BTS SIO · BLOC 3 CYBERSÉCURITÉ

Nom : .....

Audit — Panorama des cybermenaces

Durée conseillée : 2 h

Consigne : Répondez aux trois parties à partir de la brochure **CNIL Cybersécurité 2026** et du **CyberDico de l'ANSSI**.

Partie 1 — La réalité du terrain en chiffres (Brochure CNIL 2026)

1. **En 2025, combien de notifications de violations de données la CNIL a-t-elle reçues en moyenne par jour et au total sur l'année ?**

2. **Quel pourcentage des violations notifiées concerne une perte de confidentialité des données ? Que signifie concrètement cette perte ?**

3. **Quels sont les deux secteurs d'activité les plus touchés par les violations de données en France ? Précisez leurs pourcentages respectifs.**

4. **Quel type d'attaque malveillante représente à lui seul 9 % des violations (539 cas) et entraîne une indisponibilité majeure des systèmes ?**

5. **Quel est le montant maximal des sanctions financières que la CNIL peut prononcer en cas de manquement grave aux règles de sécurité du RGPD ?**

Partie 2 — Lexique officiel des cybermenaces (CyberDico ANSSI)

Renseignez le terme anglais de chaque attaque dans le premier tableau, puis reportez son numéro (1 à 10) dans la case correspondante face à sa définition simplifiée dans le second tableau.

Terme français	Terme anglais
1. Hameçonnage	
2. Hameçonnage ciblé	
3. Saisie d'identifiants	
4. Homme-du-milieu	
5. Rançongiciel	
6. Enregistreur frappes	
7. Renifleur	
8. Exfiltration données	
9. Injection indirecte	
10. Moisson courriels	

N°	Définition synthétique simplifiée
	Logiciel paralysant le système par chiffrement des données et exigeant une rançon.
	Interposition discrète d'un attaquant dans une communication réseau pour intercepter ou altérer les flux.
	Collecte automatisée et massive d'adresses électroniques sur le web pour le spam et le phishing.
	Vol d'identifiants ou données par subterfuge via un courriel imitant un tiers de confiance.
	Dispositif matériel ou logiciel enregistrant en continu toutes les frappes clavier à l'insu de l'usager.
	Ingénierie sociale ciblant précisément une personne en exploitant son contexte professionnel.
	Copie et transfert illicite de données sensibles internes vers un serveur externe sous contrôle pirate.
	Outil capturant et analysant les trames réseau et données non chiffrées qui transitent.
	Injection de scripts arbitraires dans une page web pour voler les sessions (cookies) d'usagers connectés.
	Attaque automatisée réutilisant des couples identifiant/mot de passe issus de fuites antérieures.

Partie 3 — Étude de cas réel : Fiche d'incident

Choisissez une attaque parmi les dix du CyberDico et analysez un cas réel documenté ayant conduit à une fuite de DCP.

Organisation victime : ……

Date de l'incident : ……

Type d'attaque retenu (parmi les 10) :

……

Mode opératoire (vecteur d'entrée, procédé technique, déroulement de l'attaque) :

……

……

……

……

Données personnelles compromises (catégories) & conséquences métier ou financières :

……

……

……

……