Les besoins matériels d'un Pentester (testeur d'intrusion) et d'un Analyste en Cybersécurité peuvent varier en fonction des tâches spécifiques qu'ils effectuent. Cependant, voici une liste générale des équipements et des ressources nécessaires pour ces deux profils :

### **Besoins matériels d'un Pentester :**

* **Ordinateur puissant** : Un ordinateur performant avec suffisamment de puissance de traitement pour exécuter des outils de test d'intrusion et des machines virtuelles.
* **Carte réseau sans fil** : Pour tester la sécurité des réseaux sans fil.
* **Adaptateurs réseau** : Certains tests peuvent nécessiter des adaptateurs
* réseau spécifiques pour simuler différentes configurations réseau.
* **Smartphone** : Utilisé pour tester la sécurité des applications mobiles.
* **Stockage externe chiffré** : Pour stocker en toute sécurité les données sensibles et les résultats des tests.
* **Outils matériel** : Certains pentesters peuvent utiliser des dispositifs matériels tels que des clés USB spécialisées ou des dispositifs de captage réseau.

### **Besoins matériels d'un Analyste en Cybersécurité :**

* Ordinateur puissant : Un ordinateur performant pour effectuer des analyses de sécurité, gérer les outils de sécurité et interpréter les données.
* Écrans multiples : Pour faciliter la surveillance des activités de sécurité et l'analyse des journaux.
* Outils de visualisation des données : Logiciels de visualisation de données pour comprendre rapidement les tendances et les anomalies.
* Stockage sécurisé : Pour stocker les données de sécurité de manière sécurisée, conformément aux politiques de l'entreprise.
* Serveurs dédiés : Certains analystes peuvent avoir besoin d'accéder à des serveurs dédiés pour effectuer des analyses approfondies.
* Outils de surveillance du réseau : Logiciels et matériel de surveillance du réseau pour détecter les activités suspectes.
* Logiciels de simulation d'attaque : Pour tester la résilience du réseau et des systèmes.
* Systèmes de gestion des informations et des événements de sécurité (SIEM) : Pour collecter, analyser et gérer les informations de sécurité.

Il est important de noter que les besoins spécifiques peuvent varier en fonction de la complexité des tâches et des responsabilités assignées à chaque professionnel en cybersécurité. Les mises à jour régulières des logiciels et la formation continue sont également essentielles pour rester efficace dans ces domaines en constante évolution.

Disk SSD : 512gb ou 1T (installation de machine virtuel,windows, etc …)

* disque dure externe ou cloud.

Ram : 32 Go pour tâches intensives ou 16Go de préférence, si petit budget minimum 8Go.

Processeur :