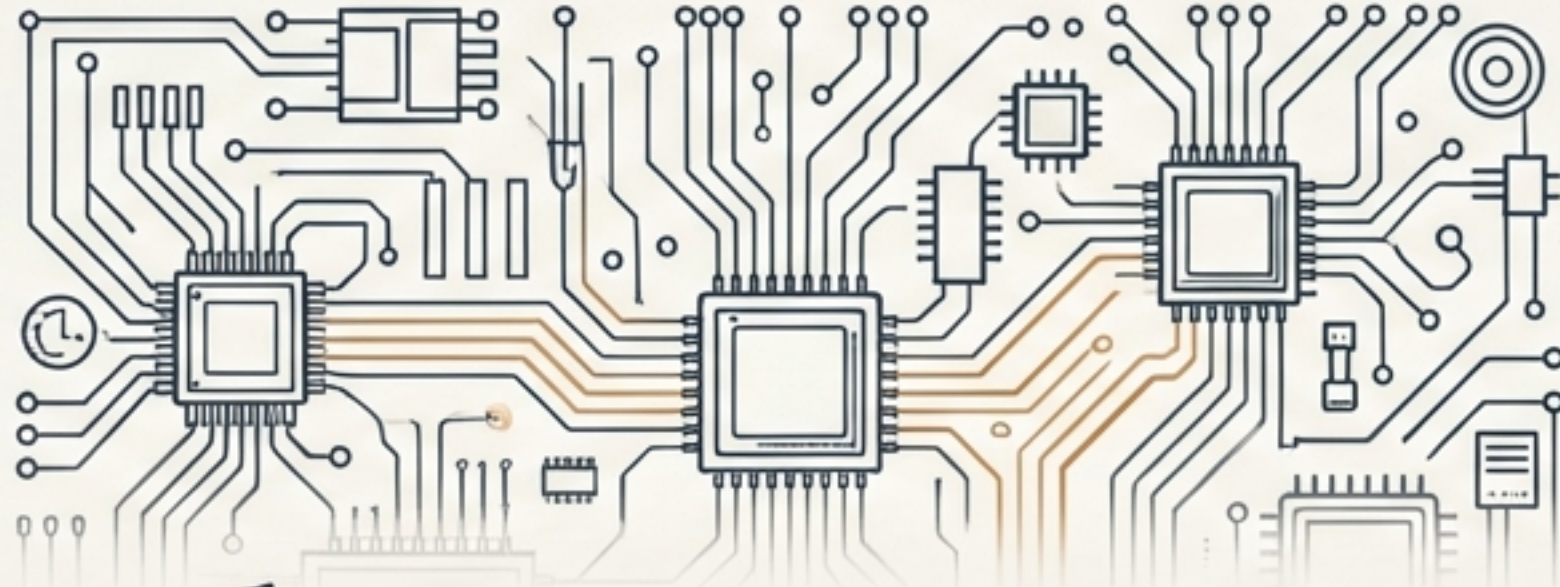




Protéger le Royaume Numérique

Les secrets pour défendre les données de votre future entreprise.



Une introduction aux principes fondamentaux de la cybersécurité.

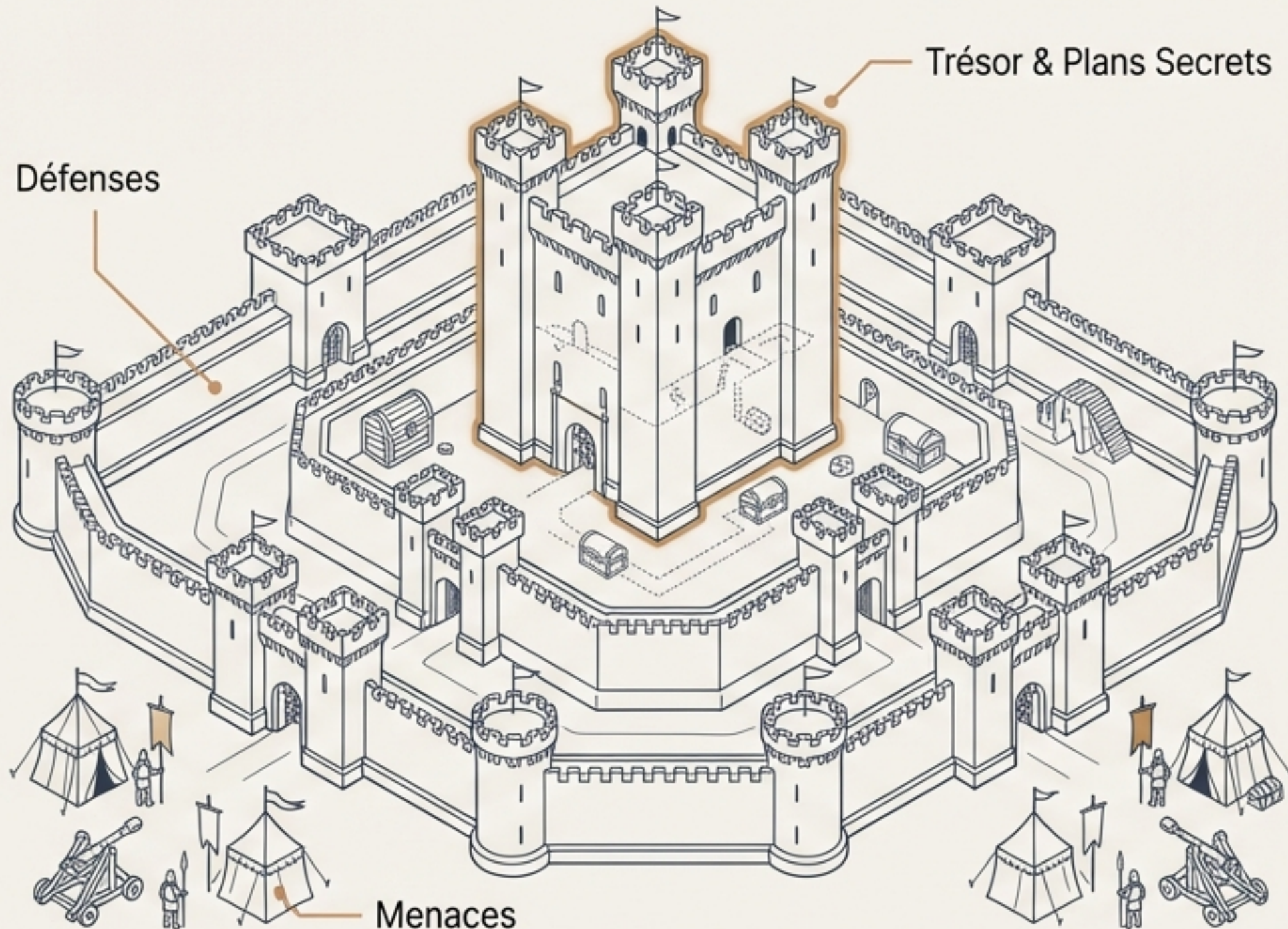


La cybersécurité vous intimide ?

On sait que ce mot peut faire un peu peur. On imagine des lignes de code complexes, des experts inaccessibles... Et si on vous disait que vous en comprenez déjà les principes fondamentaux sans même le savoir ?

Laissez-nous vous raconter une histoire simple. Une histoire de forteresse, de plans secrets et de royaumes à protéger. Vous allez voir, c'est bien plus logique que ça en a l'air.

Toute entreprise est une forteresse à défendre.



Imaginez que le système d'information de votre entreprise est une forteresse médiévale.

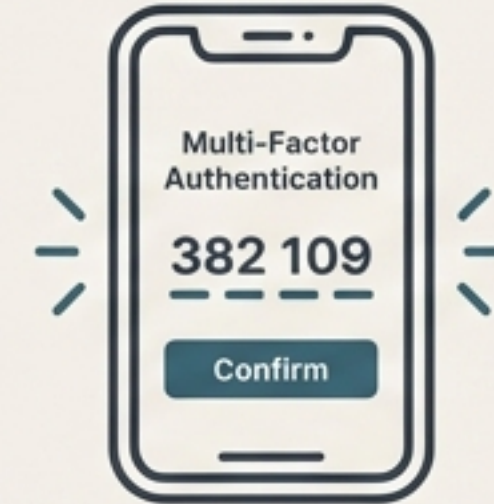
- **Les données précieuses** (fichiers clients, brevets, finances) sont le trésor et les plans secrets du royaume.
- **Les menaces** (hackers, virus) sont les armées ennemies et les espions qui rôdent.

Pour la protéger, vous n'avez pas besoin de magie, mais d'une stratégie basée sur trois piliers essentiels.

Pilier n°1 : Seuls les gardes autorisés peuvent lire les plans secrets.



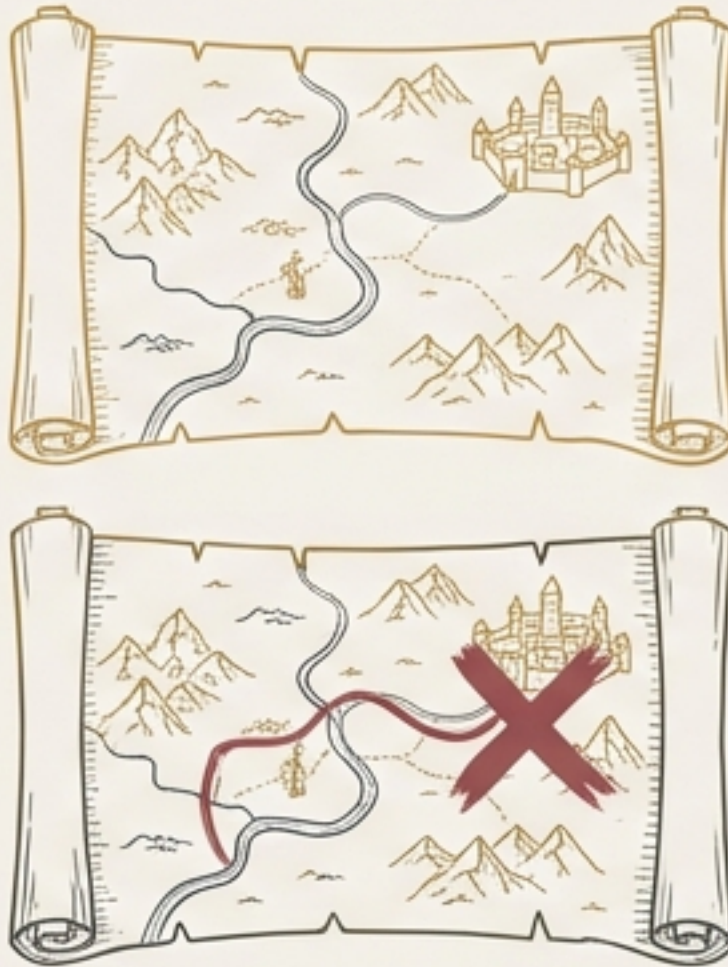
Dans notre forteresse, la première règle est simple : les informations stratégiques ne doivent pas tomber entre de mauvaises mains. Seuls le roi, la reine et les généraux ont le droit de consulter les plans de bataille. L'accès est contrôlé.



Dans le monde numérique, c'est le principe de **Confidentialité**.

- **Le but:** S'assurer que l'accès aux données est strictement réservé aux personnes autorisées.
- **Exemples concrets:**
 - Un mot de passe fort et unique.
 - La double authentification (MFA) sur votre banque en ligne ou vos mails, qui exige une seconde preuve d'identité.

Pilier n°2 : S'assurer que les cartes du royaume n'ont pas été falsifiées



Que se passe-t-il si un espion s'infiltré et modifie la carte, déplaçant un fleuve ou une forêt ? L'armée se perdra. Il est crucial que les informations soient non seulement secrètes, mais aussi exactes et fiables.



C'est le principe d'**Intégrité**.

- Le but: Garantir que les données ne sont pas modifiées ou détruites de manière non autorisée.
- Exemples concrets:
 - Les sauvegardes régulières, pour pouvoir restaurer une version "saine" des données.
 - Les systèmes de gestion de bases de données (comme Oracle ou MySQL) qui possèdent des mécanismes pour assurer la cohérence des informations.

Pilier n°3 : Garantir que les portes sont ouvertes et le ravitaillement assuré.



Une forteresse impénétrable ne sert à rien si ses propres armées ne peuvent pas en sortir pour défendre le royaume, ou si le ravitaillement n'arrive plus. Les ressources doivent être accessibles quand on en a besoin.



C'est le principe de **Disponibilité**.

- Le but: Assurer que le système et les données sont accessibles et fonctionnels pour les utilisateurs légitimes à tout moment.
- Exemples concrets:
 - Avoir des serveurs redondants (un "plan B" si le serveur principal tombe).
 - Utiliser des protections contre les attaques par déni de service (DDoS), qui visent à submerger un site pour le rendre inaccessible (ex: solutions Akamai).

Le secret des pros : La Triade CIA

Ces trois piliers que vous venez de découvrir à travers notre histoire de forteresse forment la base de toute la stratégie de cybersécurité moderne. C'est un modèle fondamental que tous les professionnels connaissent.



Confidentialité

(Qui peut voir ?)



Intégrité

(L'info est-elle fiable ?)

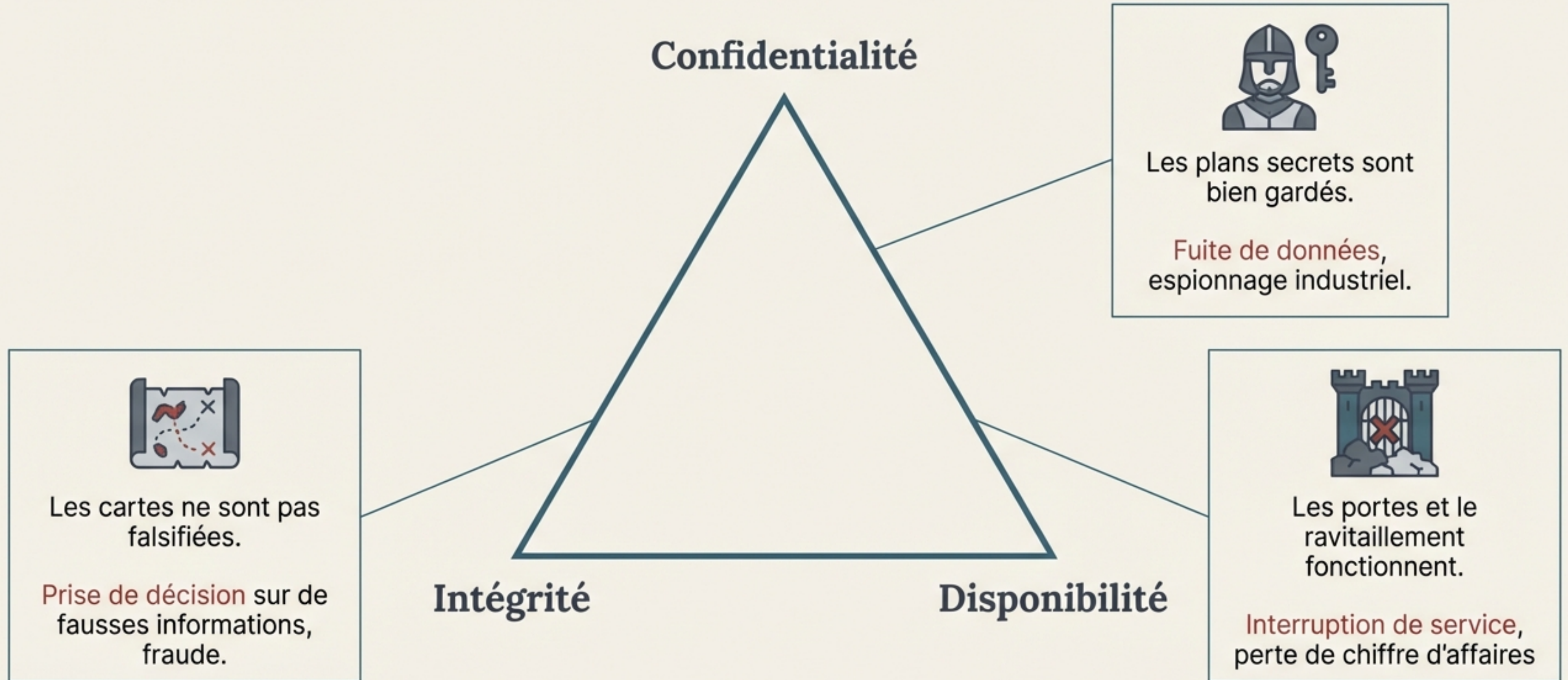


Availability (Disponibilité en anglais)

(Est-ce que ça fonctionne ?)

Vous voyez, c'est tout à fait logique. Vous venez de maîtriser le concept le plus important du domaine.

La Triade CIA : Votre feuille de route stratégique





L'erreur de débutant à éviter : la forteresse à une seule muraille.

Beaucoup de gens pensent que la cybersécurité, c'est juste une question de mots de passe. C'est comme construire une forteresse avec une porte blindée, mais sans vérifier si un espion empoisonne les puits (Intégrité) ou si les catapultes sont rouillées (Disponibilité).

Un bon mot de passe ne sert à rien si les données qu'il protège sont fausses ou si le service est inaccessible. Les trois piliers sont indissociables pour une défense solide.

Pourquoi ce combat est si important pour votre avenir professionnel.

Comprendre cette triade, ce n'est pas juste pour réussir un examen. C'est comprendre le champ de bataille numérique sur lequel chaque entreprise évolue aujourd'hui. Quand un de ces piliers s'effondre, les conséquences peuvent être dramatiques. Voyons un exemple qui a marqué l'histoire.

L'attaque "WannaCry" : quand la disponibilité s'effondre.

En 2017, le virus WannaCry a paralysé des centaines de milliers d'ordinateurs dans le monde. Son attaque ? Il n'a pas volé les données (Confidentialité) ni modifié les fichiers (Intégrité). Il a **chiffré** les données, les rendant totalement **inaccessibles**.

La cible ? La **Disponibilité**.

La conséquence ? Des hôpitaux comme le NHS britannique ont dû annuler des opérations, des usines ont stoppé leur production.

La rançon demandée était presque secondaire face à la paralysie totale des services.



Le coût d'une brèche dans la forteresse.



C'est le pourcentage d'entreprises françaises ayant subi au moins une cyberattaque en 2022. La question n'est plus "si" mais "quand".

ANSSI, 2022



C'est le coût moyen mondial d'une seule violation de données pour une entreprise en 2023. Cela inclut les pertes financières, les amendes, et l'impact sur la réputation.

IBM, 2023

Ces chiffres montrent que la sécurité n'est pas un coût, mais un investissement stratégique.

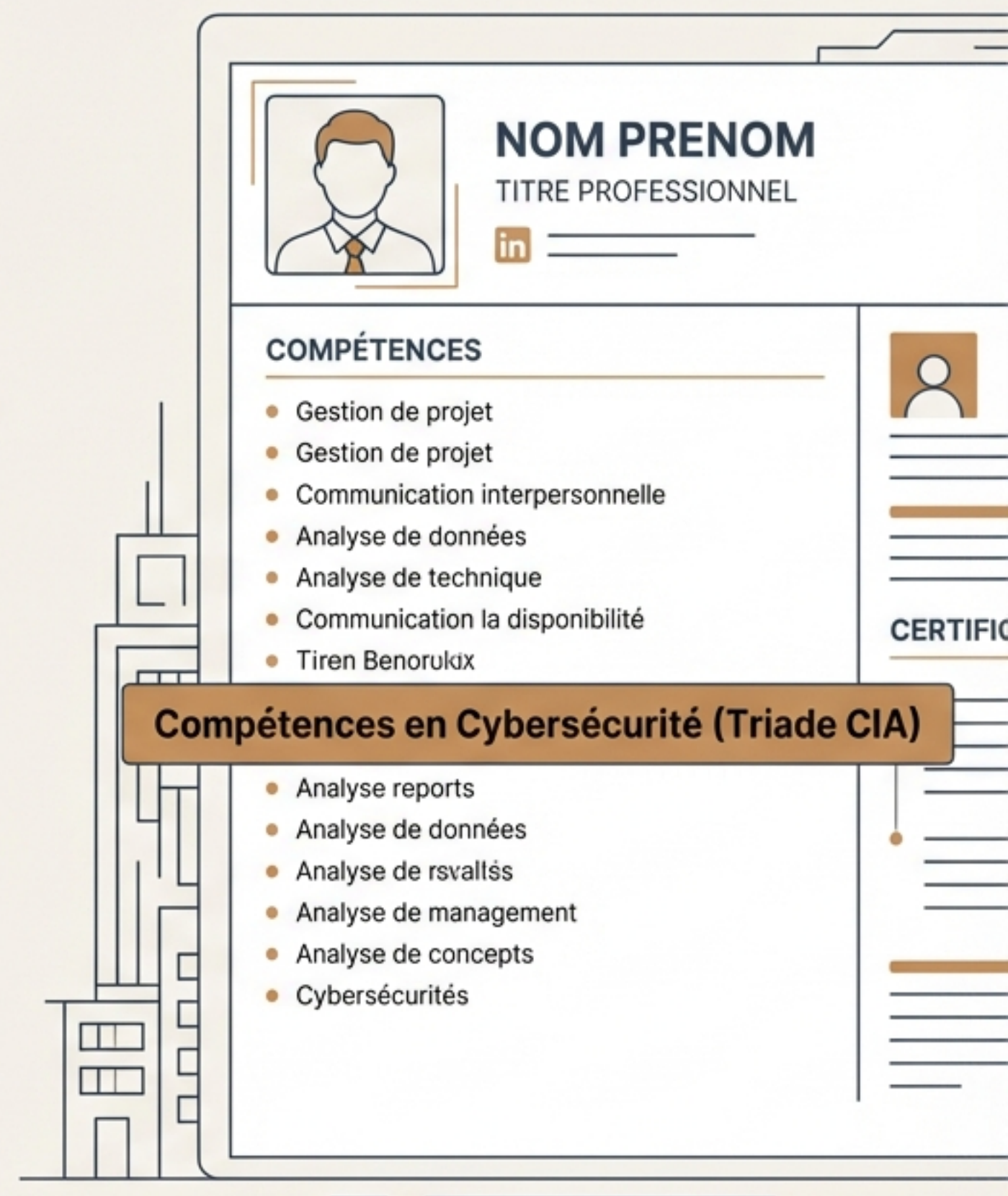
Comprendre la Triade CIA : votre atout majeur en entreprise.

En maîtrisant ces trois concepts, vous n'êtes plus seulement un futur technicien, commercial ou manager. Vous devenez un professionnel qui comprend les risques numériques.

Savoir parler de Confidentialité, d'Intégrité et de Disponibilité vous permet de :

- **Participer aux décisions stratégiques.**
- **Dialoguer efficacement avec les équipes techniques.**
- **Protéger la valeur de votre entreprise.**

C'est une compétence qui vous distinguera, quel que soit votre poste. C'est un vrai plus sur un CV.



Au-delà de la technique : une question de responsabilité.

La protection des données n'est pas qu'un enjeu technique, c'est aussi un enjeu éthique et légal.

- Le **RGPD** (Règlement Général sur la Protection des Données) impose aux entreprises de protéger les données personnelles de leurs clients, renforçant l'importance de la **Confidentialité** et de l'**Intégrité**.
- Cela s'inscrit dans la **RSE** (Responsabilité Sociale des Entreprises) : une entreprise qui protège bien ses données est une entreprise digne de confiance.



Sécurité



RGPD



Éthique & RSE



Vous êtes les futurs gardiens du royaume numérique.

La forteresse numérique évolue chaque jour, mais ses principes de défense restent les mêmes. Vous avez maintenant la carte et la boussole pour la protéger.

Ne sous-estimez jamais la valeur de ce que vous venez d'apprendre. **C'est une fondation solide pour votre réussite et pour la sécurité des entreprises que vous rejoindrez.**

Bonne chance pour vos examens, et pour votre carrière.