

## 1. Création d'une identité d'entreprise

### Nom de l'entreprise :

- **CypherGuard**  
(Évoque la protection des données avec un aspect technique et sécurisé)

### Wording (ton de communication, slogan, message clé)

- **Slogan :**  
"La cybersécurité sans compromis."
- **Message clé :**  
CypherGuard est une solution de cybersécurité avancée, dédiée à protéger vos données sensibles et à sécuriser vos infrastructures. Nous mettons l'accent sur la protection proactive des réseaux, des systèmes et des informations critiques contre les menaces évolutives. Notre objectif est de vous offrir une cybersécurité sur mesure, tout en simplifiant la gestion des risques.
- **Ton de communication :**  
Technique, rassurant et accessible. Le langage doit être à la fois professionnel et compréhensible, même pour des clients qui ne sont pas des experts en cybersécurité.

### Valeurs principales :

- **Anticipation** : Nous prévoyons les menaces et nous les neutralisons avant qu'elles ne deviennent problématiques.
  - **Excellence** : Nos solutions et services sont développés par les meilleurs experts du secteur.
  - **Personnalisation** : Nous adaptons nos services aux besoins spécifiques de chaque client.
  - **Confiance** : Nous offrons une transparence totale dans nos actions et une garantie de confidentialité absolue.
  - **Innovation** : Nous utilisons les technologies les plus récentes, notamment l'intelligence artificielle et le machine learning pour améliorer la protection.
- 

## 2. Définition des objectifs et de la stratégie

### Objectifs principaux :

- **Protéger les entreprises contre les cyberattaques :**  
CypherGuard a pour mission d'apporter des solutions de protection proactive aux entreprises de taille moyenne qui n'ont pas de département dédié à la sécurité.
- **Créer une plateforme SaaS pour la gestion des risques :**  
Offrir une solution en ligne qui surveille et protège les systèmes 24/7 avec des rapports en temps réel et des suggestions d'amélioration.
- **Former les utilisateurs :**  
Organiser des sessions de formation pour sensibiliser les employés aux bonnes pratiques de cybersécurité.

### Vision court terme (6 à 12 mois) :

- **Lancer la version initiale du service de cybersécurité :**  
Services de surveillance, audits de sécurité, tests de pénétration (pentests), et formation en

cybersécurité.

- **Obtenir 10 à 20 clients PME :**

Tester la plateforme et recevoir des retours afin d'améliorer l'offre.

- **Développer un programme de sensibilisation et de formation pour les clients :**

Créer des modules en ligne et en présentiel pour les aider à comprendre les bases de la cybersécurité.

### Vision long terme (3 à 5 ans) :

- **Intégrer des services avancés avec IA :**

Mettre en place une plateforme capable d'anticiper les menaces grâce à l'intelligence artificielle et l'analyse comportementale des systèmes.

- **Créer des solutions personnalisées pour des secteurs spécifiques :**

Proposer des services adaptés aux secteurs à haut risque comme la finance, la santé ou l'industrie.

- **S'étendre à l'international :**

Proposer des services via une plateforme cloud pour s'ouvrir à des marchés internationaux, et développer des partenariats avec des entreprises technologiques dans différents pays.

- **Proposer des services de réponse aux incidents :**

Étendre les services à la réponse aux incidents en temps réel, avec des équipes prêtes à intervenir lors d'une cyberattaque.

## 3. Création d'un budget de lancement

### Dépenses initiales :

Dépenses	Montant (€)
Développement des outils de sécurité (logiciels de surveillance, outils d'audit)	30 000
Marketing (site web, pub en ligne)	7 000
Outils et infrastructure cloud	5 000
R&D et formation interne (IA, apprentissage des systèmes)	8 000
Assurances, certifications de sécurité	4 000
Recrutement et salaires initiaux	15 000
<b>Total</b>	<b>69 000 €</b>

### Revenus attendus :

Source de revenu	Montant mensuel estimé (€)
Contrats de sécurité (service continu)	1 000 € par client (objectif de 10 clients la première année)
Audits et tests de pénétration	2 000 € par audit (objectif de 2 audits par mois)
Formation des employés (services annexes)	500 € par session de formation
<b>Revenus prévisionnels 1ère année</b>	<b>144 000 €</b>

### Sources de financement :

- **Apports personnels :** 20 000 €
- **Prêt bancaire ou microcrédit :** 30 000 €

- **Investisseurs privés ou Business Angels : 19 000 €**
- 

#### **4. Suggestions de noms alternatifs pour l'entreprise :**

- **FortiTech**  
*(Évoque la solidité et la protection technologique)*
  - **SecuraMind**  
*(Un nom moderne et professionnel qui combine sécurité et réflexion stratégique)*
  - **Vigilance360**  
*(Suggère une protection constante et omniprésente, idéal pour un service de cybersécurité)*
  - **HexaShield**  
*(Un nom qui évoque un bouclier numérique, solide et multifacette)*
  - **NetSentinel**  
*(Le réseau étant au cœur de la cybersécurité, cela évoque la surveillance continue)*
- 

#### **Avantages de cette entreprise :**

- **Demande croissante :**  
Avec l'augmentation des cyberattaques, la cybersécurité est un secteur en pleine expansion, surtout pour les PME.
  - **Scalabilité :**  
Une fois les solutions développées, elles peuvent être proposées en tant que services à distance (SaaS), ce qui permet de gérer plusieurs clients sans augmenter significativement les coûts.
  - **Innovation continue :**  
Les technologies comme l'IA et l'automatisation permettent de rester à la pointe de la technologie, en offrant des services toujours plus efficaces.
-