonge les médecins dans le désarroi et l'épuisement

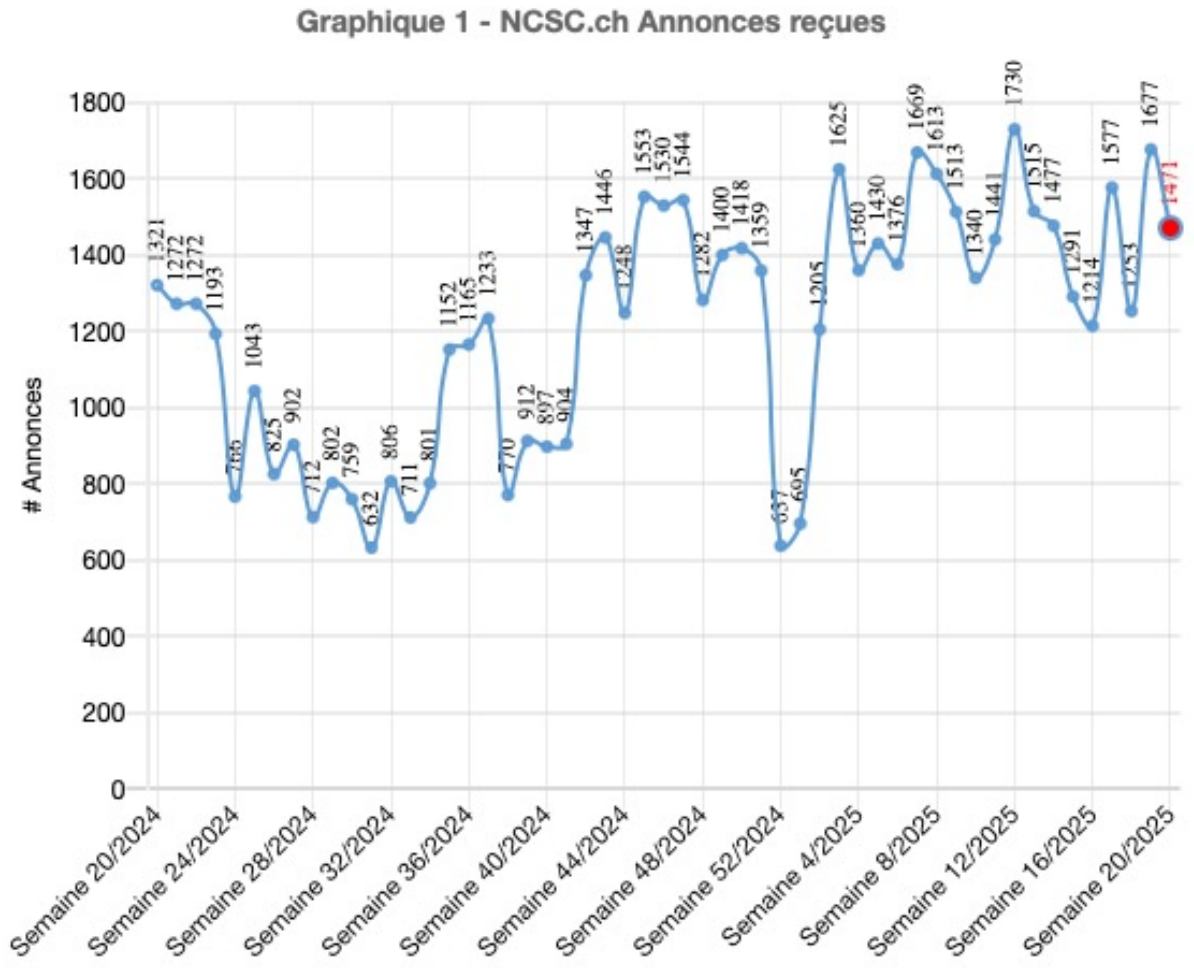
Vaud
Modifié le 10 janvier 2025 à 12:08

Partager



Le site Internet de l'Etat du Valais victime d'une cyberattaque

Etat de la menace



Source: https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/aktuelle-zahlen.html

- **En 2024, 63’000 cas annoncés (+27.5%)**
- **80% des cas: tentatives d’arnaque et hameçonnage**
- **Uniquement les cas annoncés…**

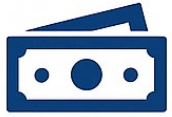
Acteurs et motivations

Script Kiddie (pour le fun ou la reconnaissance)

Personne mécontente (vengeance, menace interne)

Hacktivistes (motivations idéologiques)

Gouvernements et acteurs étatiques (espionnage, guerre)

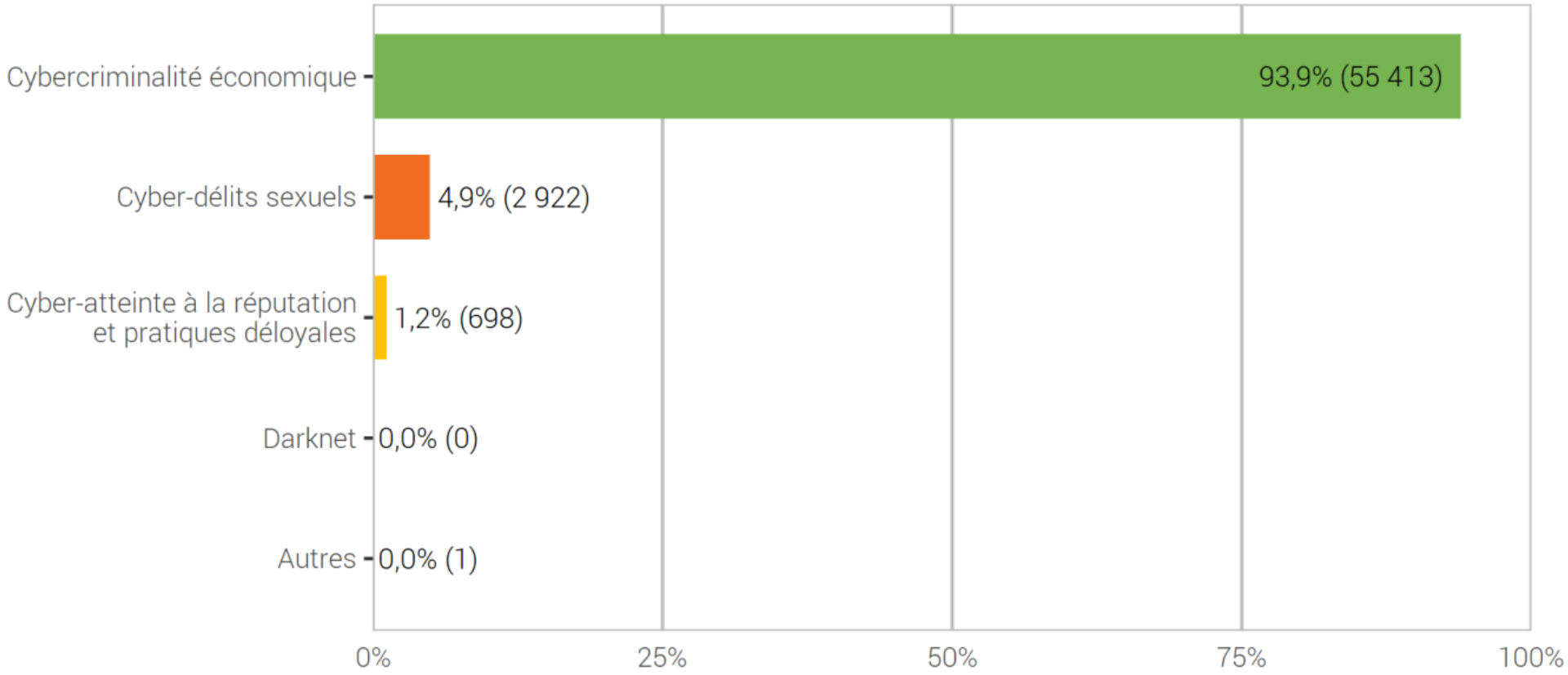


Groupes malveillants (motivations financières)

- **Des groupes organisés et structurés:**
  - **Reconnaissance**
  - **Exploitation**
  - **Négociation**
  - **Service après vente**
- **Transnationaux**

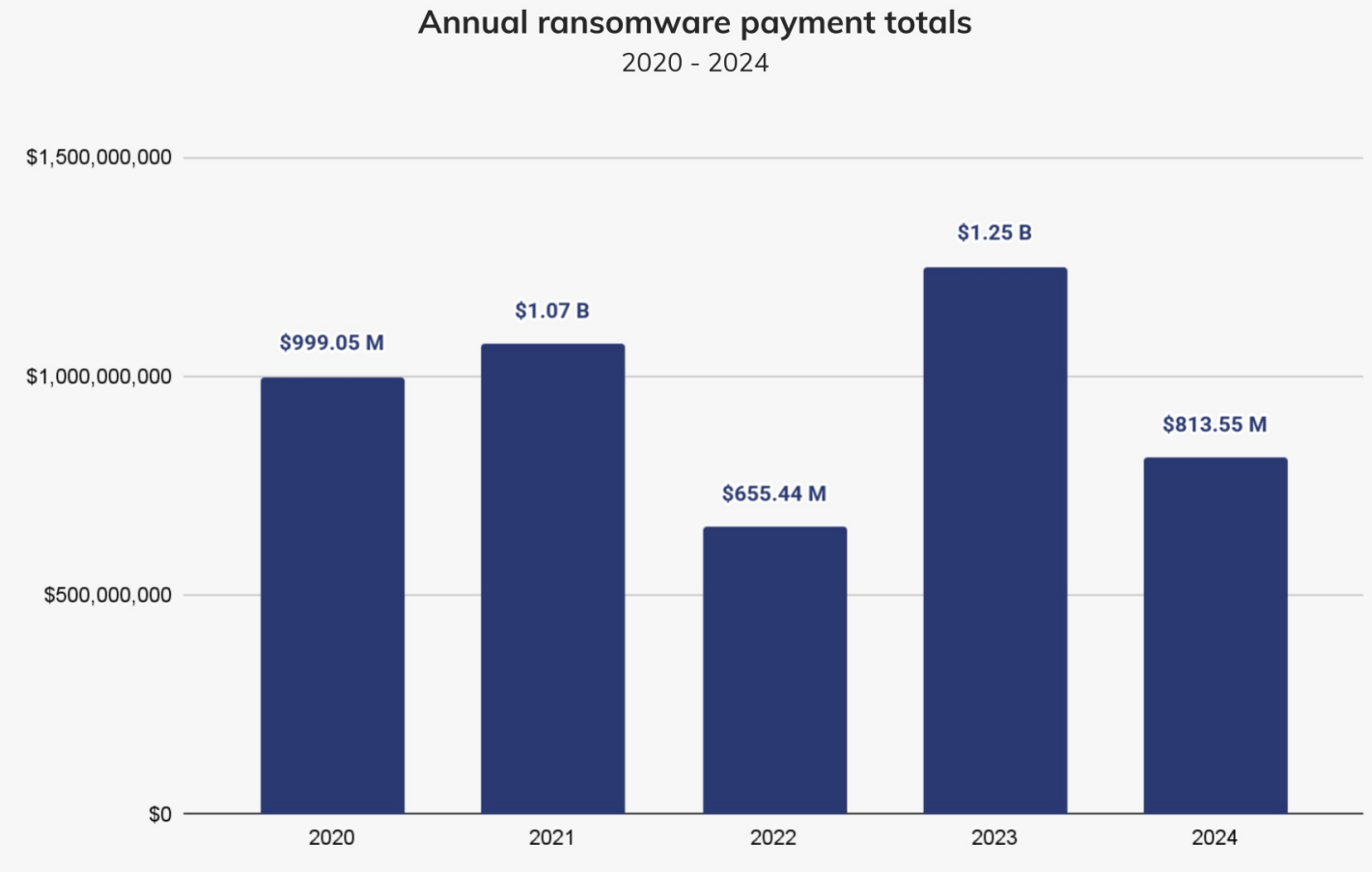
Acteurs et motivations

Infractions de criminalité numérique par domaine **G 24**



Source(s): OFS – Statistique policière de la criminalité (SPC) 2024

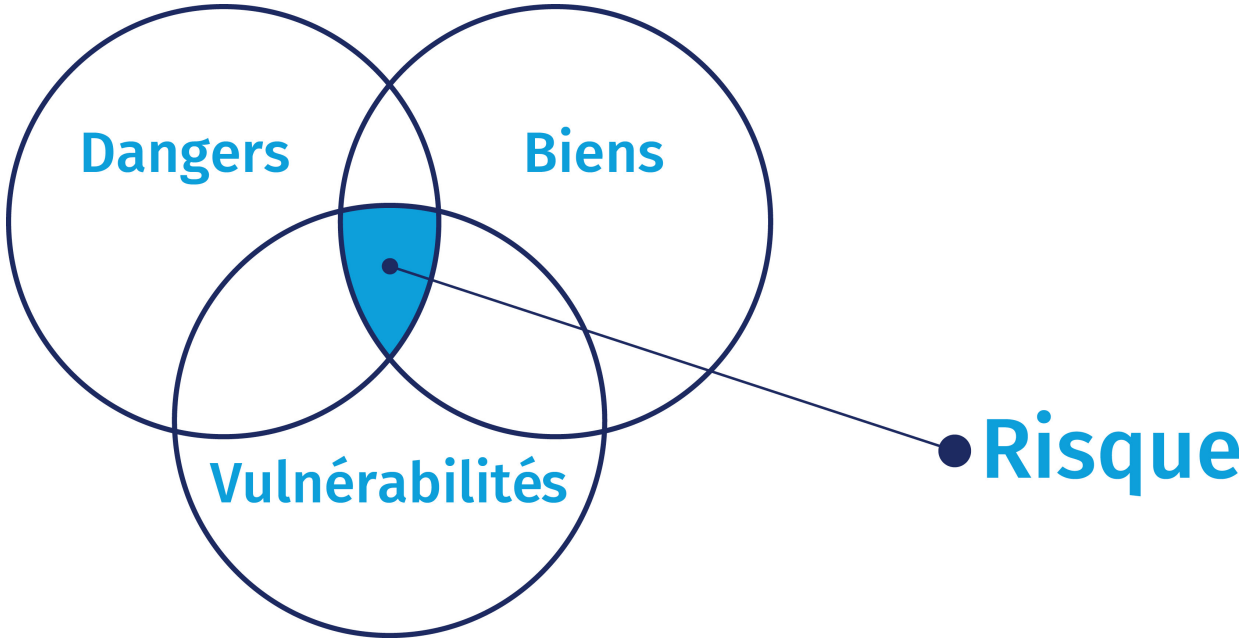
Les dangers



Source: https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf

- **Paiement final typique entre 150k – 250k $**
- Concerne uniquement **le montant de la rançon…**

La notion de risque cyber



Avant de choisir comment vous protéger ou vous assurer:

Quels sont les impacts en cas d'incident ?

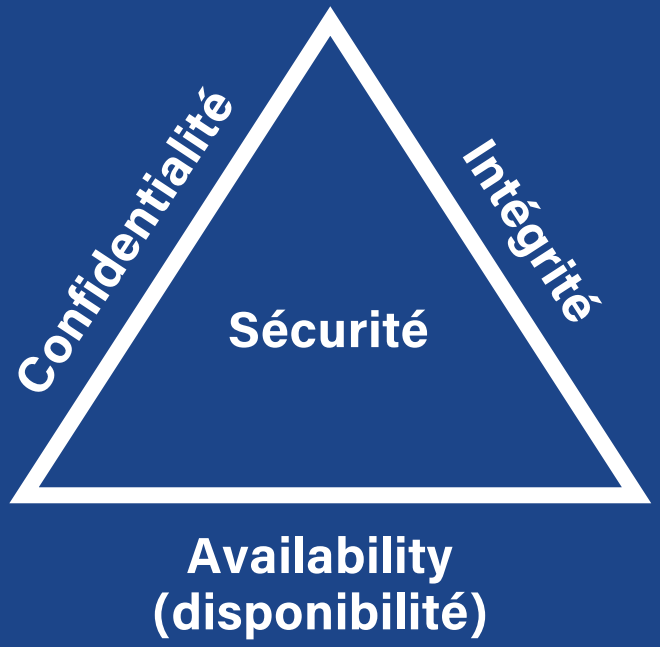
Type de données:

- **Données administratives**
- **Données financières**
- **Données de tiers**
- **…**

Valeur des données

- Point de vue de l'attaquant:
  - Combien valent-elles sur le darkweb?
  - Quelle rançon pourriez-vous supporter?

- Point de vue de la victime:
  - **Combien valent-elles POUR MON ORGANISATION**, quels sont les impacts en cas de cyber-incident?
  - Question complexe...



Valeur des données & CIA

Confidentialité: combien perdrez-vous si ces données sont divulguées au grand public ?
Ex: impact en % de votre chiffre d'affaires

Intégrité: Combien perdrez-vous si ces données sont modifiées ?
Ex: montant des factures ouvertes

Disponibilité: Combien perdrez-vous si ces données ne sont plus accessibles?
Ex: (nombre d'employés à l'arrêt) x (nombre d'heures) x (salaire horaire)

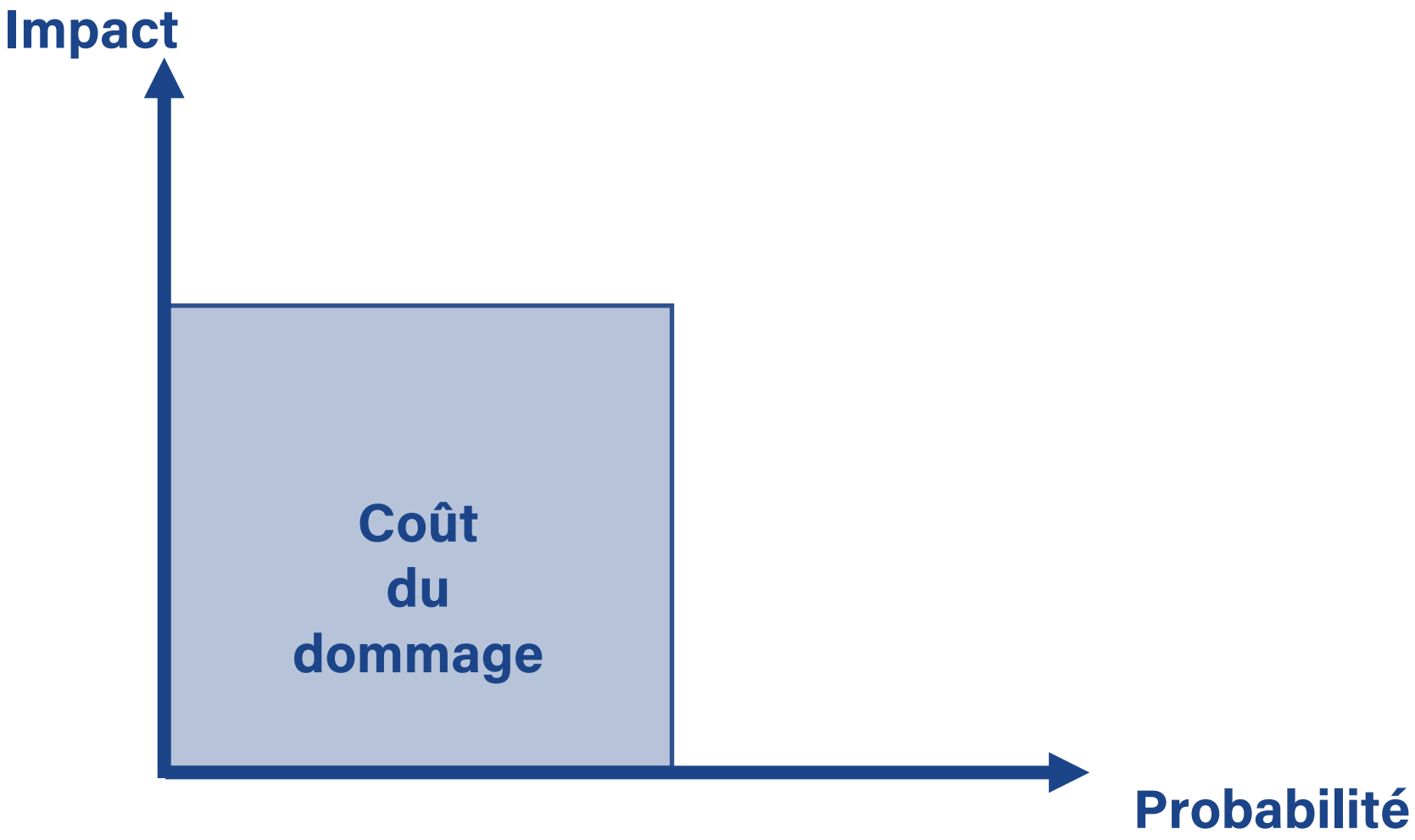
À suivre...

Quels impacts

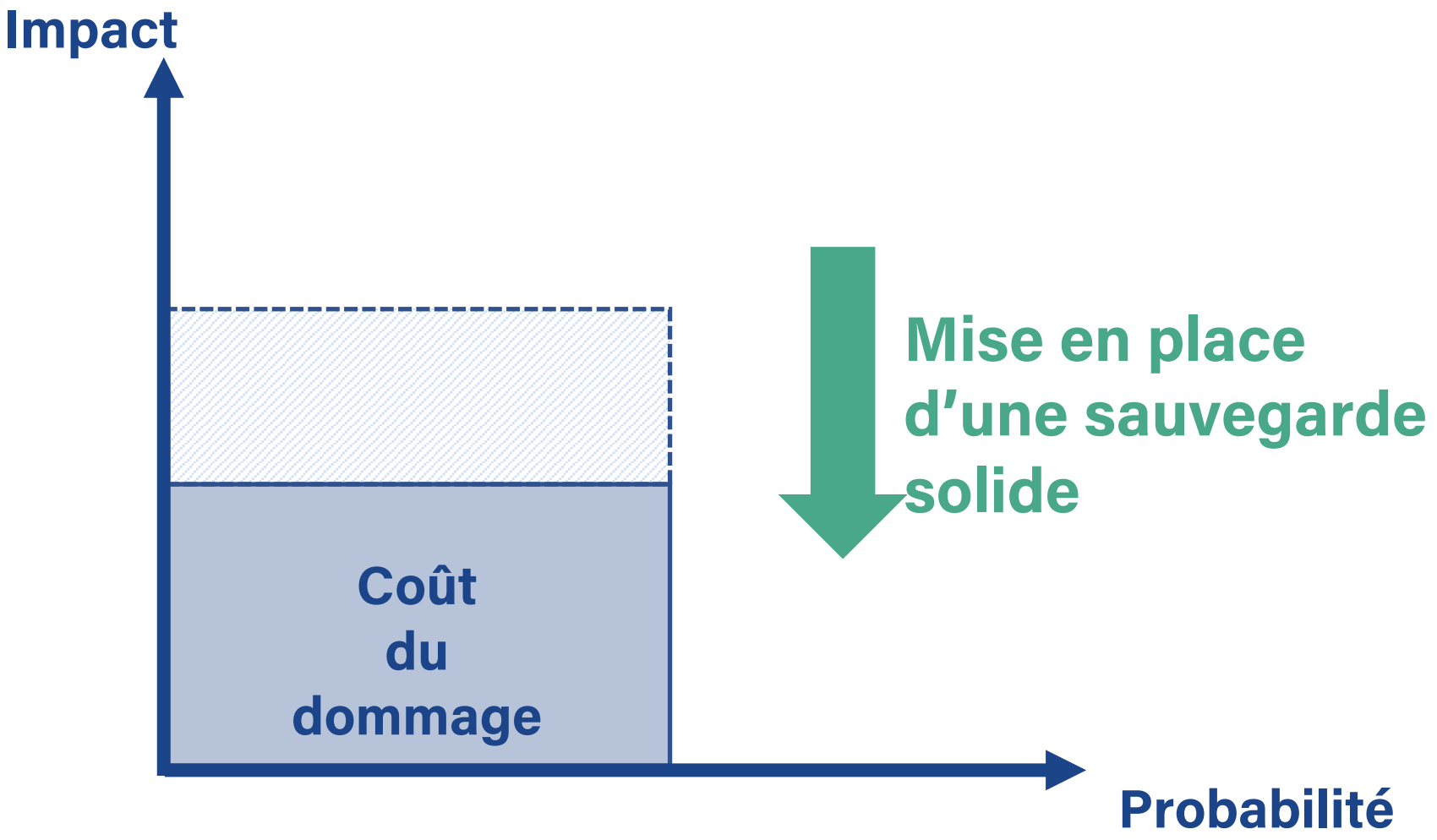
- Impacts CIA
- Consultants externes (réponse à incident, communication, etc.)
- Correction faille(s) technique(s)
- Frais de récupération, restauration des données et systèmes (mode dégradé)
- Améliorations et enseignements
- Suivi administratif et légal (poursuites, assurances, etc.)
- Quid du coût humain?

>100k CHF ?

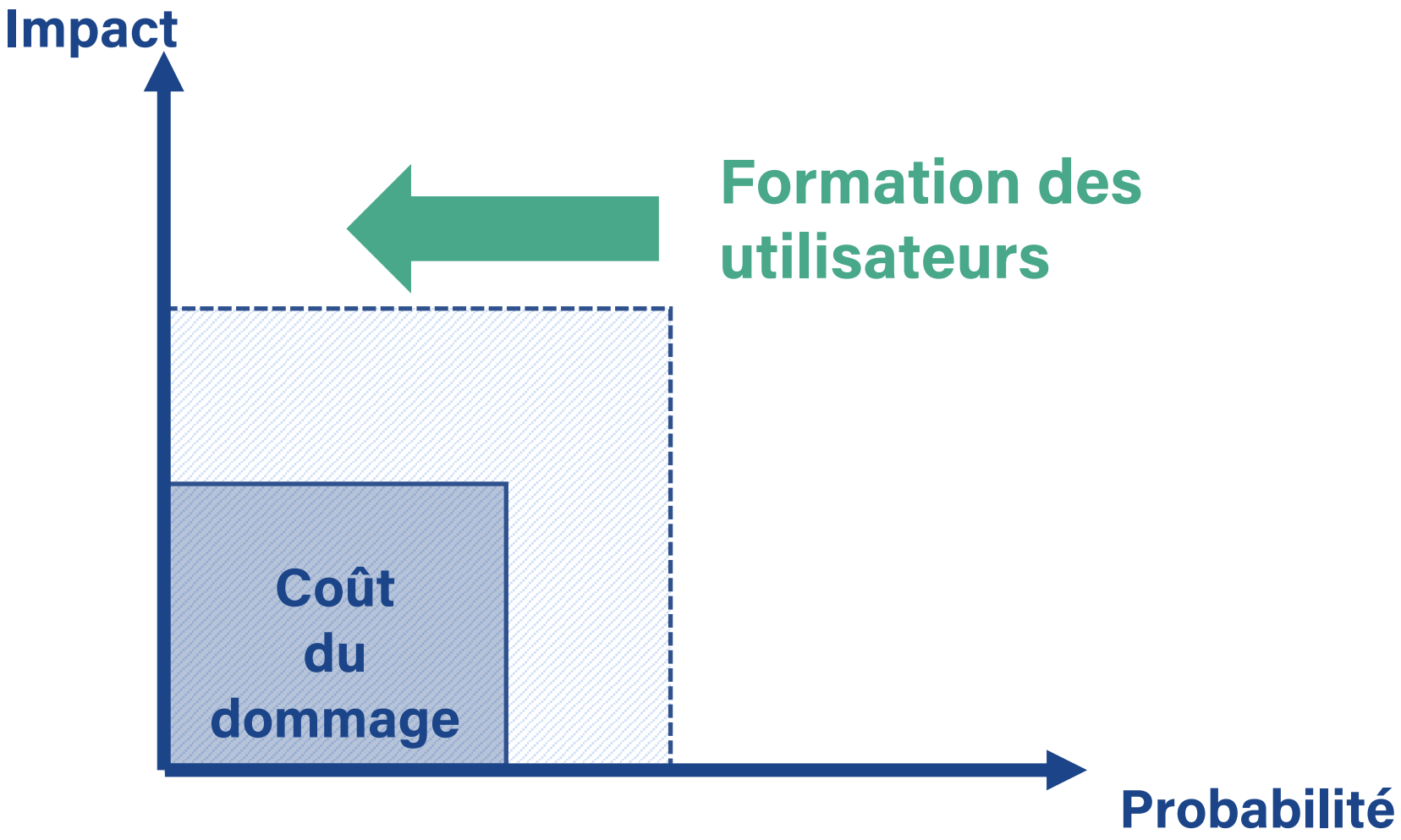
Le risque cyber: résumé



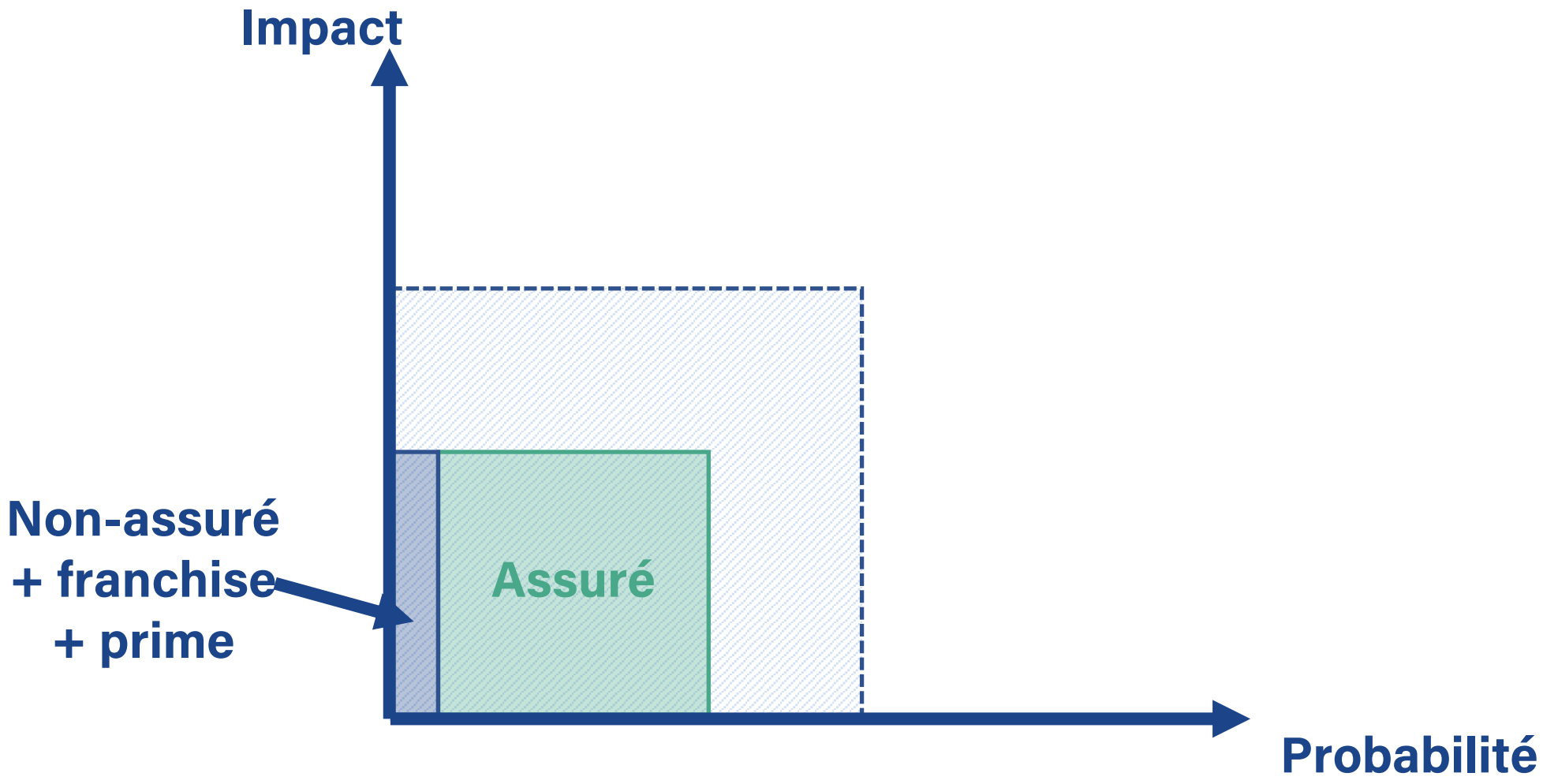
Le risque cyber: résumé



Le risque cyber: résumé



Le risque résiduel



Quels aspects pour faire face aux risques cyber?

Humains

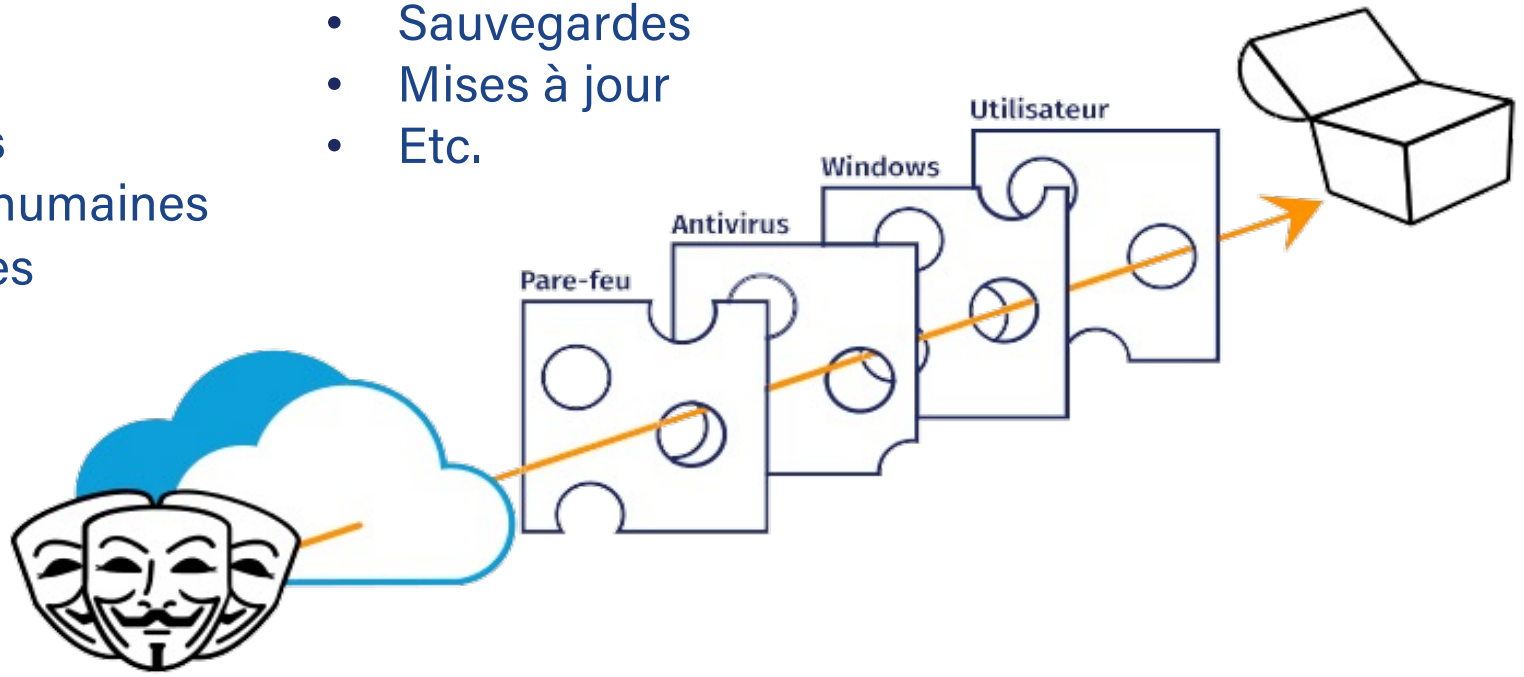
- Responsabilités
- Sensibilisation au phishing
- Compétences techniques du responsable
- Etc.

Organisationnels

- Ressources humaines
- Droits d'accès
- Procédures
- Etc.

Infrastructure informatique

- Inventaire
- Antivirus sur TOUS les PC de l'inventaire
- Pare-feu fonctionnel
- Chiffrement
- Sauvegardes
- Mises à jour
- Etc.



La technique

Quelques points :

- **Sauvegardes immuables et tests de récupération**
- Inventaire et mise à jour des programmes et du matériel
- Pare-feu, anti-virus et gestion des alertes
- Authentification forte
- Etc.

Le risque cyber est un un risque opérationnel !

LABEL CYBER SAFE

L'organisation

Chappatte, Le Temps, 28.01.2022

Le risque cyber: une affaire de direction

- Responsabilité (qui peut couper internet?)
- Le(s) prestataire(s): qui fait quoi?
- Droits d'accès: qui a accès à quoi?
- **Se préparer** à l'inévitable: gestion de crise, plan de continuité et de reprise, etc.

L’humain

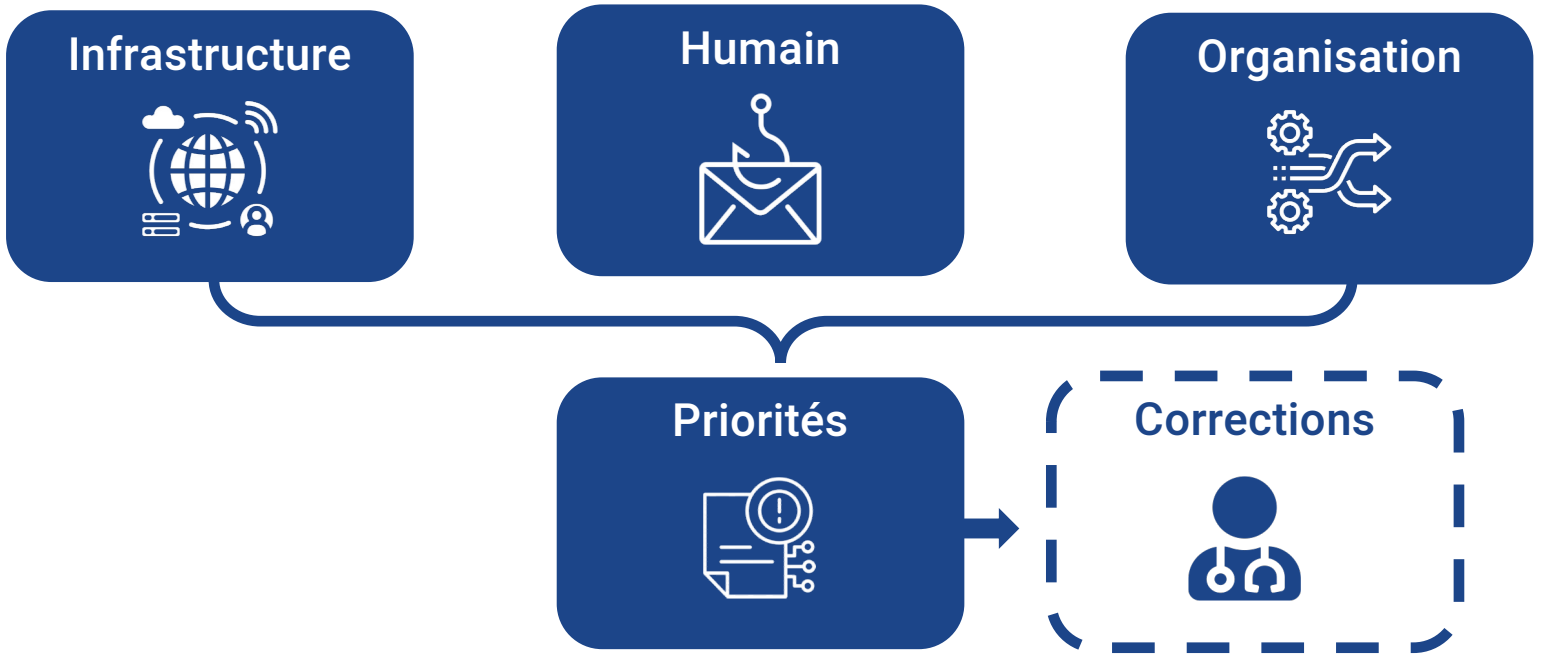
Première ligne de protection face au risque cyber:

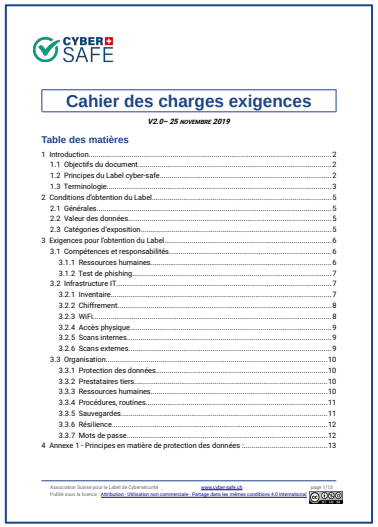
- Partage d’informations, annonce de cas
- **Sensibilisation** à l’hameçonnage
- Chartes utilisateurs:
  - Droits et devoirs
  - **Décomplexer** la parole!

1. Évaluez le contenu (Urgence? Autorité?)
2. Identifiez l’émetteur
3. Identifiez les liens suspects
4. Demandez de l’aide et informez

Association Label Cyber-Safe

Diagnostic:





CYBER SAFE

Cahier des charges exigences

V2.0– 25 novembre 2019

Table des matières

Vérification:

15ème FORUM DES COURTIERS 2025

LABEL CYBER SAFE

Merci pour votre attention

demo.cyber-safe.ch/

chauert@cyber-safe.ch