



FORMATION

La Cybersécurité

Comprendre les menaces, adopter les bons réflexes
et protéger son environnement numérique

Samuel Vermeulen
Consultant Informatique & Internet



Sommaire

01



Qu'est-ce que la cybersécurité ?

02



Panorama des menaces actuelles

03



Anatomie d'une cyberattaque

04



Zoom sur le phishing

05



Les logiciels malveillants

06



Mots de passe & authentification

07



Sécuriser son réseau

08



Bonnes pratiques au quotidien

09



Réagir en cas d'incident

Qu'est-ce que la cybersécurité ?

L'ensemble des lois, politiques, outils et pratiques mis en œuvre pour protéger les systèmes, les réseaux, les logiciels et les données contre les attaques, les dommages ou les accès non autorisés.

Les 3 piliers : le triangle DIC



Disponibilité

Les données et services doivent être accessibles quand on en a besoin.



Intégrité

Les données ne doivent pas être altérées ou modifiées sans autorisation.



Confidentialité

Seules les personnes autorisées peuvent accéder à l'information.

POURQUOI S'EN PRÉOCCUPER

Une menace bien réelle et croissante



+90%

des cyberattaques débutent par
un e-mail de phishing



x3

augmentation des attaques par
rançongiciel en quelques années



60%

des petites structures ferment
dans les 6 mois suivant une
cyberattaque majeure



220 j

délai moyen avant la détection
d'une intrusion dans un système

Panorama des menaces



Phishing

Usurpation d'identité par e-mail ou SMS pour voler des informations



Rançongiciel

Chiffrement des données contre une demande de rançon



Logiciels malveillants

Virus, vers, chevaux de Troie qui infectent les systèmes



Ingénierie sociale

Manipulation psychologique pour obtenir un accès ou une information



Déni de service

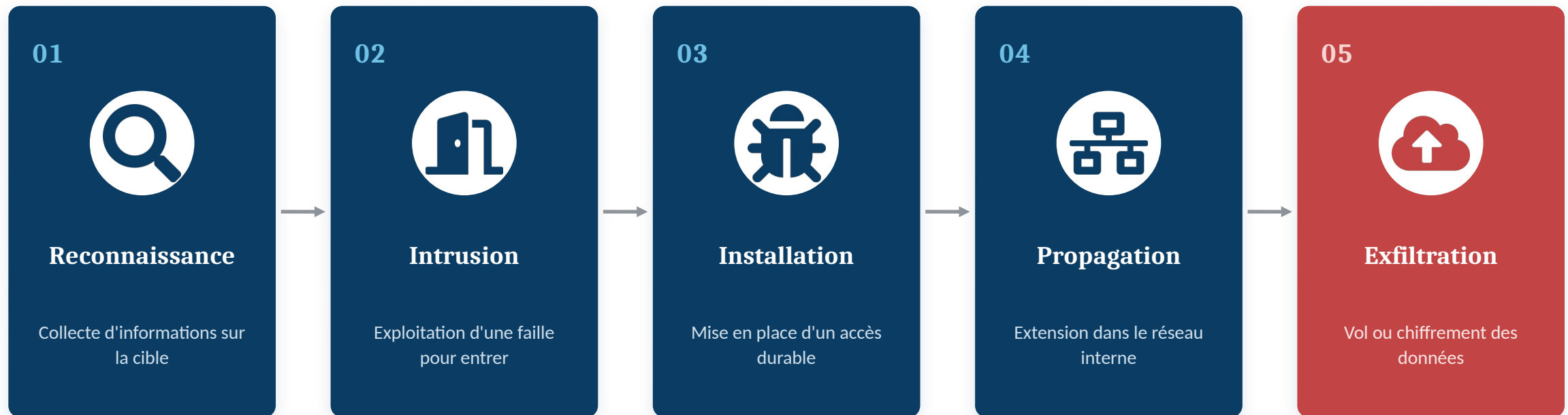
Saturation d'un service pour le rendre inaccessible (DDoS)



Vol de données

Exfiltration d'informations sensibles ou confidentielles

Anatomie d'une cyberattaque



Rompres la chaîne à n'importe quelle étape suffit à stopper l'attaque.

Zoom sur le phishing



Signaux d'alerte à repérer

- Urgence ou menace inhabituelle dans le message
- Adresse d'expéditeur légèrement différente de l'originale
- Lien dont l'URL ne correspond pas au domaine attendu
- Demande d'informations confidentielles ou de paiement

Les logiciels malveillants

Virus



S'attache à un programme sain et se propage lorsque celui-ci est exécuté.

Ver informatique



Se réplique et se propage seul à travers un réseau, sans intervention humaine.

Cheval de Troie



Se fait passer pour un logiciel légitime pour ouvrir une porte dérobée.

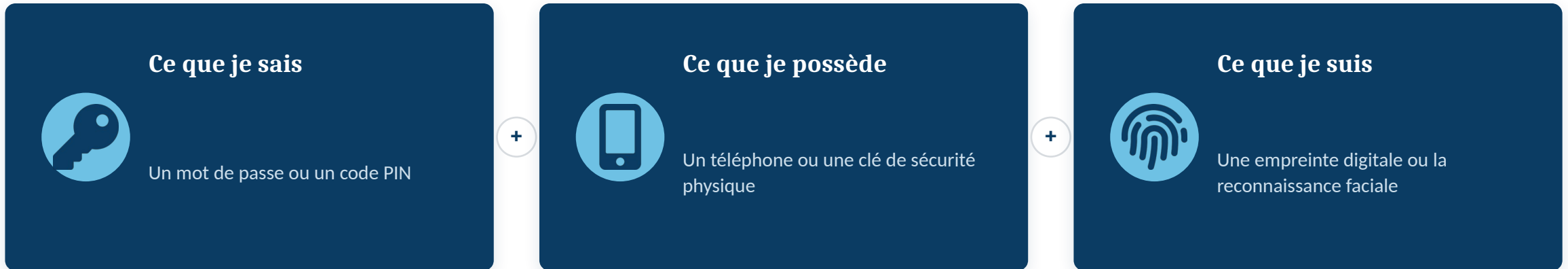
Rançongiciel



Chiffre les fichiers de la victime et exige une rançon pour les déverrouiller.

Mots de passe & authentification

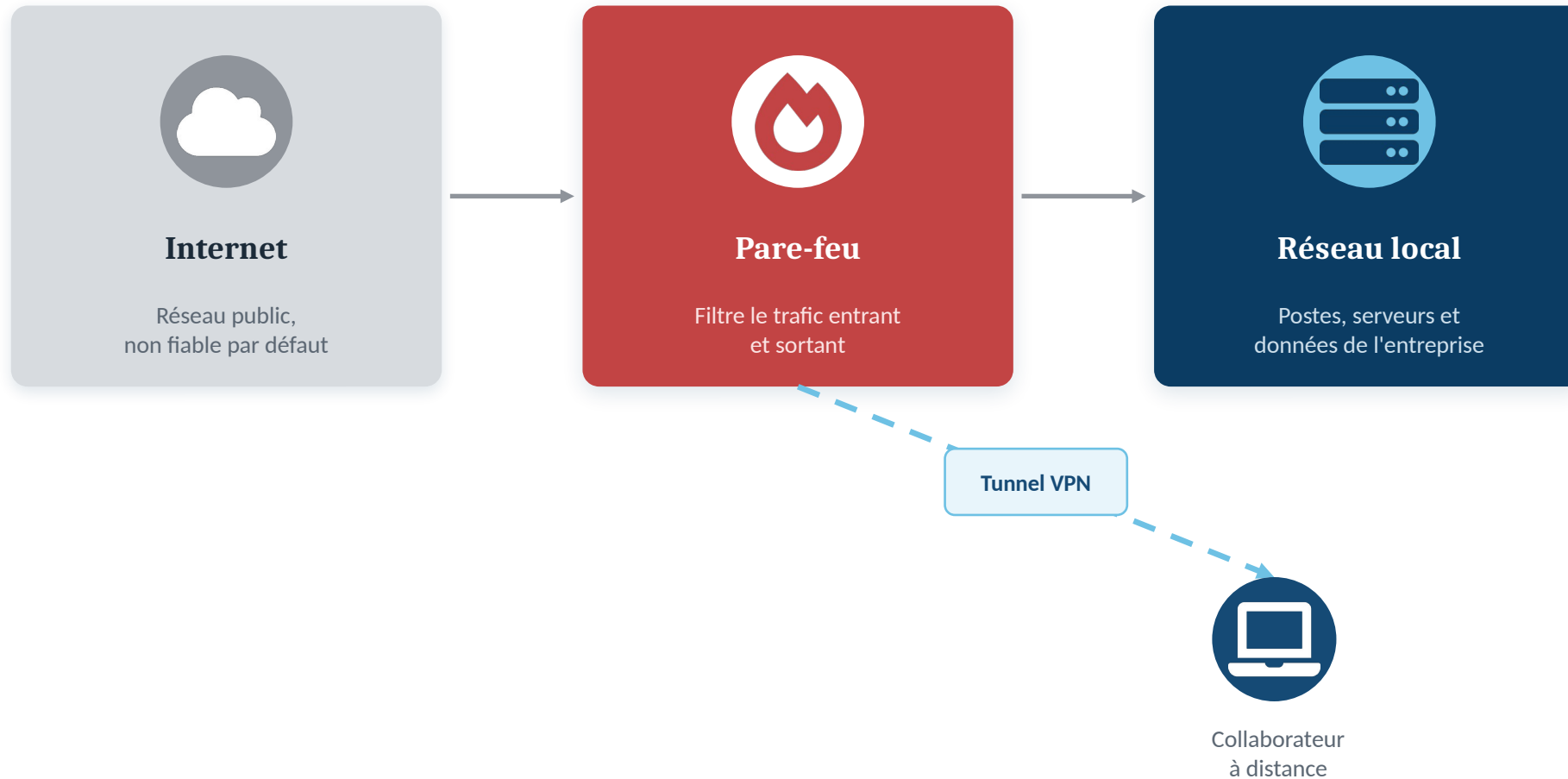
L'authentification multifacteur (MFA) combine plusieurs preuves d'identité



Créer un mot de passe robuste

- Au moins 12 caractères, en mélangeant majuscules, minuscules, chiffres et symboles
- Un mot de passe unique pour chaque service important
- Une phrase de passe facile à retenir mais difficile à deviner
- Un gestionnaire de mots de passe pour éviter de les réutiliser

Sécuriser son réseau



Bonnes pratiques

- Segmenter le réseau (Wi-Fi invités séparé)
- Chiffrer les connexions à distance (VPN)
- Mettre à jour les équipements réseau

Bonnes pratiques à adopter



Mettre à jour

Systèmes et logiciels à jour en permanence



Sauvegarder

Copies régulières, testées et hors ligne



Vérifier les liens

Survoler avant de cliquer, vérifier l'expéditeur



Verrouiller son poste

Session verrouillée dès qu'on s'absente



Séparer les usages

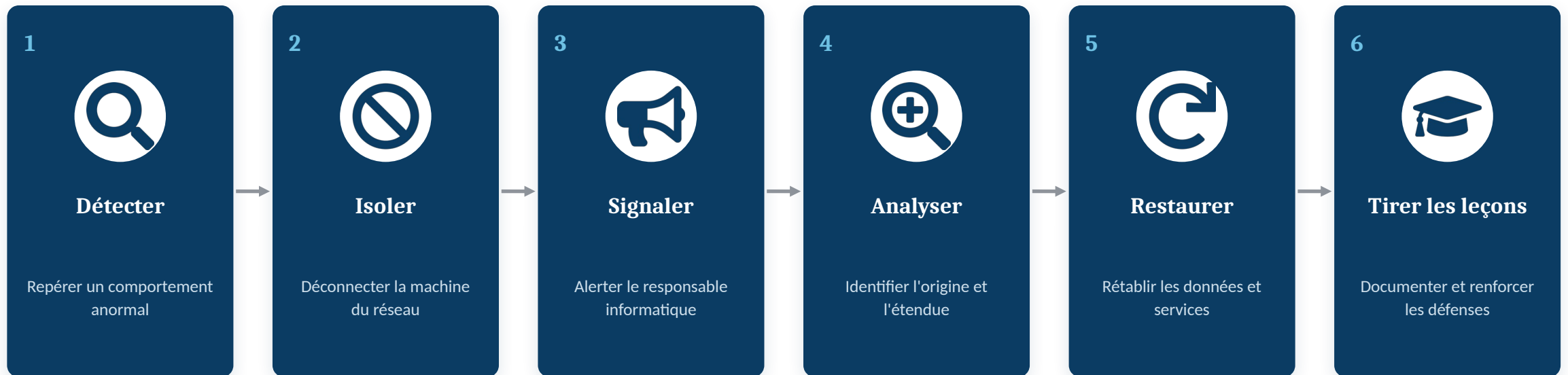
Comptes professionnels et personnels distincts



Signaler

Tout comportement suspect signalé sans délai

Réagir face à un incident



Un seul réflexe compte : signaler immédiatement plutôt que de tenter de résoudre seul.



Merci de votre attention

La cybersécurité est l'affaire de tous : rester vigilant, c'est déjà se protéger.

Samuel Vermeulen

Consultant Informatique & Internet — SVPRO