Devoir Surveillé – BTS SIO 1ère année (B3)

Introduction à la cybersécurité

Durée totale : 1 heure
Partie 1 – Questions de cours (6 points)
Partie 2 – Étude de cas simplifiée (12 points)

La justification, la rigueur, la rédaction et le soin de la copie entrent dans la notation sur 2 points.

Partie 1 – Révision de cours (6 points)

Système d'Information et actifs (1,5 point)

1. Citer **3 catégories d'actifs** différentes et donner un exemple concret pour chacune.
2. Expliquer ce qu'est la **criticité** d'un actif et donner 2 critères qui l'influencent.

Triade CIA (2 points)

1. Définir **Confidentialité**, **Intégrité**, **Disponibilité**.
2. Associer chaque scénario au(x) pilier(s) compromis et justifier:

Scénario	Pilier(s) compromis	Justification
Un administrateur modifie accidentellement la configuration d'un routeur, causant des pertes de paquets		
Un mail confidentiel est envoyé par erreur à tous les employés		
Une attaque DDoS rend le site web inaccessible pendant 6 heures		

Menace, vulnérabilité, incident, risque (1,5 point)

1. Donner une **définition** courte de chacun des 4 termes.
2. Classer les situations ci-dessous et justifier en une phrase:
   a) Les mots de passe administrateurs sont stockés dans un fichier Excel non protégé
   b) Un groupe de hackers spécialisé dans les ransomwares cible le secteur de la santé
   c) Un employé clique sur un lien de phishing et installe un malware sur son poste

QCM — notions rapides (1 point)

Donner la bonne réponse et justifier en une phrase:

1. L'intégrité protège contre: (A) divulgation de données, (B) interruption de service, (C) altération de données
2. La propriété de **non-répudiation** permet de: (A) chiffrer les données, (B) prouver qu'une action a été faite par quelqu'un, (C) bloquer les virus
3. Un serveur web obsolète non patché depuis 1 an est une: (A) menace, (B) vulnérabilité, (C) incident

Partie 2 – Étude de cas (12 points)

Contexte

« BioLab » est un laboratoire d'analyses médicales (15 personnes). Le système informatique gère les dossiers patients, les résultats d'analyses et la facturation. Le laboratoire doit respecter des obligations RGPD strictes car il manipule des données de santé.

Étape 1 – Actifs et criticité (3 points)

1. Lister **4 actifs** de BioLab et les **classer par catégorie** (matériel, logiciel, informationnel, humain, immatériel).
2. Donner une **criticité** (faible/moyenne/élevée/critique) pour chaque actif et **justifier les 2 plus critiques**.

Étape 2 – Typologie des menaces (3 points)

Classer chaque situation dans la bonne catégorie (Humaine intentionnelle / Humaine non intentionnelle / Technique / Environnementale / Légale) et justifier:

Situation	Catégorie	Justification
Un technicien de maintenance insère une clé USB infectée par erreur		
Une inondation endommage la salle serveurs située au sous-sol		
Un concurrent tente de voler la base de données clients		
La CNIL sanctionne le laboratoire pour non-conformité RGPD		

Étape 3 – Scénarios CIA et mesures (3 points)

Associer chaque scénario au(x) pilier(s) compromis et proposer **UNE mesure de protection** prioritaire.

N°	Scénario	Pilier(s) compromis	Mesure prioritaire
1	Employé mécontent exfiltre des résultats d'analyses sensibles		
2	Attaque par force brute sur le portail web des résultats patients		
3	Les sauvegardes sont hors service depuis 1 mois suite à une panne		

Étape 4 – Calcul du risque (3 points)

Vous ne traiterez que **3 risques** parmi la liste suivante :

- Injection SQL sur le formulaire de connexion du portail patients
- Absence de formation anti-phishing pour les employés
- Serveur hébergeant les données patients sans chiffrement
- Pas de contrôle d'accès physique à la salle serveurs (libre accès)
- Utilisation d'un logiciel médical dont la licence a expiré

Pour chaque risque choisi :

1. Évaluer la **vraisemblance** (1-5) et l'**impact** (1-5) en justifiant chaque note.
2. Calculer **Risque = Vraisemblance × Impact**.
3. Classer vos 3 risques du plus critique au moins critique.
4. Pour le risque le plus critique, proposer **2 mesures de protection** concrètes.