1 . Vous devez rechercher les types de menaces, identifier leurs origines potentielles et les méthodes par lesquelles elles peuvent pénétrer les systèmes d'information.

1/ Vol de données : sur cloud et BDD
2/ coupures électriques
3/ catastrophe naturelle et épidémie
4/ Ransomware hameçonnage ingénierie sociale
5/ vol des comptes
6/ vulnérabilité logicielles : CRM, logiciel métier
7/ Problèmes hébergeur

	Origine potentielle	méthode	Niveau de risque
Vol de données	Cybercriminalité concurrents menaces internes	Mot de passe faible Phishing malwares erreurs humaines	Élevé
coupures électriques	Accidents criminel	Désastre naturel	Faible (cloud)
catastrophe naturelle et épidémie	Éléments naturels	Environnemental	Élevé
ransomware hameçonnage ingénierie sociale	Cybercriminalité concurrents	Erreur humaine	Élevé
vol des comptes	Cybercriminalité	Mot de passes faibles Malwares Phishing	Moyen
vulnérabilité logicielles : CRM, logiciels métiers, applications mobiles	Concurrents (vol données clients) Cybercriminalité	Malwares Failles logicielles	Élevé
Problèmes hébergeur	Accident	Environnemental	Faible

2. Votre mission est de sélectionner 5 à 10 principes de sécurité essentiels, justifier leur choix et les prioriser.

	Spécifique	Mesurable	Atteignable	Réaliste	temporel
Authentification forte	Mise en place de l'AF pour tous les utilisateurs	Évolution de l'activation de l'AF	Formation et sensibilisation aux utilisateurs	Réduction du risque aux comptes et données sensibles	Mise en place de quotas avec objectif de 100% sur le trimestre
Chiffrement des données sensibles	Chiffrer sur support de stockage pour en assurer la confidentialité	Evolution du chiffrage de la totalité des données	Utilisation des bons outils de chiffrement, pour assurer un flux continu de chiffrement des données sensibles	Chiffrer les données en cas de fuite	Chiffrer l'ensemble des données sensibles de façon continue, 100% données chiffrés par trimestre
Mise à jour des logiciels et systèmes	Établir une politique de MAJ	Suivre le % des applications à jour	Mettre en place un suivi hebdomadaire de MAJ	Réduire les risques de vulnérabilité	Politique de MAJ avant la fin du trimestre
Sauvegarde	Sauvegarder de façon quotidienne les données	Suivre le % des sauvegardes effectuées et réussies	Mettre en place un logiciel de sauvegarde automatisé	Assurer la disponibilité et l'intégrité des données en cas de pertes ou de vol	Politique de sauvegarde à instaurer avant la fin du mois
Pare-feu et surveillance et détection des menaces	Mettre en place par feu pour contrôle trafic entrant et sortant	Suivre les activités du pare feu, mesurer le nombre d'incidents de sécurité et détecté	Configurer et déployer par feu adapté, installer et installer des outils de détection des menaces	Contribution à protéger les données de l'entreprise en sécurisant le réseau	Mettre en place les pare feu et systèmes de détection de menaces d'ici la fin du trimestre, et faire les MAJ de façon périodique
Formation continue et Sensibilisation à la sécurité	Organisation de journées formation à la cybersécurité	Suivre l'évolution des participants et l'accompagnement	Formation continue en fonction d l'évolution des menaces	Réduire les risques liées aux erreurs humaines	Organisation de sessions de formation d'ici la fin du semestre

Les principes fondamentaux de sécurité au spectre des trois principes fondamentaux:

1/ Chiffrement des données sensibles : Intégrité et Confidentialité
2/ Sauvegarde : Intégrité et disponibilité
3/ Authentification forte : Confidentialité

4/ Mise à jour des logiciels et systèmes : Intégrité et Disponibilité
5/ Pare-feu et surveillance et détection des menaces : Confidentialité et Intégrité
6/ Formation continue et sensibilisation à la sécurité : Confidentialité