CYBER SAFE

Cybersécurité : prévention – actions concrètes

Soirée d'information de l'UCV
18 novembre 2021

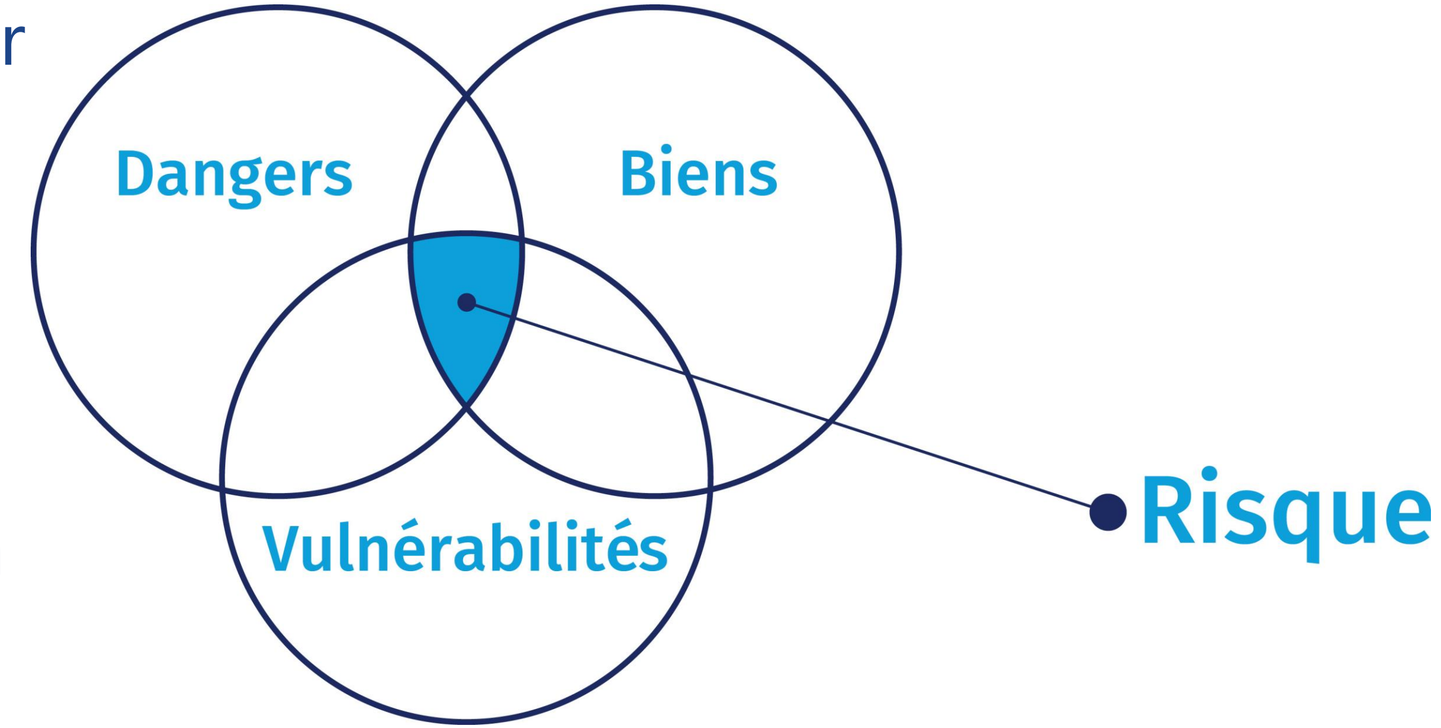
CYBER SAFE

La notion de risque cyber

Notion de risque

Il faut trois éléments pour constituer un risque :

- Des dangers
- Une valeur (biens)
- L’absence de protection (vulnérabilité)

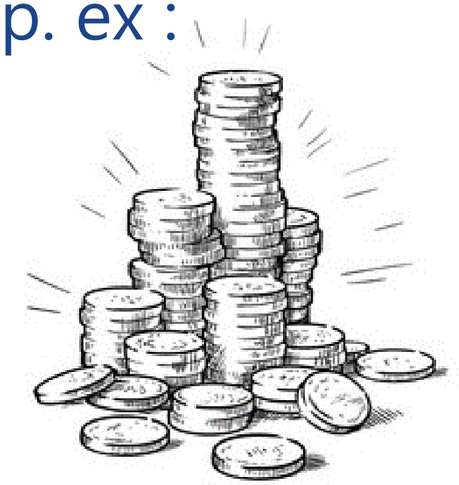


La valeur de vos données

- Avant de choisir comment vous protéger ou vous assurer, une question

Quels sont les impacts en cas d'incident ?

- Question complexe
- Pour la résoudre il faut décomposer par type de donnée, p. ex :
  - Données administratives
  - Données financières
  - Données de tiers
  - ….



Valeurs CIA

- Pour chaque type de données, il faut considérer chaque axe :
  - **Confidentialité**
    Combien perdrez-vous si ces données sont divulguées au grand public ?
    P. ex. vos données de R&D
  - **Intégrité**
    Combien perdrez-vous si ces données sont modifiées ?
    P. ex. comptes de paiement
  - **Accessibilité** (disponibilité)
    Combien perdrez-vous si ces données ne sont plus accessibles, temporairement ou définitivement ?
    P. ex. combien d'employés ne peuvent travailler pendant une panne de 3 jours ?

Quelques cas concrets

- Rolle
- Comparis => 350k+
- Lake city => 460k$, 12k pers.
- Riviera Beach => 600k$, mais 10k pour eux, 32k pers.
- Maersk : 80k employés, coût : 300M$
- TNT, poste suisse, …

Quels aspects pour une bonne protection ?

Humains

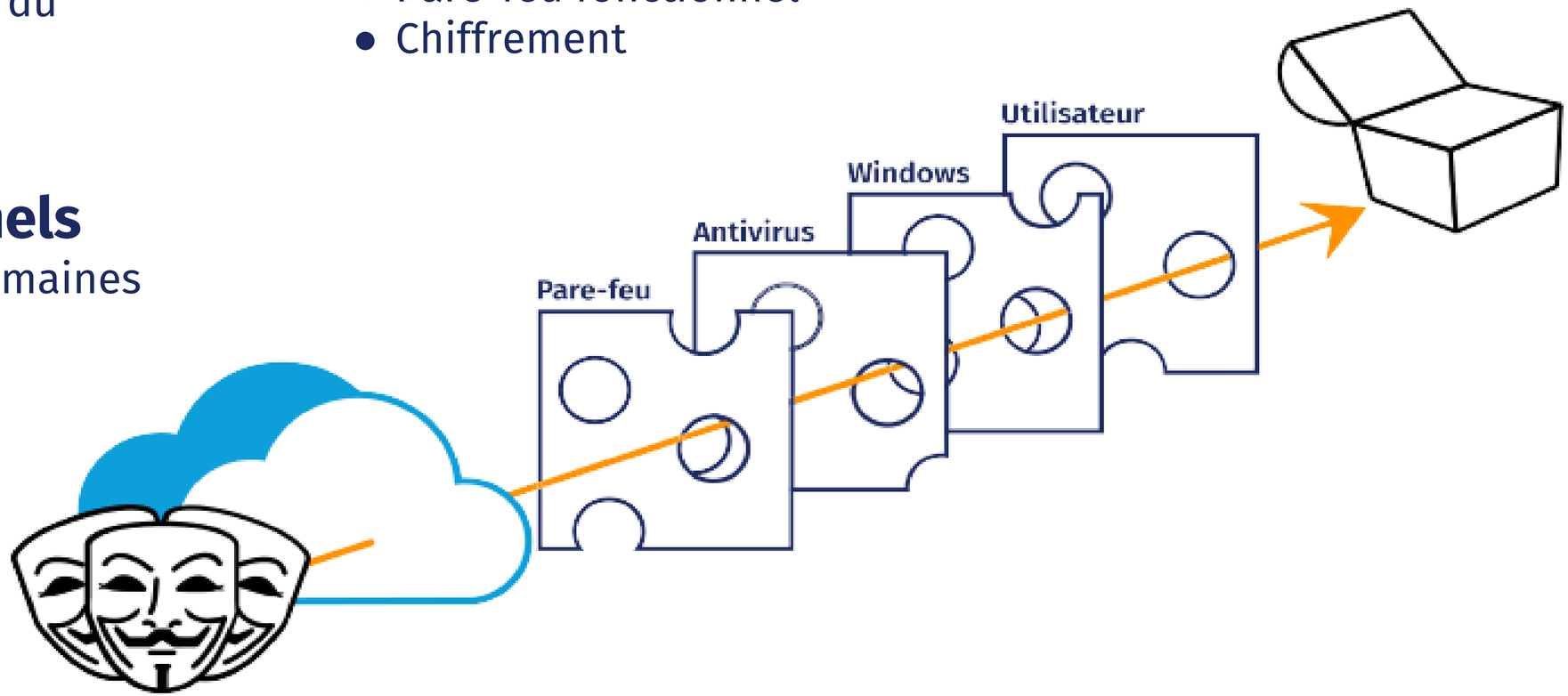
- Responsabilités
- Sensibilité au phishing
- Compétences techniques du responsable

Infrastructure informatique

- Inventaire
- Antivirus sur TOUS les PC de l’inventaire
- Pare-feu fonctionnel
- Chiffrement

Organisationnels

- Ressources humaines
- Droits d’accès
- Sauvegardes
- Procédures

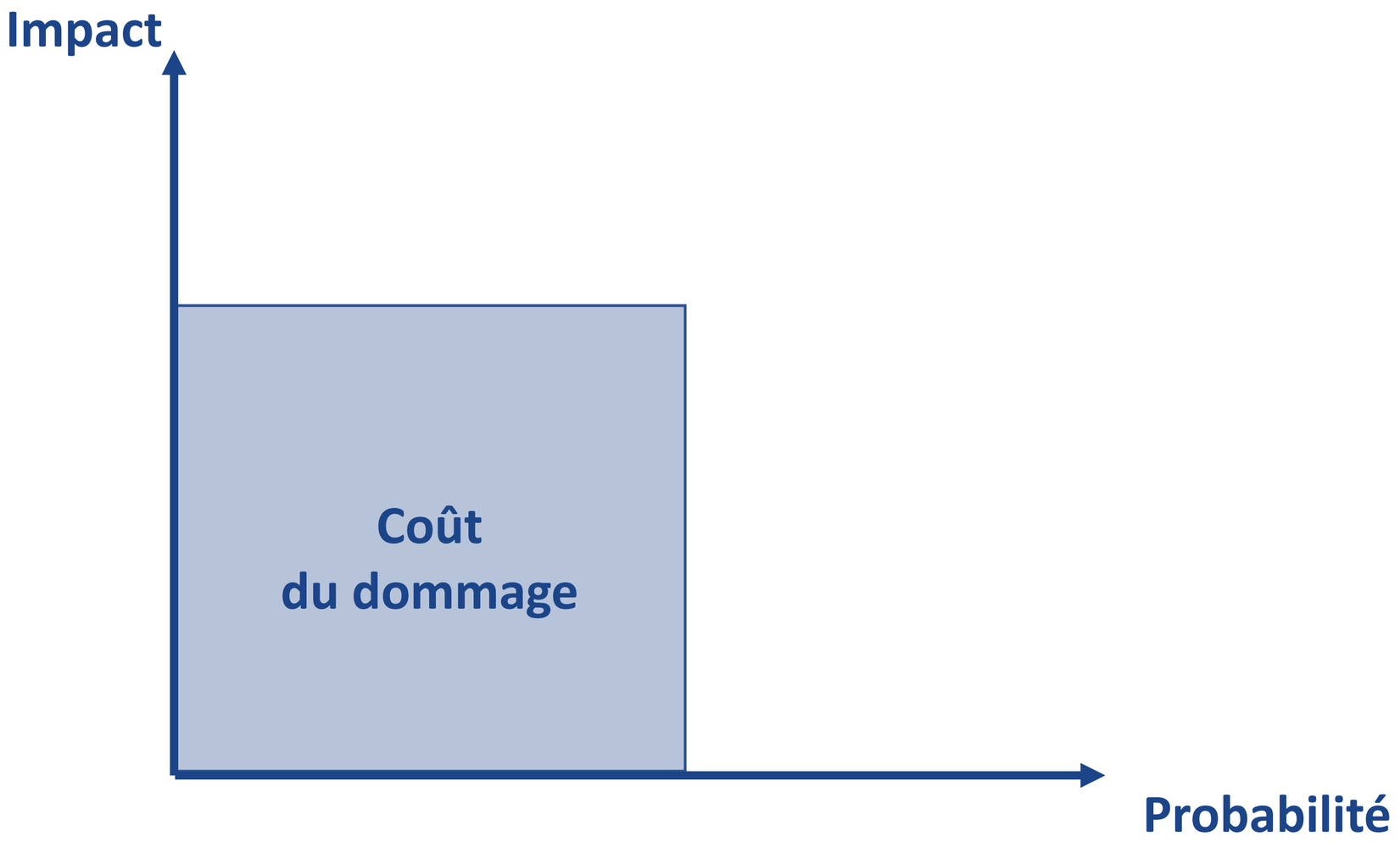


FAIL

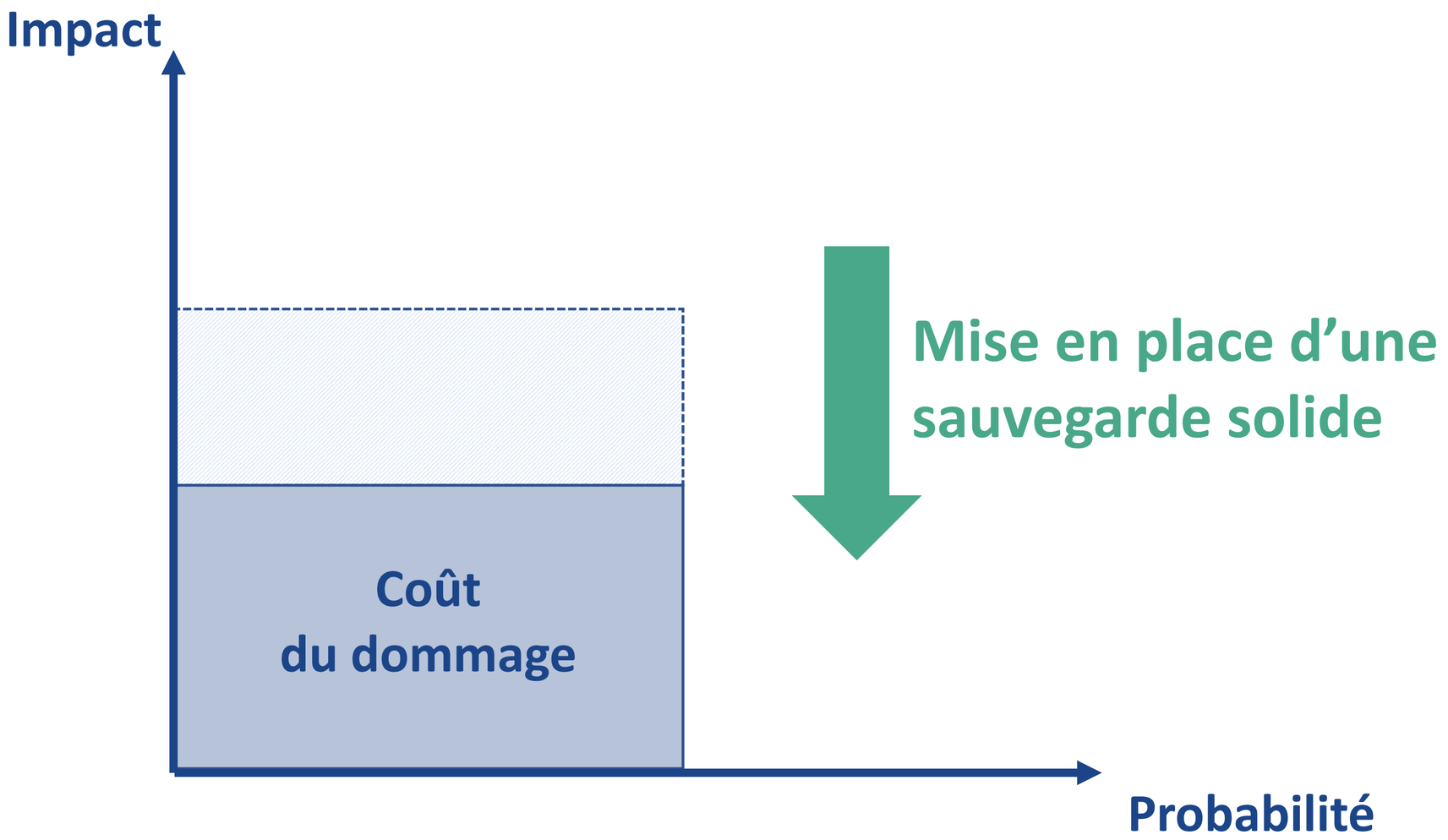
Protection

Un code
à 4 chiffres
peut-être ?

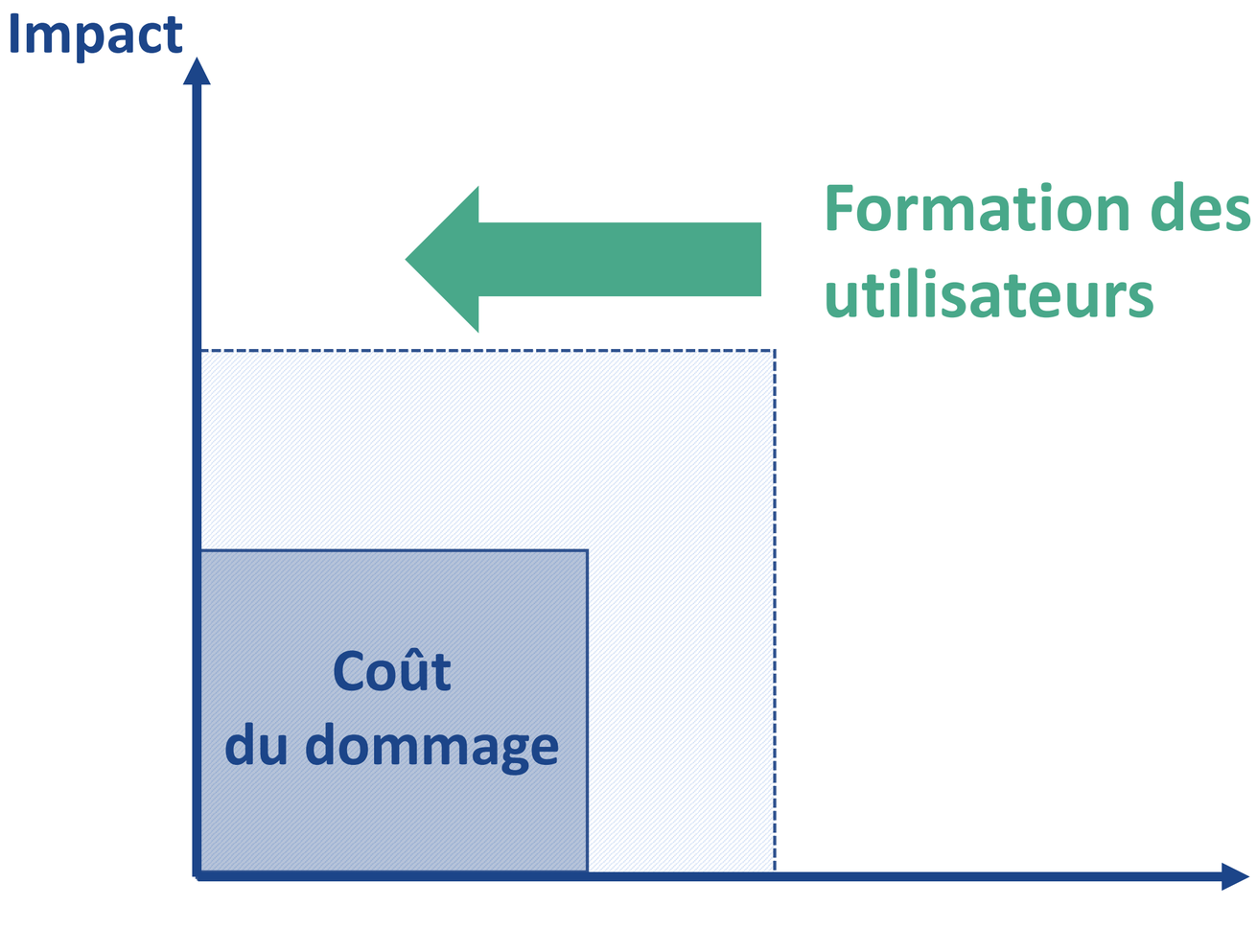
Le risque cyber : résumé



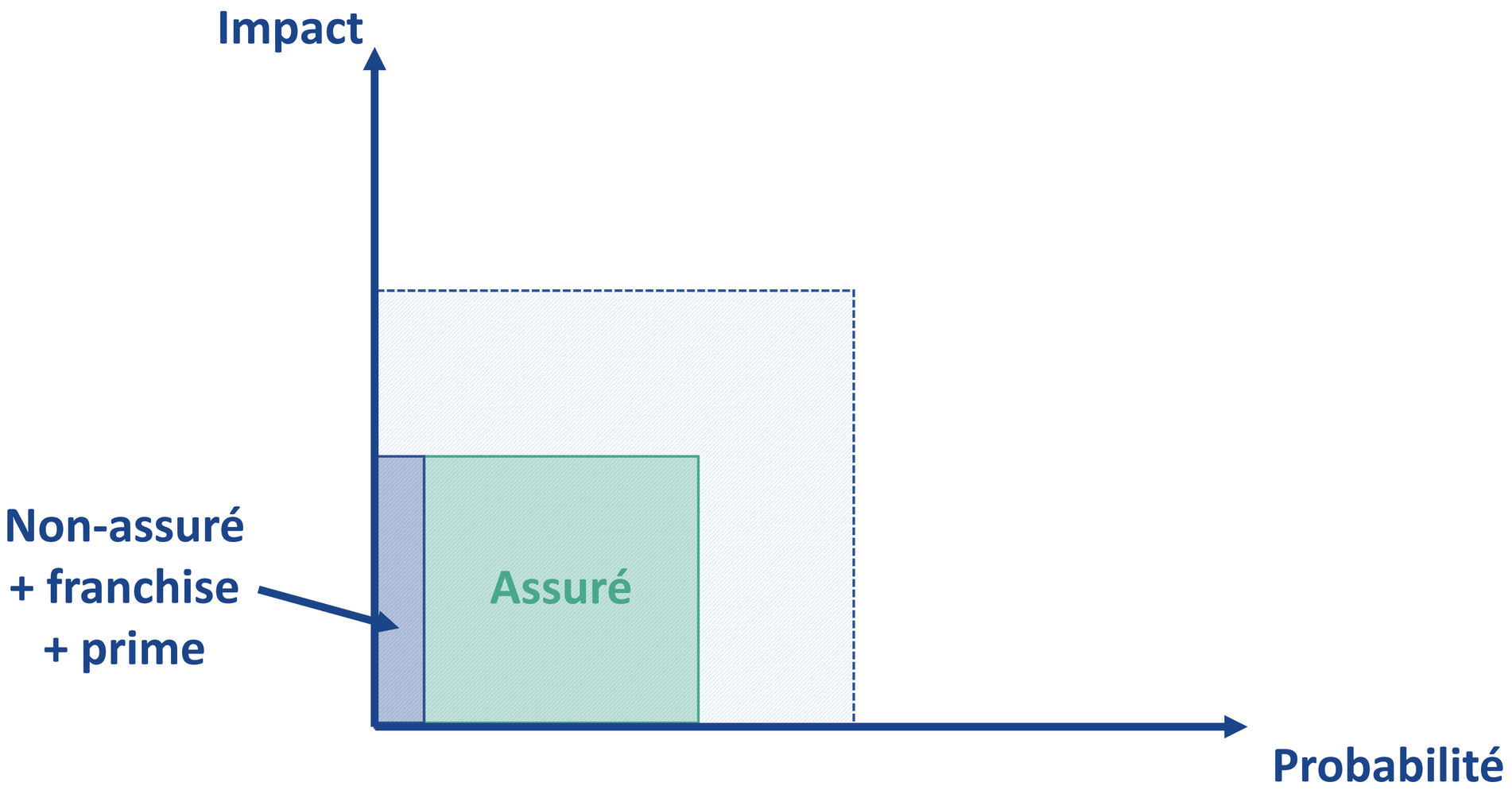
Le risque cyber : résumé



Le risque cyber : résumé



Le risque résiduel



CYBER SAFE

Démo de hacking

CYBER SAFE

Quelques bonnes pratiques

THE bonne pratique

Evaluez vos risques cyber:

- Types de données en votre possession
- Impacts en cas de perte:
  - Retards administratifs?
  - Arrêt temporaire de la production?
  - Faillite?
- Impacts en cas de divulgation:
  - Dégâts d'image, perte de CA
  - Procès, dommages et intérêts?

Gestion des périphériques mobiles

Souvent inévitables dans une commune, ils peuvent représenter un danger supplémentaire. Veillez donc à :

- Un **anti-virus** y est installé
- Effectuer le suivi des **mises à jour**
- Relever les **alertes de sécurité**
- **Identifier** les données et accès qui s'y trouvent
- **Chiffrer le disque**, si des données s'y trouvent

Sauvegardes

Votre sauvegarde n’a de la valeur que si vous pouvez la récupérer !!!

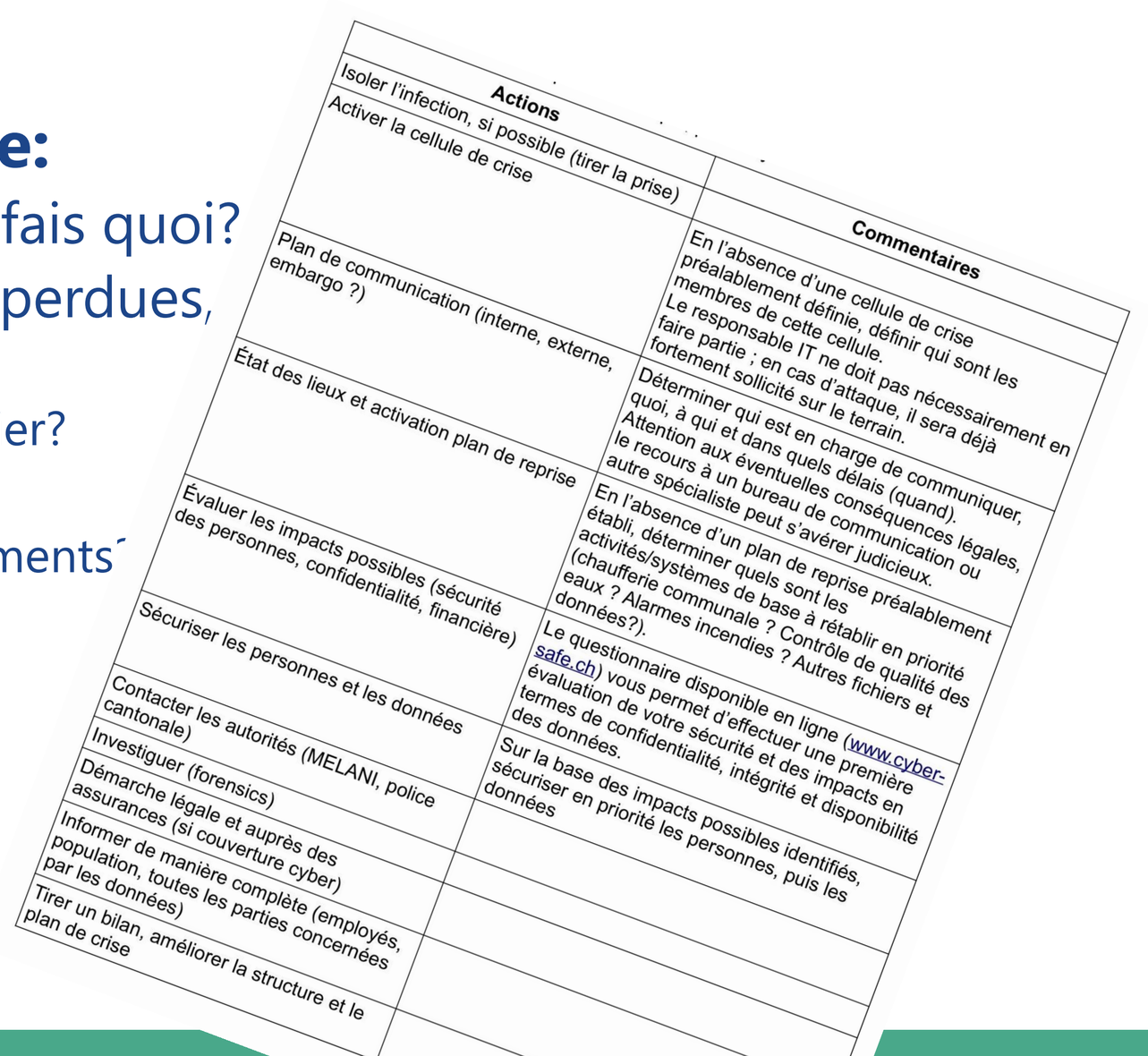
- Règle du 3 – 2 – 1 – 0
  - 3 copies
  - 2 formats
  - **1 copie hors site**
  - **0 erreurs au test de récupération**
- Non accessibles employés / administrateurs
- **Vérification régulière**

Mesures organisationnelles

- **Politique de mots de passe**
  - 10 caractères: majuscules, minuscules, chiffres et caractères spéciaux.

Mesures organisationnelles

- **Simulation et plan de reprise:**
  - Si je suis attaqué aujourd'hui, je fais quoi?
  - Et si demain, mes données sont perdues, je fais quoi?
    - Quelles données récupérer en premier?
    - Procédure d'accès à la sauvegarde?
    - Dépendance entre les différents éléments?
    - Etc.



Actions	Commentaires
Isoler l'infection, si possible (tirer la prise)	En l'absence d'une cellule de crise préalablement définie, définir qui sont les membres de cette cellule. Le responsable IT ne doit pas nécessairement en faire partie ; en cas d'attaque, il sera déjà fortement sollicité sur le terrain.
Activer la cellule de crise	
Plan de communication (interne, externe, embargo ?)	Déterminer qui est en charge de communiquer, quoi, à qui et dans quels délais (quand). Attention aux éventuelles conséquences légales, le recours à un bureau de communication ou autre spécialiste peut s'avérer judicieux.
État des lieux et activation plan de reprise	En l'absence d'un plan de reprise préalablement établi, déterminer quels sont les activités/systèmes de base à rétablir en priorité (chaufferie communale ? Contrôle de qualité des eaux ? Alarmes incendies ? Autres fichiers et données?).
Évaluer les impacts possibles (sécurité des personnes, confidentialité, financière)	Le questionnaire disponible en ligne (www.cyber-safe.ch) vous permet d'effectuer une première évaluation de votre sécurité et des impacts en termes de confidentialité, intégrité et disponibilité des données.
Sécuriser les personnes et les données	Sur la base des impacts possibles identifiés, sécuriser en priorité les personnes, puis les données
Contacter les autorités (MELANI, police cantonale)	
Investiguer (forensics)	
Démarche légale et auprès des assurances (si couverture cyber)	
Informer de manière complète (employés, population, toutes les parties concernées par les données)	
Tirer un bilan, améliorer la structure et le plan de crise	

Phishing – identification

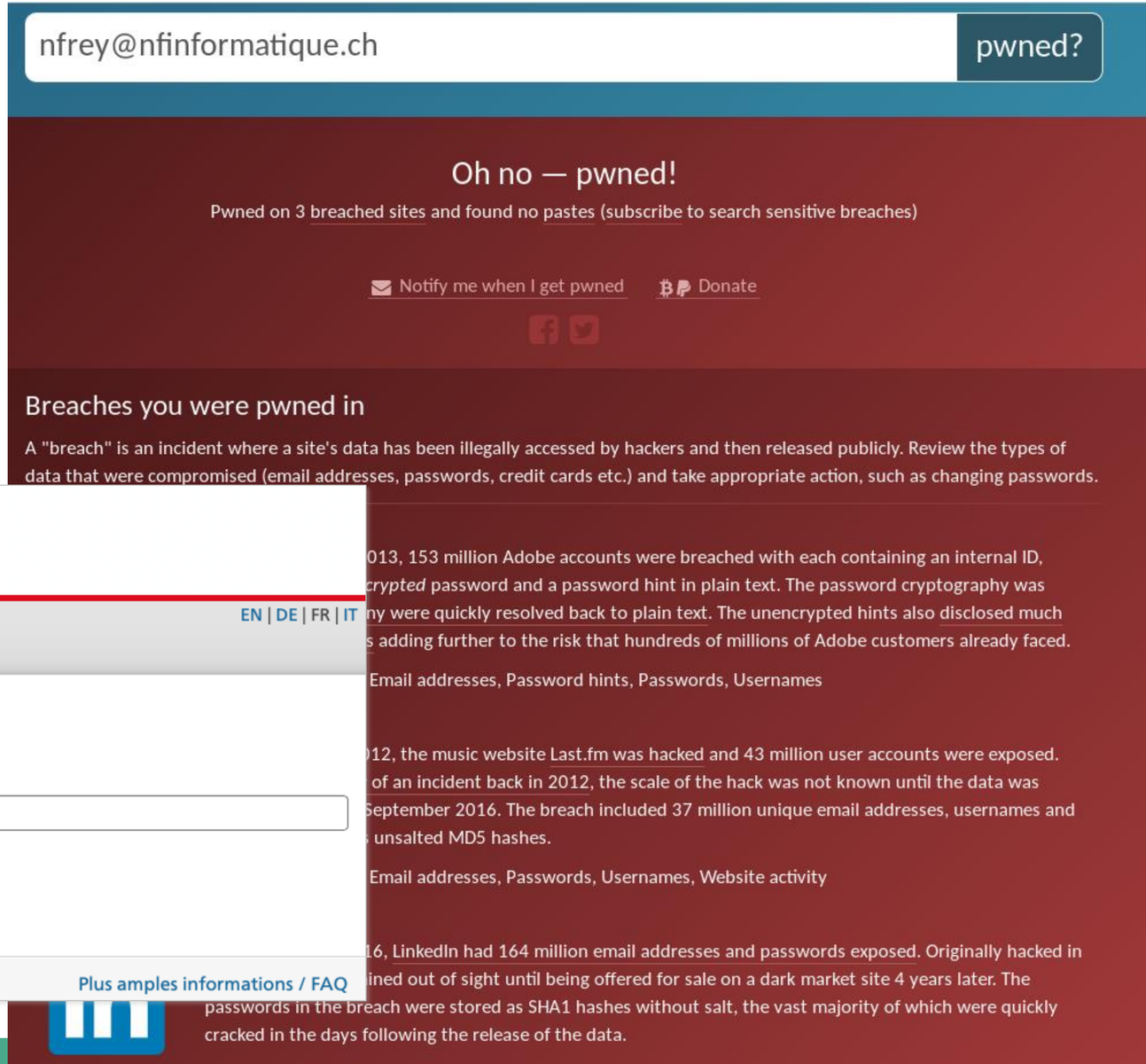
Pour distinguer **un e-mail légitime** d'un **e-mail de phishing:**

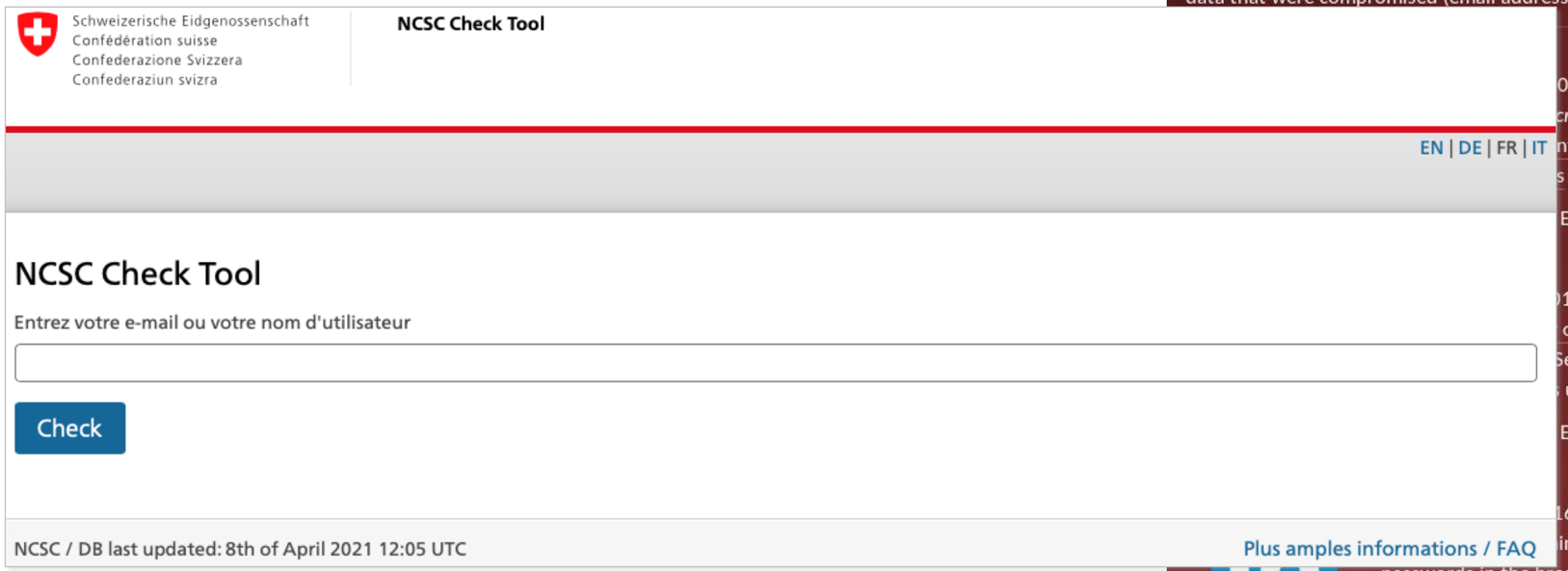
1. **Évaluation du contenu**
   - Urgence? Fautes d'orthographes? Données d'accès?
2. **Identifier l'émetteur**
   - ≠ nom affiché, mais adresse d'envoi effective
3. **Identifier les liens suspects**
   - Positionner la souris dessus pour l'afficher – ne pas cliquer!!
4. **Demander de l'aide et informer**

Vérifiez vos comptes

https://haveibeenpwned.com/

https://www.checktool.ch





CYBER SAFE

Le Label Suisse de Cybersécurité

Origines

Association créée en 2018
9 Membres fondateurs

Constats:

- Importance grandissante de la cybersécurité
- PME démunies (65% vs. 1%)
- Barrières: coûts, compétences, incertitudes

Sensibilisation: nécessaire, mais pas suffisante

CYBER SAFE

Objectif et approche

*Le Label pour aider les PME à atteindre un niveau de cybersécurité **acceptable***

- Définition **collective** des exigences: par et pour les PME (disponibles en ligne, licence CC)
- Les exigences varient selon le **niveau d'impact** des cyber incidents de l'organisation candidate.
- **Neutralité, indépendance**: pas de vente de mesures de remédiations (association et auditeurs).

CYBER SAFE

CYBER SAFE

Qui sommes-nous ?

- Monde économique, politique, académique et associatif
- 8’500 PME et >300 communes représentées
- Partenaire en CH-D

SKO ASC ASQ Association suisse des cadres

GIM-CH Groupement suisse de l'industrie mécanique
SWISSMECHANIC Suisse romande

heig-vd

Hes·so

EPFL C4DT Center for Digital Trust

CVCI Chambre vaudoise du commerce et de l'industrie

FPE-CIGA Fédération Patronale et Économique

Chambre Valaisanne de Commerce et d'Industrie
Walliser Industrie- und Handelskammer

Fédération des Entreprises Romandes Neuchâtel

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX

CCIG Chambre de commerce, d'industrie et des services de Genève

UNION DES COMMUNES VAUDOISES

ISSS Information Security Society Switzerland

.ICØN

Un Label reconnu

- Membre COPIL SNPC
- Partenaire RNS
- Projets communes suisses

Octobre 2020 | www.ncsc.ch

Rapport sur l'avancement des travaux concernant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018–2022

État au premier trimestre 2020

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Le Conseil fédéral

Sicherheitsverbund Schweiz
Réseau national de sécurité
Rete integrata Svizzera per la sicurezza

4.1.2 Label de cybersécurité

L'absence de normes ou des normes trop complexes empêchent les PME d'évaluer de façon transparente leur niveau de cybersécurité et de l'indiquer à des tiers. Le label de cybersécurité élaboré par l'Association suisse pour le label de cybersécurité (ASLaC) entend remédier à cette situation. Initiative privée développée en étroite collaboration avec des représentants des PME[6], ce label a été lancé le 18 décembre 2019 et contribue fortement à la mise en œuvre de la SNPC. Toutes les informations le concernant sont disponibles à l'adresse www.cyber-safe.ch.

Illustration 6: Cyber-safe.ch

4.2 Promotion de la recherche et de la formation

D'importants progrès ont été réalisés dans le champ d'action 1 «Acquisition de compétences et de connaissances». Le diplôme qui sanctionne le nouvel examen professionnel de spécialiste de la cybersécurité aidera à pallier le manque de main-d'œuvre qualifiée. Encouragé par l'armée dans le cadre de la création de sa propre instruction dans le domaine cybernétique, ce projet illustre parfaitement la collaboration constructive entre les services civils et militaires.
L'ouverture du Campus cyberdéfense (Campus CYD) dans les deux EPF et à Thoune constitue également une étape majeure. En tant que centre de compétences scientifique et technique, celui-ci améliorera le transfert de savoir entre les autorités et les milieux universitaires et contribuera à développer en Suisse un écosystème économique consacré à la cybersécurité. En cours de création, le nouveau «Swiss Support Centre for Cyber-Security» (SSCC) des deux EPF y contribuera également et jouera un rôle de coordination en servant de point de contact pour la Confédération et les cantons.

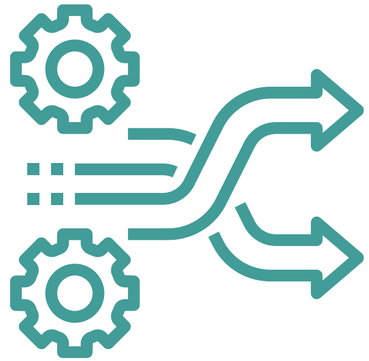
4.2.1 Examen professionnel de spécialiste en cybersécurité

Le 11 novembre 2019, l'organisation nationale du monde du travail ICT Formation

Label cyber-safe.ch – diagnostique

Scans de vulnérabilités

Tests de phishing (hameçonnage)



Processus, organisation

CYBER SAFE

ASSOCIATION SUISSE POUR LE LABEL DE CYBERSÉCURITÉ

Analyse de vos cyberrisques

Impacts possibles

Nous avons évalué le coût approximatif que des incidents de cybersécurité pourraient avoir sur vos activités. Les cinq événements les plus dangereux pour vos activités sont :

Type de donnée	Description
	Fuite de vos données

ASSOCIATION SUISSE POUR LE LABEL DE CYBERSÉCURITÉ

Niveau de protection

Selon les différentes informations que nous avons pu collecter jusqu'à présent, nous avons pu déterminer quelles sont les mesures de protection qui sont adaptées à votre situation. Nous avons pu évaluer lesquelles sont actuellement en place.

Votre niveau global de protection est MOYEN .

Protection globale

ASSOCIATION SUISSE POUR LE LABEL DE CYBERSÉCURITÉ

Vos priorités en un coup d'oeil

Voici, par ordre de priorité, les prochaines étapes que nous vous suggérons d'implémenter:

Priorité	Action	Détail	Requis	Coût	Effort
TRÈS HAUTE	Corriger les vulnérabilités critiques du réseau interne	Plusieurs vulnérabilités critiques existent sur votre réseau interne. Les détails se trouvent dans l'annexe. Dans la plupart des cas il s'agit d'effectuer une mise à jour des systèmes concernés.	Oui doc	$	15,0 [h]
HAUTE	Contrôler la sauvegarde	En cas de coup dur votre sauvegarde pourrait être salvatrice. Vérifiez qu'elle se passe correctement.	Oui doc	$$	5,0 [h]
HAUTE	Installer, mettre à jour et contrôler les antivirus	Les anti-virus sont des vaccins pour votre informatique. Vous devez vous assurer qu'ils sont installés sur chaque poste de travail et qu'ils sont bien mis à jour.	Oui doc	$$	20,0 [h]
HAUTE	Appliquer et contrôler les mises à jour des systèmes d'exploitation	Les mises à jour des systèmes d'exploitation des appareils contiennent des correctifs de sécurité. Vous devez veillez à ce que les mises à jour soient correctement appliquées.	Oui doc	$	20,0 [h]
HAUTE	Faire un test de récupération	La seule sauvegarde valable est celle qui vous permet de récupérer vos données. Vous devez régulièrement vérifier que ce soit bien possible.	Oui doc	$	18,0 [h]
HAUTE	Vérifier le fonctionnement et la mise à jour du pare-feu	Il est important que votre pare-feu soit fonctionnel et à jour pour détecter les comportements frauduleux.	Oui doc	$	35,0 [h]
HAUTE	Limiter les	Lorsqu'un utilisateur dispose d'un accès	Oui	$	28,0

ASSOCIATION SUISSE POUR LE LABEL DE CYBERSÉCURITÉ

Scans de votre réseau

Sur le réseau de travail

À corriger d'urgence :

[OSVDB:142291] The SSH service running on the remote host is affected by multiple vulnerabilities.
Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
Niveau de criticité : 10,0
Sur les hôtes suivants : *NBG6617.local*

[OSVDB:153673] The remote Windows host is affected by multiple vulnerabilities.
MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
Niveau de criticité : 10,0
Sur les hôtes suivants : *LIPSTICK36.local*

À corriger dès que possible :

[OSVDB:79590] The remote host is affected by a remote code execution vulnerability.
Dropbear SSH Server Channel Concurrency Use-after-free Remote Code Execution
Niveau de criticité : 7,1
Sur les hôtes suivants : *NBG6617.local*

À considérer :

[OSVDB:104810] The remote host is affected by a vulnerability that could allow sensitive data to be decrypted.
OpenSSL 'ChangeCipherSpec' MiTM Vulnerability
Niveau de criticité : 6,8
Sur les hôtes suivants : *NBG6617.local*

[nessus-plugin:57582] The SSL certificate chain for this service ends in an unrecognized

Label cyber-safe.ch – audit

Mise en œuvre des mesures correctives (en interne ou avec votre prestataire)

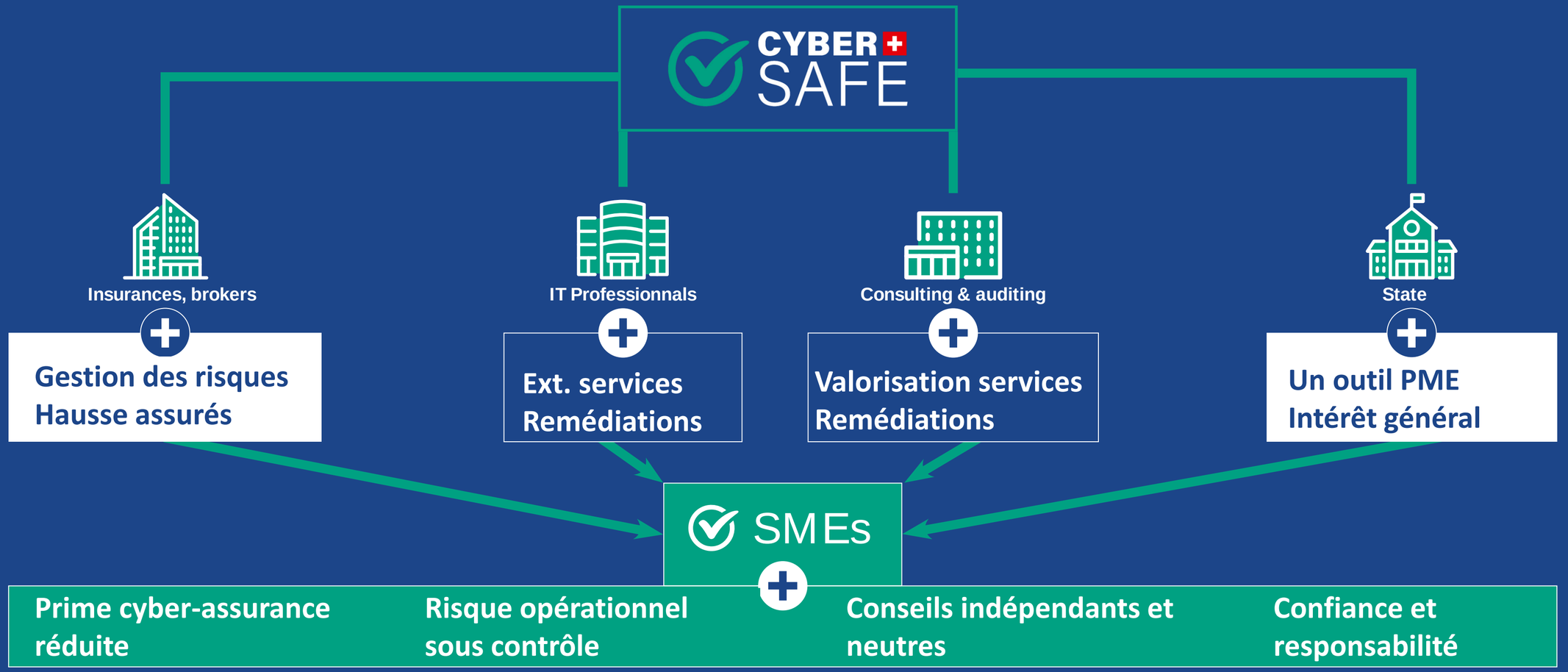
Audit de cybersécurité (3rd party)

Démarrer votre évaluation: www.cyber-safe.ch

CYBER SAFE

Label: quels avantages?

Ecosystème


CYBER SAFE
Insurances, brokers
IT Professionnals
Consulting & auditing
State
Gestion des risques
Hausse assurés
Ext. services
Remédiations
Valorisation services
Remédiations
Un outil PME
Intérêt général
SMEs
Prime cyber-assurance réduite
Risque opérationnel sous contrôle
Conseils indépendants et neutres
Confiance et responsabilité

Données en Suisse

Dès 4’000.-
Valable 2 ans

info@cyber-safe.ch

Des questions?