

Devoir Surveillé – BTS SIO 2e année (B3)

Introduction à la cybersécurité

Durée totale : 2 heures

Partie 1 – Questions de cours (12 points)

Partie 2 – Étude de cas et analyse de risque (28 points)

La justification, la rigueur, la rédaction et le soin de la copie entrent dans la notation sur 2 points. Un manquement de ces 4 critères entraîne une perte de 2 points.

Partie 1 – Révision de cours (12 points)

Système d'Information et actifs (2 points)

1. Définir un **Système d'Information (SI)** et donner 3 exemples d'actifs.
2. Citer **5 catégories d'actifs** et donner un exemple pour chacune.
3. Expliquer la notion de **criticité** d'un actif et donner 3 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
Ransomware chiffre les serveurs de fichiers		
Interception de mots de passe en transit		
Modification non autorisée des prix en base		
Panne électrique longue durée		

Menace, vulnérabilité, incident, risque (2 points)

1. Donner une **définition** courte de chacun des termes.
2. Classer les situations ci-dessous et justifier:
 - a) Serveur web non patché depuis 6 mois
 - b) Groupe de cybercriminels ciblant le secteur
 - c) Compromission réussie d'un poste par phishing
 - d) Probabilité élevée d'attaque avec impact majeur

Mesures de sécurité (2 points)

1. Proposer 3 **mesures techniques** contre le phishing.
2. Proposer 3 **mesures humaines** pour réduire les risques internes.
3. Proposer 3 **mesures physiques** pour améliorer la sécurité.

Propriétés complémentaires de sécurité (1 point)

1. Citer et définir 2 propriétés complémentaires parmi: **Traçabilité (Auditabilité), Non-répudiation, Authenticité, Preuve.**

Typologie des menaces – classification rapide (1 point)

Classer chaque élément dans la catégorie appropriée (Humaine intentionnelle / Humaine non intentionnelle / Technique / Environnementale / Légale) et justifier en une phrase:

- Employé qui envoie par erreur un document confidentiel à un mauvais destinataire
- Groupe de hacker ciblant un secteur industriel
- Inondation dans la salle serveurs
- CNIL constate une non-conformité RGPD
- Ransomware via phishing
- Configuration par défaut exposée sur une base de données
- Tremblement de terre impactant le datacenter
- Utilisation d'un logiciel sans licence

QCM – notions rapides (2 points)

Donner la bonne réponse et justifier en une phrase:

1. La disponibilité protège contre: (A) divulgation, (B) interruption de service, (C) altération de données
2. Un ransomware compromet d'abord: (A) intégrité, (B) confidentialité, (C) disponibilité
3. Un log centralisé sert principalement à: (A) chiffrement, (B) traçabilité, (C) DDoS
4. La non-répudiation est garantie par: (A) signature numérique, (B) pare-feu, (C) antivirus
5. Une configuration par défaut exposée est une: (A) menace, (B) vulnérabilité, (C) incident

Partie 2 – Étude de cas (28 points)

Contexte

« PetitCommerce » est une boutique en ligne (10 personnes). Le site web (PHP/MySQL) représente 95% du chiffre d'affaires. Vous réalisez une **analyse de risque** sur le périmètre du service e-commerce.

Étape 0 – Définitions appliquées (4 points)

1. Dans le **contexte de PetitCommerce**, donner une définition concise, contextualisée avec un exemple de :
 - a) Menace
 - b) Vulnérabilité
 - c) Incident
 - d) Risque

Étape 1 – Actifs et criticité (4 points)

1. Lister 5 actifs de la société **PetitCommerce** et les **classer par catégorie**.
2. Donner une **criticité** (faible/moyenne/elevée/critique) pour ces actifs et **justifier** les 3 plus élevés.

Étape 2 – Triade CIA et scénarios (4 points)

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

N°	Scénario	Pilier(s) compromis	Mesure prioritaire
1	Phishing sur comptable, vol d'identifiants		
2	DDoS sur le site e-commerce		
3	Injection SQL sur formulaire de login		
4	Sauvegardes hors service pendant 3 semaines		
5	Employé mécontent exfiltre des données		

Étape 3 – Menaces, vulnérabilités, incidents, risques (4 points)

Associer à chaque élément de la liste ci-dessous une catégorie (menace, vulnérabilité, incident, risque) et justifier.

Élément	Catégorie	Justification
Version obsolète d'Apache		
Absence de MFA sur VPN		
Groupe APT ciblant le secteur		
Chiffrement réussi de la base clients		
Probabilité élevée de fuite de données sensibles		

Étape 4 – Calcul du risque et matrice (4 points)

- Fuite de données clients via injection SQL sur formulaire de login
- Partage d'un mot de passe administrateur au sein de l'équipe
- Base de données exposée par mauvaise configuration réseau
- Dégâts des eaux dans la salle serveurs
- Non-conformité RGPD (registre absent / notification tardive)
- Sauvegardes non testées, restauration impossible
- Envoi par erreur d'un fichier CSV clients à un destinataire externe
- Utilisation d'un logiciel sans licence (risque d'interruption / sanctions)

Vous ne choisirez que 5 risques de votre choix :

1. Utiliser l'échelle 1–5 pour la **vraisemblance** et l'**impact** en justifiant chacune des valeurs.
2. Calculer **Risque = Vraisemblance × Impact**. Classer 5 risques et identifier le **Top 3**.
3. Pour chaque risque, donner une mesure de protection qui pourrait réduire le risque.

Étape 5 – Enjeux et impacts détaillés (4 points)

Pour chacun des incidents ci-dessous, détailler les **impacts financiers, opérationnels, juridiques, réputationnels, humains** (au moins 2 points par catégorie):

- Ransomware sur serveurs de fichiers
- Fuite de données clients (base e-commerce)
- DDoS rendant le site indisponible 48h

Étape 6 – Attaques courantes (phishing, DDoS, injection SQL) (4 points)

Pour chaque attaque:

1. Décrire brièvement « comment ça fonctionne » (4 étapes).
2. Indiquer le(s) pilier(s) CIA principalement compromis.
3. Donner 2 exemples de **vulnérabilités** typiques qui facilitent l'attaque.