CORRIGÉ NON OFFICIEL

BTS Services Informatiques aux Organisations

E6 - Cybersécurité des services informatiques (spécifique à l'option)

Session 2026

Proposition de corrigé rédigée par FormaV pour s'entraîner. Ce n'est pas le corrigé officiel de l'examen et elle ne remplace pas les éléments de correction officiels.

Ce document a été mis en ligne par l'organisme FormaV®.

Toute reproduction, représentation ou diffusion, même partielle, sans autorisation préalable, est strictement interdite.

Pour consulter tous nos sujets d'annales et corrigés du BTS SIO, veuillez visiter :
coursbtssio.fr/annales-sujets-et-corriges

BTS Services informatiques aux organisations – Option A : Solutions d'infrastructure, systèmes et réseaux

Session 2026

U7 – Cybersécurité des services informatiques

PROPOSITION DE CORRIGÉ

Proposition de corrigé établie par FormaV à partir du sujet, non officielle. Elle ne préjuge pas des consignes nationales de correction données aux jurys.

DOSSIER A – INTÉGRATION DU SITE DISTANT « LE BON FROMAGER » 30 points

Mission A1 – Mise en conformité de l'infrastructure informatique « Le Bon Fromager »

Question A1.1

Indiquer pourquoi la mise en place de réseaux locaux virtuels est essentielle mais insuffisante pour une bonne sécurisation du réseau.

La mise en place de VLAN est essentielle car elle segmente logiquement un réseau aujourd'hui non segmenté. Elle permet d'isoler les flux selon leur nature (production, DMZ publique, DMZ privée sauvegarde, DMZ privée RADIUS, sur le modèle de l'infrastructure du siège, document 2), de limiter la propagation d'un logiciel malveillant ou d'un attaquant d'un segment à l'autre, de réduire la surface d'attaque et d'appliquer des règles de filtrage différenciées selon les segments.

Elle reste toutefois insuffisante. Un VLAN n'est pas une barrière de sécurité en soi : le trafic entre VLAN doit transiter par un routeur ou un pare-feu, et sans règles de filtrage précises (listes de contrôle d'accès, pare-feu), les segments communiquent librement. Les VLAN ne protègent pas contre une attaque menée au sein d'un même segment (usurpation ARP, écoute du trafic en clair). Ils n'assurent ni la confidentialité ni l'intégrité des données transportées, qui nécessitent un chiffrement, comme celui du VPN prévu. Une configuration défaillante des ports (VLAN natif, port trunk mal maîtrisé) peut enfin permettre de contourner la segmentation (VLAN hopping). Une sécurisation efficace combine donc les VLAN avec un filtrage inter-VLAN, l'authentification des équipements (norme IEEE 802.1X), la désactivation des ports inutilisés et une supervision.

Mission A2 – Mise à jour de la solution de supervision

Question A2.1

Proposer et justifier au moins trois indicateurs que l'on devrait surveiller si on se concentre uniquement sur le routeur de l'entreprise « Le Bon Fromager », pièce maîtresse du lien établi avec le siège.

1. **Taux d'utilisation de la bande passante du lien** (débit entrant et sortant) : il permet de détecter la saturation du lien VPN avec le siège et les pics de trafic anormaux, qui peuvent révéler une exfiltration de données ou une attaque par déni de service.
2. **Disponibilité du routeur, état des interfaces (UP/DOWN) et des tunnels VPN** : ce routeur est le point de passage unique entre le site et le siège ; sa panne ou la chute du tunnel isole le site.
3. **Charge processeur et mémoire du routeur** : une charge anormale peut révéler une attaque ou un sous-dimensionnement de l'équipement lorsque l'inspection des flux est activée.
4. **Nombre de sessions simultanées (table d'états)** : une valeur anormalement élevée signale une tentative de saturation ou un balayage réseau.

5. **Latence, gigue et perte de paquets sur le lien VPN** : ces indicateurs conditionnent la qualité des échanges applicatifs avec le siège.
6. **Nombre d'alertes et de paquets rejetés par les règles de filtrage** : il mesure le niveau des tentatives d'intrusion ciblant le site et l'efficacité de la politique de sécurité.

Mission A3 – Application de la charte

Question A3.1

a) Expliquer l'intérêt pour une entreprise comme NELAIT de disposer d'une charte informatique. Vous illustrerez avec des exemples.
b) Préciser à quelle(s) condition(s) et par quels moyens cette charte est applicable aux salariés de l'entreprise NELAIT.

a) La charte informatique fixe les règles d'usage des ressources informatiques et des services internet. Elle présente plusieurs intérêts pour une entreprise comme NELAIT, qui traite des données essentielles à son activité et compte désormais des salariés issus d'une entreprise rachetée. Elle responsabilise les utilisateurs, prévient les risques de sécurité (virus, fuite de données, usage détourné des ressources), fixe un cadre juridique aux contrôles de l'utilisation des ressources et aux sanctions, et contribue à la conformité avec le RGPD. Exemples tirés du document A1 : interdiction de connecter un équipement privé au réseau sans autorisation du directeur des systèmes d'information (point 2) ; obligation d'appliquer les recommandations de sécurité et de se conformer aux dispositifs de lutte contre les virus (point 3) ; interdiction de se connecter à un serveur autrement que par les dispositions prévues (point 4) ; présomption de caractère professionnel des messages, sauf mention particulière dans l'objet ou stockage dans un espace privé (point 4) ; avertissements, limitations ou sanctions disciplinaires en cas de manquement (point 6).

b) Pour être opposable, la charte doit être acceptée par les utilisateurs, par signature ou par une annexe au contrat de travail (document A2). Pour éviter tout refus ou toute renégociation du contrat, elle peut être annexée au règlement intérieur ; cette procédure suppose la consultation des instances représentatives du personnel lorsqu'elles existent et la communication à l'inspection du travail. Dans tous les cas, la charte doit être portée à la connaissance des utilisateurs, par une notification individuelle (remise en main propre, message électronique) ou par affichage ou diffusion sur l'intranet. À défaut, les sanctions prises contre un utilisateur qui n'en avait pas connaissance pourraient être annulées par les juges. Les salariés issus de « Le Bon Fromager » doivent donc recevoir cette notification lors de leur intégration.

Mission A4 – Audit du service d'annuaire Active Directory

Question A4.1

Expliquer en quoi consiste un audit de sécurité du réseau et ses objectifs.

Un audit de sécurité du réseau est une évaluation méthodique et documentée du système d'information, réalisée à l'aide d'outils techniques (scans, analyse de configuration, outils comme PingCastle) et d'entretiens, afin de mesurer le niveau de sécurité de l'infrastructure par rapport à des référentiels et bonnes pratiques.

Ses objectifs sont : identifier les vulnérabilités, les erreurs de configuration et les comptes à risque ; évaluer les risques et leur niveau de criticité ; vérifier la conformité aux obligations (RGPD, charte informatique, réglementation) ; proposer un plan d'actions correctives priorisé ; établir un état de référence permettant un suivi dans le temps et une amélioration continue.

Question A4.2

Donner trois éléments permettant d'améliorer le score PingCastle et donc la sécurité de l'annuaire AD, en justifiant pour chacun en quoi cela est bénéfique pour la sécurité.

Le score PingCastle est un indicateur de sécurité d'autant plus favorable qu'il se rapproche de 0. Le score « Objets obsolètes » est à 100/100, avec dix règles déclenchées (document A3). Trois actions permettent de le réduire :

1. **Retirer ou migrer les systèmes obsolètes** : présence de 3 machines sous Windows 2003 (+20 points), de 18 machines sous Windows 2008 (+15 points) et de 490 postes sous Windows 7 (+5 points). Ces systèmes ne reçoivent plus de correctifs de sécurité ; leur remplacement réduit la surface d'attaque de l'annuaire et supprime des failles non corrigeables.
2. **Supprimer les mots de passe vides et désactiver le chiffrement DES** : six comptes peuvent avoir un mot de passe vide et onze comptes utilisent DES. Imposer une politique de mots de passe robustes (longueur, complexité, interdiction des mots vides) et désactiver DES, au profit de chiffrements modernes (AES) pour Kerberos, empêche l'accès frauduleux aux comptes et le craquage des authentifications.
3. **Désactiver ou supprimer les comptes et ordinateurs inactifs, et renouveler les mots de passe des machines** : 40 % des comptes utilisateurs et 24 % des comptes ordinateurs sont inactifs, et sept ordinateurs n'ont pas changé de mot de passe depuis trois mois. Les comptes inactifs constituent des identifiants exploitables par un attaquant sans être surveillés ; leur suppression réduit ce risque et améliore la gestion des identités.

Les catégories « Comptes privilégiés » (21/100) et « Anomalies » (33/100) devront ensuite être analysées règle par règle pour poursuivre l'amélioration du score.

Question A4.3

Indiquer en quoi l'outil PingCastle respecte les obligations en matière de collecte et de traitement de données à caractère personnel.

PingCastle répond aux principes du RGPD (article 5) et aux exigences de sécurité du traitement (article 32) pour les raisons suivantes, selon le document A3 (questions fréquemment posées) :

- **Minimisation des données** : l'outil essaie de limiter la quantité de données collectées. Les seules données à caractère personnel concernées sont le nom du compte administrateur, l'heure de création du compte et l'heure de la dernière connexion, contenues dans le rapport lisible par l'homme.
- **Maîtrise du traitement par l'entreprise** : l'outil est décentralisé, de sorte que l'entreprise reste responsable du traitement et sous-traitante de ses propres données ; l'outil ne collecte aucune autre information que celles du rapport et ne nécessite pas de connexion internet, sauf pour vérifier la signature.
- **Confidentialité et sécurité** : le rapport peut être chiffré avec une clé RSA, de sorte que seule l'instance détenant la clé privée peut le traiter, ce qui sécurise son transfert par courrier électronique ou sur le réseau.
- **Accès limité** : la collecte repose sur des protocoles d'annuaire (LDAP, ADWS, SMB) et sur une autorisation de connexion accordée aux comptes du domaine ; elle est donc soumise aux droits existants.

L'auditeur reste responsable de l'utilisation des données contenues dans le rapport ; la déléguée à la protection des données doit donc veiller à leur diffusion restreinte et à leur durée de conservation.

DOSSIER B – SÛRETÉ DU RÉSEAU DE STOCKAGE (BAIE SAN) 23 points

Mission B1 – Vérification et reconfiguration de la baie SAN

Question B1.1

Analyser la situation actuelle (en justifiant vos réponses) :
a) Calculer la capacité utile disponible actuellement.
b) Indiquer le nombre de disque(s) dur(s) que l'on peut perdre simultanément, par grappe, tout en maintenant la disponibilité des données.
c) Préciser le rôle du disque de rechange (spare) dans l'objectif d'une meilleure disponibilité de données.
d) Justifier le fait que le disque de rechange (spare) soit configuré en mode global à la baie et non dédié à une grappe donnée.

a) La baie compte 11 disques de 2 To. Deux grappes de 5 disques sont configurées en RAID 5, soit 10 disques actifs ; le 11e disque est le disque de rechange (spare) et n'apporte pas de capacité utile. En RAID 5, la capacité utile d'une grappe vaut (n – 1) × capacité unitaire, soit (5 – 1) × 2 To = 8 To. Pour les deux grappes : 2 × 8 To = **16 To de capacité utile**.

b) Le RAID 5 tolère la perte d'un seul disque par grappe. Une seconde panne dans la même grappe entraîne la perte des données de cette grappe.

c) Le disque de rechange est immédiatement utilisé pour reconstruire la grappe dès qu'un disque tombe en panne. Il réduit ainsi la durée pendant laquelle la grappe fonctionne en mode dégradé, donc la fenêtre de risque avant une seconde panne, et améliore la disponibilité des données.

d) Un spare global est mutualisé entre les deux grappes : il peut être utilisé pour reconstruire l'une ou l'autre grappe, ce qui est nécessaire puisque la panne peut survenir sur n'importe laquelle. Un spare dédié à une grappe resterait inutilisé pour l'autre et laisserait cette dernière sans protection de reconstruction. Le spare global optimise donc l'usage du matériel et la couverture des pannes.

Question B1.2

Analyser la proposition d'évolution de la baie (en justifiant vos réponses) :
a) Calculer la future capacité utile totale disponible avec la configuration proposée.
b) Indiquer le nombre de disque(s) dur(s) que l'on peut perdre simultanément, par grappe, tout en maintenant la disponibilité des données.
c) Indiquer si la nouvelle configuration permet d'atteindre les objectifs prévus : meilleures performances, meilleure disponibilité, augmentation de la capacité disque utile.

a) La proposition utilise les 24 emplacements de la baie (document B1) :

Élément	Positions	Nombre et type de disques	Niveau RAID	Calcul	Capacité utile
Grappe HDD 1	1 à 7	7 disques HDD SAS de 2 To	RAID 6	(7 – 2) × 2 To	10 To
Grappe HDD 2	8 à 14	7 disques HDD SAS de 2 To	RAID 6	(7 – 2) × 2 To	10 To
Grappe SSD 1	16 à 19	4 disques SSD SAS de 1 To	RAID 6	(4 – 2) × 1 To	2 To
Grappe SSD 2	20 à 23	4 disques SSD SAS de 1 To	RAID 6	(4 – 2) × 1 To	2 To
Spare HDD	15	1 disque HDD SAS de 2 To	–	non compté	0 To
Spare SSD	24	1 disque SSD SAS de 1 To	–	non compté	0 To
Capacité utile totale (Auto-Tiering)					**24 To**

La capacité utile totale est donc de 24 To. Par rapport aux 16 To actuels, le gain est de 8 To, soit une augmentation de 50 %, conforme au besoin exprimé. La part des SSD dans la capacité utile est de 4/24, soit environ 16,7 %, ce qui respecte la fourchette de 10 à 20 % préconisée par l'ESN.

b) Le RAID 6 tolère la perte simultanée de deux disques par grappe, sans interruption d'accès ni perte de données.

c) Objectif capacité : atteint (24 To contre 16 To). Objectif disponibilité : atteint, car le RAID 6 tolère deux pannes par grappe contre une en RAID 5, et chaque technologie dispose de son propre spare. Objectif performances : partiellement atteint. Les deux contrôleurs fonctionnent en parallèle grâce aux quatre grappes, et la technologie Auto-Tiering place les données les plus sollicitées sur les SSD. En revanche, la double parité du RAID 6 pénalise les écritures (document B3), ce qui limite le gain de performance pour les charges d'écriture intensives. La proposition atteint donc les objectifs de capacité et de disponibilité ; les performances sont globalement améliorées (lecture, données actives sur SSD, deux contrôleurs actifs), avec une réserve pour les charges d'écriture intensives.

Question B1.3

Indiquer l'impact éventuel du temps de reconstruction sur la disponibilité des données.

Le temps de reconstruction constaté est d'environ 12 heures (document B1). Pendant cette durée, la grappe fonctionne en mode dégradé : les accès peuvent être ralentis, et toute panne supplémentaire dans la même grappe augmente le risque de perte de données. Plus la reconstruction est longue, plus cette fenêtre de risque est importante, d'autant que la durée de reconstruction croît avec la capacité des disques.

Le RAID 6 limite ce risque, puisqu'une grappe peut supporter une seconde panne pendant la reconstruction, alors que le RAID 5 ne le permet pas. La présence d'un spare disponible permet de démarrer la reconstruction immédiatement, sans attendre le remplacement physique du disque, ce qui réduit la durée de la fenêtre de risque. Enfin, un temps de reconstruction élevé allonge la période pendant laquelle la disponibilité des données n'est plus totalement garantie et peut dégrader les performances des serveurs virtualisés du cluster qui s'appuient sur cette grappe.

Mission B2 – Utiliser l'interface d'administration iLO pour l'administration à distance

Question B2.1

Indiquer quelles peuvent être les atouts d'un outil comme iLO dans les domaines suivants :
- cybersécurité dans le cadre de la surveillance des équipements,
- maintenance des serveurs,
- intervention en cas d'incident sur un serveur physique.

Cybersécurité et surveillance des équipements : iLO assure une surveillance en temps réel des paramètres matériels (température, tension, processeur, mémoire) et envoie des alertes en cas d'anomalie (document B4, point 2). L'interface intègre des fonctionnalités de sécurité avancées : authentification à deux facteurs, chiffrement SSL/TLS et autorisations d'accès basées sur les rôles (point 6). L'enregistrement vidéo des sessions de console à distance (point 7) assure la traçabilité des interventions et permet l'audit. Contrairement à vSphere, au bureau à distance ou à SSH, qui dépendent du système d'exploitation ou de l'hyperviseur, iLO reste accessible même si le système est compromis ou en panne, ce qui en fait un canal d'administration indépendant.

Maintenance des serveurs : iLO permet la mise à jour du micrologiciel (firmware) à distance, la gestion des licences depuis une interface centralisée et la surveillance de la consommation d'énergie pour optimiser l'utilisation des serveurs (points 1, 5 et 8). Ces opérations peuvent être planifiées et

réalisées sans déplacement, dans les fenêtres de maintenance, y compris sur des serveurs situés hors du réseau local.

Intervention en cas d'incident sur un serveur physique : l'administrateur peut redémarrer ou réinitialiser le serveur à distance, accéder à sa console graphique (redirection graphique à distance, point 5), réinstaller un système d'exploitation à distance et diagnostiquer le problème matériel avant tout déplacement (points 3 et 4). Le gain est particulièrement net par rapport aux outils classiques : vSphere ne permet pas d'agir sur un serveur dont l'hyperviseur est hors service, le bureau à distance et SSH nécessitent un système d'exploitation fonctionnel.

DOSSIER C – ANALYSE DES VULNÉRABILITÉS — 27 points

Mission C1 – Étude d'opportunité de la solution IKare

Question C1.1

a) Expliquer l'intérêt de posséder le service IKare dans l'infrastructure du groupe NELAIT, en justifiant sa valeur ajoutée par rapport aux services réseaux existants (GLPI, Centreon et WSUS).
b) Indiquer au moins deux caractéristiques essentielles du produit IKare en ce qui concerne le respect des données à caractère personnel.

a) GLPI gère les tickets et l'inventaire, Centreon supervise la disponibilité et les performances, et WSUS diffuse les mises à jour Microsoft. Aucun de ces services ne recherche de manière systématique les vulnérabilités de l'ensemble du réseau. WSUS ne traite que les correctifs Microsoft, et ne couvre ni les équipements réseau, ni les logiciels tiers comme Adobe Flash Player ou VMware Tools. IKare apporte donc une valeur ajoutée : découverte automatique du réseau, détection des ports ouverts, des services, des mots de passe par défaut et des clés de chiffrement faibles (document C2), évaluation des vulnérabilités selon le référentiel CVSS et classement par criticité, analyses récurrentes et quasi temps réel, rapports adaptés à chaque niveau de l'entreprise. Il est complémentaire : IKare identifie les failles, GLPI permet de les tracer en tickets, WSUS applique les correctifs Microsoft, et Centreon supervise les effets sur la disponibilité.

b) Deux caractéristiques d'IKare utiles au respect du RGPD, d'après les documents : le produit est présenté comme « labellisé et souverain » et « Made in France » (document C2) : il s'agit d'un éditeur français, ce qui permet de penser que les données analysées restent soumises au droit européen et sous la maîtrise de l'entreprise ; les tableaux de bord et rapports sont adaptés à chaque strate de l'entreprise, chacun n'accédant qu'au niveau de détail qui le concerne, ce qui correspond à la limitation des accès selon le besoin d'en connaître (confidentialité, article 32 du RGPD). Le produit permet en outre de suivre la conformité au RGPD, notamment l'exigence de surveillance des vulnérabilités, et de créer des groupes virtuels selon les contraintes de conformité.

Mission C2 – Analyse des vulnérabilités critiques et moyennes remontées par l'outil IKare

Question C2.1

a) Expliquer pourquoi le fait qu'une faille ne possédant pas encore de code d'exploitation justifie une note CVSS moyenne et non très élevée. Vous préciserez la métrique qui la prend en compte.
b) Déduire de l'identifiant CVE de la vulnérabilité 2 nommée « Vulnérabilités multiples Microsoft Windows (KB4558998) » votre étonnement. Justifier votre réaction.
c) Expliquer l'intérêt de prendre contact avec le responsable du service WSUS de NELAIT, suite à l'étude de cette vulnérabilité 2, avant de demander la mise en œuvre d'une solution pour y remédier.

a) Le score CVSS comporte trois métriques : la métrique de base, immuable, fondée sur les

caractéristiques intrinsèques de la vulnérabilité, la métrique temporelle, qui évolue au fil du temps, et la métrique environnementale, propre à chaque système (document C3). C'est la **métrique temporelle** qui prend en compte la maturité des codes d'exploitation : elle varie à mesure que les exploits sont développés, divulgués et automatisés, ainsi que la disponibilité des correctifs. Une faille sans code d'exploitation connu présente un risque immédiat moindre, ce qui abaisse le score global, qui reste donc moyen. Ce score doit toutefois être réévalué si un exploit apparaît.

b) Les identifiants CVE associés à la vulnérabilité 2 (CVE-2020-1350 dite SIGRed, CVE-2020-1085, CVE-2020-1463, CVE-2020-1468, document C5) sont tous de la forme CVE-2020-NNNN (document C4). L'année 2020 indique que la faille a été publiée en 2020, soit plusieurs années avant l'analyse. Il est donc étonnant qu'une faille aussi ancienne soit encore présente sur un contrôleur de domaine et serveur DNS critique : or le fournisseur a publié un correctif (solution « FournisseurFix », document C5) et NELAIT dispose d'un serveur WSUS chargé de diffuser les mises à jour Microsoft : le correctif KB4558998 n'a donc pas été approuvé ou pas été déployé sur ce serveur, ce qui révèle une défaillance de la gestion des correctifs. Ce constat est aggravé par la référence au catalogue des vulnérabilités exploitées de la CISA, qui indique une exploitation avérée.

c) Le responsable WSUS connaît l'état d'approbation et de déploiement des mises à jour Microsoft (ici le bulletin KB4558998) ; il peut vérifier si le correctif est déjà approuvé ou en attente, si le serveur AD figure dans un groupe de mise à jour, et identifier une éventuelle erreur de déploiement. Il peut aussi tester la compatibilité du correctif sur un contrôleur de domaine, fixer une fenêtre de maintenance et éviter les interruptions du service d'annuaire. Ce contact permet d'éviter une demande de mise en œuvre redondante ou non maîtrisée.

Le RSSI vous demande d'intervenir en priorité sur la vulnérabilité 1 (critique) liée au serveur web www.nelait.fr (192.168.30.1).

Question C2.2

a) Expliquer en quoi la résolution de cette faille est prioritaire pour votre RSSI. Vous donnerez au moins deux raisons.
b) Indiquer votre préconisation, en précisant les différentes phases à prévoir, pour répondre à cette faille.

a) La résolution est prioritaire pour deux raisons principales. D'une part, le serveur est situé dans la DMZ publique (192.168.30.0/24, document 2) et est donc directement accessible depuis Internet : toute faille y est exposée à un attaquant extérieur. D'autre part, Adobe Flash Player a atteint sa fin de vie le 31 décembre 2020 ; le fournisseur ne publie plus de mise à jour de sécurité, la solution proposée est « WillNotFix » (document C5). Les failles présentes restent donc non corrigées et peuvent être exploitées pour compromettre l'hôte. La criticité, signalée par l'outil IKare, confirme cette priorité.

b) Préconisation : Flash Player ne doit pas être mis à niveau, il doit être supprimé, comme le recommandent les options générales de l'outil (désinstallation du produit ou remplacement par une technologie maintenue).

1. **Diagnostic** : vérifier la présence de Flash Player sur le serveur (chemin C:\Windows\SysWOW64 indiqué par l'analyse), identifier les sites ou applications qui l'utilisent, et inventorier l'ensemble des postes et serveurs concernés dans GLPI.
2. **Analyse d'impact et sauvegarde** : vérifier qu'aucun contenu du site www.nelait.fr ne dépend de Flash, prévoir de remplacer les contenus éventuels par des technologies actuelles (HTML5), et réaliser une sauvegarde complète du serveur web avant toute modification.
3. **Test** : désinstaller Flash Player sur un environnement de préproduction ou une maquette, puis contrôler le bon fonctionnement du site et des applications.

4. **Mise en production** : planifier l'intervention dans une fenêtre de maintenance, informer les services concernés, désinstaller Flash Player sur le serveur de production et bloquer son exécution dans les navigateurs par une stratégie de groupe.
5. **Vérification** : relancer une analyse IKare pour confirmer la disparition de la vulnérabilité, puis fermer le ticket dans GLPI avec la documentation de l'intervention.
6. **Suivi** : maintenir une surveillance continue du serveur via Centreon et les analyses récurrentes d'IKare, et vérifier que les autres logiciels en fin de vie ne sont pas présents sur le parc.

BARÈME — 80 points

Dossier	Intitulé	Points
Dossier A	Intégration du site distant « Le Bon Fromager »	30
Dossier B	Sûreté du réseau de stockage (baie SAN)	23
Dossier C	Analyse des vulnérabilités	27
Total		**80**

Continue à t'entraîner

Retrouve tous les sujets et corrigés du BTS SIO, classés par épreuve et par année :
coursbtssio.fr/annales-sujets-et-corriges

Pour réviser tout le programme avant l'examen, les Fiches de Révision du BTS SIO reprennent l'essentiel de chaque épreuve :
coursbtssio.fr/fiches-de-revision

Copyright © 2027 FormaV®. Tous droits réservés.

FormaV® est une marque déposée auprès de l'INPI sous le numéro 5227897.

Ce document a été élaboré par FormaV® avec le plus grand soin afin d'accompagner chaque apprenant vers la réussite de ses examens. Son contenu (textes, graphiques, méthodologies, tableaux, exercices, concepts, mises en forme) constitue une œuvre protégée par le droit d'auteur.

Toute copie, partage, reproduction, diffusion ou mise à disposition, même partielle, gratuite ou payante, est strictement interdite sans accord préalable et écrit de FormaV®, conformément aux articles L.111-1 et suivants du Code de la propriété intellectuelle. Dans une logique anti-plagiat, FormaV® se réserve le droit de vérifier toute utilisation illicite, y compris sur les plateformes en ligne ou sites tiers.

En utilisant ce document, vous vous engagez à respecter ces règles et à préserver l'intégrité du travail fourni. La consultation de ce document est strictement personnelle.

Merci de respecter le travail accompli afin de permettre la création continue de ressources pédagogiques fiables et accessibles.