

Correction DS Cybersecurité - BTS SIO B3

Question	Correction Attendue	Barème Indicatif
Critères Généraux	Justification, rigueur, rédaction, soin.	2 pts (Bonus/ Malus)
PARTIE 1	RÉVISION DE COURS	12 pts Total
1.1 SI et Actifs	SI : Ensemble organisé de ressources (matériel, logiciel, personnel, données) permettant d'acquérir, traiter, stocker, communiquer des informations. Exemples : Serveur BDD, Fichier client, Routeur, PC Portable RH.	1 pt
1.2 Catégories	1. Matériel (Serveur) 2. Logiciel (OS, ERP) 3. Données (Fichier client) 4. Humain (Administrateur) 5. Environnement (Salle serveur).	0.5 pt
1.3 Criticité	Importance d'un actif pour l'organisation. Critères : Impact financier, Image de marque, Juridique/Réglementaire, Opérationnel.	0.5 pt
2.1 CIA	Confidentialité : Accès limité aux personnes autorisées. Intégrité : Données exactes et non altérées. Disponibilité : Service accessible au moment voulu.	1 pt
2.2 Scénarios CIA	1. Ransomware -> D (Disponibilité) (+ I/C possible) 2. Interception MDP -> C (Confidentialité) 3. Modif prix -> I (Intégrité) 4. Panne élec -> D (Disponibilité)	1 pt
3.1 Définitions	Menace : Cause potentielle d'incident (ex: hacker). Vulnérabilité : Faiblesse du système (ex: faille logicielle). Incident : Événement indésirable concret. Risque : Probabilité qu'une menace exploite une vulnérabilité (Couple Proba/Impact).	1 pt
3.2 Classification	a) Vulnérabilité (Faille) b) Menace (Source) c) Incident (Réalisé) d) Risque (Projection)	1 pt
4.1 Mesures Tech	Antispam, SPF/DKIM/DMARC, Filtrage URL, Désactivation macros.	0.5 pt
4.2 Mesures Humaines	Sensibilisation/Formation, Charte informatique, Gestion des droits (moindre privilège).	0.5 pt
4.3 Mesures Physiques	Badge d'accès, Caméras, Verrouillage salle serveur, Extincteurs.	1 pt

Question	Correction Attendue	Barème Indicatif
5.1 Propriétés Compl.	Traçabilité : Capacité à retrouver l'historique (Logs). Non-réputation : Impossible de nier une action (Signature). Authenticité : Garantie de l'origine (Source sûre). Preuve : Élément juridique recevable.	1 pt
6. Typologie	1. Humaine non intentionnelle (Erreur) 2. Humaine intentionnelle (Attaque) 3. Environnementale (Inondation) 4. Légale (CNIL) 5. Technique/Humaine int. (Ransomware) 6. Technique (Config) 7. Environnementale (Séisme) 8. Légale (Licence)	1 pt
7. QCM	1. (B) Interruption 2. (C) Disponibilité (accès bloqué) 3. (B) Traçabilité 4. (A) Signature num. 5. (B) Vulnérabilité	2 pts
PARTIE 2	ÉTUDE DE CAS (PetitCommerce)	28 pts Total
Etape 0 - Défs	a) Menace : Concurrent malveillant, Hacker. b) Vulnérabilité : Site PHP non mis à jour. c) Incident : Site hors ligne le jour des soldes. d) Risque : Perte de CA suite à DDoS.	4 pts
Etape 1 - Actifs	Liste cohérente (Site Web, Base Clients, Serveur, Admin, Local). Classement correct (Log, Donnée, Mat, Hum, Env). Criticité justifiée (ex: Site Web = Critique car 95% CA).	4 pts
Etape 2 - Scénarios	1. Phishing -> C/I -> MFA / Formation. 2. DDoS -> D -> Pare-feu WAF / Anti-DDoS. 3. Injection SQL -> C/I -> Requêtes préparées / Input validation. 4. Sauvegardes HS -> D -> Test restauration / 3-2-1. 5. Employé mécontent -> C/I/D -> Gestion droits / Désactivation compte départ.	4 pts
Etape 3 - Catégories	1. Version obsolète -> Vulnérabilité (Faiblesse) 2. Absence MFA -> Vulnérabilité (Faiblesse) 3. Groupe APT -> Menace (Source) 4. Chiffrement réussi -> Incident (Réalisé) 5. Proba élevée... -> Risque (Projection)	4 pts
Etape 4 - Matrice	1. Justification cohérente des scores (1-5). 2. Calcul correct ($P \times I$).	4 pts

Question	Correction Attendue	Barème Indicatif
	<p>3. Top 3 logique (ex: Injection SQL base client > Licence).</p> <p>4. Mesures pertinentes proposées.</p>	
Etape 5 - Impacts	<p>Analyse complète pour chaque incident :</p> <ul style="list-style-type: none"> - Financier (Perte CA, Rançon) - Opérationnel (Arrêt activité) - Juridique (RGPD, amendes) - Réputation (Perte confiance) - Humain (Stress, Licenciement) 	4 pts
Etape 6 - Attaques	<p>Phishing : Email piégé -> Clic -> Site faux -> Vol ID (C). Vuln: Pas de MFA, Humain non formé.</p> <p>DDoS : Botnet -> Saturation requêtes -> Serveur KO (D). Vuln: Pas d'anti-DDoS, Bande passante faible.</p> <p>SQLi : Champ input -> Code SQL malveillant -> Exécution BDD -> Vol données (C/I). Vuln: Pas de requêtes préparées, Input non assaini.</p>	4 pts