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 en savoir plus sur nos formations disponibles, veuillez visiter :
formav.co/explorer

BUT R&T : compétence C8, parcours cybersécurité

Session 2026 • Code sujet : **26-BUT-RT-C8** • Durée : **2 heures** • Coefficient : **3 (indicatif)**

Sommaire

Cliquez sur une partie pour y accéder directement

1. Comprendre le système d'information et qualifier les enjeux (3 questions) **Page 3**

2. Diagnostiquer et hiérarchiser les risques (3 questions) **Page 5**

3. Proposer un plan de remédiation opérationnel (3 questions) **Page 8**

4. Communiquer et respecter les obligations de sécurité (3 questions) **Page 11**

5. Ce qu'il faut retenir & Questions fréquentes (FAQ) (Synthèse & Q&A Examen) **Page 13**

Sujet officiel (PDF) : https://butrt.fr/assets/annales/but-rt/C8 - Sensibiliser aux vulnérabilités d'un système d'information et aux remédiations possibles/2026/BUT Réseaux et Télécommunications - C8 - Sensibiliser aux vulnérabilités d'un système d'information et aux remédiations possibles - Session 2026 - 1-Sujet.pdf

1. Comprendre le système d’information et qualifier les enjeux

Dans le contexte de la PME Alpina Services Numériques, il faut caractériser les actifs, les données et les conséquences possibles d’une compromission à partir de l’architecture et de l’inventaire fournis. Les journaux signalent notamment une connexion VPN inhabituelle, sans démontrer qu’un incident a eu lieu.

Identification des actifs et des enjeux

Question 1.1. Relevez deux actifs importants du système d’information. Pour chacun, indiquez la donnée ou le service concerné et justifiez son importance au regard de la confidentialité, de l’intégrité ou de la disponibilité.

Actif	Donnée ou service	Enjeu
Serveur applicatif	Application RH et données personnelles des salariés	Confidentialité, intégrité et disponibilité
Serveur de fichiers	Documents commerciaux et administratifs partagés	Confidentialité, intégrité et disponibilité

Une divulgation des données RH porterait atteinte à la confidentialité et à la vie privée des salariés. Une modification ou une perte de ces données compromettrait leur intégrité. Pour le serveur de fichiers, l’indisponibilité des documents partagés pourrait perturber les activités de l’entreprise, tandis qu’une divulgation ou une altération nuirait à leur confidentialité ou à leur fiabilité. Ces deux actifs soutiennent donc des activités essentielles et concentrent des enjeux importants.

> ✓ RÉPONSE À RETENIR
>
> Actifs majeurs : serveur applicatif RH et serveur de fichiers, pour les données sensibles et les services essentiels qu’ils hébergent.

Analyse des événements

Question 1.2. À partir du DT 3, expliquez pourquoi les événements observés constituent un signal d’alerte sans suffire, à eux seuls, à démontrer qu’une compromission a eu lieu. Citez deux vérifications complémentaires à effectuer.

Deux échecs d’authentification suivis d’une connexion réussie au même compte en trois minutes, à une heure où le salarié dit ne pas avoir travaillé, constituent un signal d’alerte. Cela peut toutefois correspondre à une connexion légitime ou à une erreur de saisie. Le dossier ne confirme aucune extraction de données, modification de fichiers ou interruption de service : une compromission n’est donc pas démontrée.

- Confirmer auprès du salarié la légitimité de la connexion, l’appareil utilisé et son contexte.
- Corréler les journaux VPN avec ceux des postes et des accès aux fichiers pour rechercher des actions inhabituelles, en contrôlant aussi la complétude des journaux.

> ✓ RÉPONSE À RETENIR
>
> Signal d’alerte, mais pas preuve de compromission. Vérifier la connexion avec le salarié et corréler les journaux avec les accès aux ressources.

Vocabulaire de sécurité

Question 1.3. Expliquez la différence entre une vulnérabilité et une menace, puis illustrez chaque terme par un élément distinct du dossier.

Une vulnérabilité est une faiblesse du système susceptible d'être exploitée : ici, le serveur de fichiers accepte SMBv1. Une menace est un acteur ou un événement susceptible de provoquer un dommage en exploitant une faiblesse. Le dossier signale des échecs suivis d'une connexion VPN réussie ; un accès non autorisé au compte est donc une menace possible, mais non confirmée. Le risque désigne la possibilité que cette menace exploite une vulnérabilité et entraîne des conséquences. Un incident correspondrait à la réalisation effective de ce scénario, qui n'est pas établie par les éléments fournis.

> ✓ **RÉPONSE À RETENIR**
>
> Vulnérabilité : SMBv1 actif. Menace : accès non autorisé possible au compte VPN, hypothèse non confirmée par les journaux.

2. Diagnostiquer et hiérarchiser les risques

Quatre vulnérabilités sont recensées sur la passerelle VPN, le serveur de fichiers, le réseau Wi-Fi invité et le commutateur cœur. Il faut appliquer la méthode interne de cotation du DT 2, puis comparer les risques sans présenter comme avéré un incident non démontré.

Cotation de V1 et V2

Question 2.1. Pour V1 et V2, déterminez une vraisemblance, un impact et une criticité. Présentez les calculs sous la forme C = V × I en utilisant les échelles du DT 2, puis indiquez la classe de criticité obtenue.

V1 : la passerelle VPN est accessible depuis Internet et l'administration repose uniquement sur un mot de passe. La vraisemblance est très probable (4) ; une prise de contrôle pourrait donner accès aux ressources internes, avec un impact potentiel majeur (4). V2 : SMBv1 est une faiblesse exploitable dans des conditions réalistes (vraisemblance 3). La perte de fichiers pourrait être importante, car aucune sauvegarde immuable ni restauration récemment testée n'est consignée (impact 4).

Selon le DT 2, la criticité est le produit de la vraisemblance par l'impact : V1, 4 × 4 = 16 ; V2, 3 × 4 = 12. Les deux risques sont critiques.

> **✓ RÉPONSE À RETENIR**
>
> V1 : V = 4, I = 4, C = 16, critique. V2 : V = 3, I = 4, C = 12, critique.

Tableau d'analyse des vulnérabilités

Question 2.2. Complétez le tableau du DR 1 pour V1 à V4 : actif, vulnérabilité, scénario de risque, valeurs de vraisemblance et d'impact, criticité et classe. Formulez les scénarios comme des conséquences plausibles, sans présenter comme avéré un incident que le dossier ne démontre pas.

Repère	Actif	Vulnérabilité constatée	Scénario de risque plausible	V	I	C	Classe
V1	Passerelle VPN	Administration distante sans MFA	Prise de contrôle du VPN et accès non autorisé aux ressources internes.	4	4	16	Critique
V2	Serveur de fichiers	SMBv1 actif, sans sauvegarde immuable	Compromission, chiffrement ou perte importante des fichiers partagés.	3	4	12	Critique
V3	Réseau interne	Le Wi-Fi invité peut joindre le réseau des postes	Un visiteur pourrait atteindre des postes et exposer des données internes.	3	3	9	Élevée
V4	Commutateur cœur	SNMPv2 avec communauté par défaut	Un accès à l'interface de gestion pourrait divulguer des informations ou faciliter une perturbation du réseau.	2	3	6	Modérée

Les valeurs suivent les définitions du DT 2 : exposition directe pour V1, faiblesse exploitable dans des conditions réalistes pour V2 et V3, et plusieurs conditions nécessaires pour V4. Les impacts traduisent les conséquences possibles sur les données ou les services. Les constats de configuration et les journaux fournis ne prouvent pas qu'une exploitation a eu lieu.

DR 1 complété : cotation des risques

Repère	Actif	Vulnérabilité constatée	Scénario de risque	V	I	C = V × I	Classe
V1	VPN	Admin sans MFA	Accès ressources	4	4	16	Critique
V2	Fichiers	SMBv1, pas immuable	Perte ou chiffremen	3	4	12	Critique
V3	Réseau interne	Wi-Fi vers postes	Exposition interne	3	3	9	Élevée
V4	Commutateur cœur	SNMPv2, défaut	Divulgation ou pert	2	atio 3	6	Modérée

✓ **RÉPONSE À RETENIR**

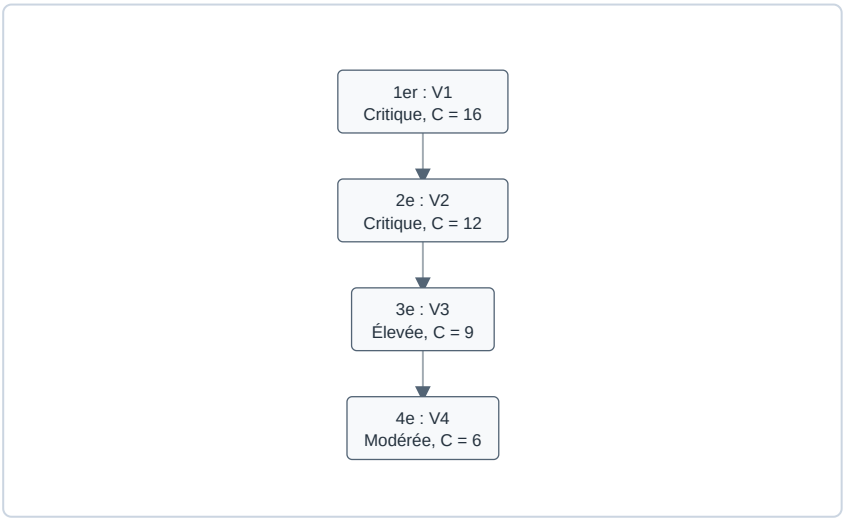
V1 : 16, critique ; V2 : 12, critique ; V3 : 9, élevée ; V4 : 6, modérée.

Ordre de traitement des risques

Question 2.3. Classez les quatre risques par ordre de traitement décroissant en vous appuyant sur leur criticité calculée. En cas d'égalité, appliquez le départage prévu dans le DT 2. Justifiez brièvement le premier et le dernier rang.

Le classement décroissant est V1 (16), V2 (12), V3 (9), puis V4 (6). V1 est premier : la passerelle VPN est accessible depuis Internet et l'absence de MFA facilite une prise de contrôle susceptible d'ouvrir l'accès aux ressources internes. V4 est dernier car sa vraisemblance est évaluée à 2, contre 3 pour V3, ce qui donne une criticité plus faible. Les criticités étant toutes différentes, la règle de départage du DT 2 ne s'applique pas.

Ordre de traitement décroissant



Priorité décroissante selon les criticités calculées avec le DT 2.

✓ RÉPONSE À RETENIR

Ordre décroissant : V1 (16, critique), V2 (12, critique), V3 (9, élevée), puis V4 (6, modérée).

3. Proposer un plan de remédiation opérationnel

Les remédiations doivent être proportionnées aux risques et formulées de façon compréhensible pour un responsable non spécialiste. Le travail porte sur la réduction des vulnérabilités, la limitation des conséquences, la vérification des corrections et la préparation d'un plan de traitement incluant sauvegarde et restauration.

Mesures prioritaires pour V1 et V2

Question 3.1. Proposez une mesure technique prioritaire pour V1 et une pour V2. Pour chaque mesure, indiquez le risque réduit et une précaution de mise en œuvre destinée à limiter les interruptions de service ou les erreurs de configuration.

Risque	Mesure prioritaire	Précaution de mise en œuvre
V1, VPN	Activer l'authentification multifacteur pour l'administration distante.	Tester sur un compte pilote et conserver un accès de secours contrôlé.
V2, fichiers	Désactiver SMBv1 et créer une sauvegarde immuable hors site.	Vérifier la compatibilité des équipements et tester la restauration avant le changement définitif.

La MFA réduit le risque d'accès interne après le vol d'un mot de passe. Désactiver SMBv1 réduit l'exposition du serveur de fichiers ; une copie immuable limite les conséquences d'une attaque ou d'un incident affectant le site. Planifier le changement à une période de faible activité.

> **✓ RÉPONSE À RETENIR**
>
> V1 : activer la MFA. V2 : désactiver SMBv1 et disposer d'une sauvegarde immuable hors site, restaurable.

Remédiations pour V3 et V4

Question 3.2. Proposez une remédiation pour V3 et une pour V4. Pour chacune, indiquez un test simple permettant de vérifier que la correction est effective.

Corriger les règles réseau et sécuriser la supervision :

1. **V3 :** isoler le Wi-Fi invité des sous-réseaux internes, en conservant l'accès à Internet. Test : depuis un appareil invité, vérifier qu'Internet fonctionne et que les postes internes sont injoignables.
2. **V4 :** remplacer SNMPv2 par SNMPv3 avec authentification et chiffrement, et limiter l'accès aux postes d'administration. Test : vérifier que la communauté par défaut est refusée et que la supervision fonctionne en SNMPv3 depuis un poste autorisé.

Ces tests contrôlent le blocage des accès non souhaités et le maintien des usages prévus.

> **✓ RÉPONSE À RETENIR**
>
> V3 : isoler le Wi-Fi invité. V4 : sécuriser et restreindre SNMP. Tester le blocage interne et la supervision autorisée.

Plan de traitement

Question 3.3. Complétez le DR 2 avec un plan comprenant au moins trois actions. Pour chaque action, indiquez une priorité, un responsable fonctionnel choisi parmi les rôles du DT 2, une échéance cohérente avec la criticité et un indicateur de vérification. Faites apparaître une mesure de sauvegarde et de restauration.

Les risques critiques nécessitent une mesure immédiate de réduction et une correction planifiée sous 7 jours ; les risques élevés sont à corriger sous 30 jours. Le tableau prévoit une mesure temporaire pour le VPN et une copie immuable hors site pour les fichiers, puis les corrections définitives. Le responsable systèmes et réseaux peut réaliser les tests techniques.

Risque ou repère	Action de remédiation	Priorité	Responsable fonctionnel	Échéance	Indicateur ou test
V1, VPN	Restreindre provisoirement l'administration distante, puis activer la MFA.	Critique	Administrateur systèmes et réseaux	Mesure immédiate ; correction sous 7 jours	Accès restreint ; connexion MFA testée.
V2, fichiers	Créer une copie immuable hors site, tester sa restauration, puis désactiver SMBv1.	Critique	Administrateur systèmes et réseaux	Mesure immédiate ; correction sous 7 jours	Restauration documentée ; SMBv1 désactivé.
V3, Wi-Fi invité	Bloquer l'accès du réseau invité aux réseaux internes.	Élevée	Administrateur systèmes et réseaux	Sous 30 jours	Ressources internes injoignables depuis le Wi-Fi invité.
V4, commutateur	Passer à SNMPv3 et limiter l'accès aux postes d'administration.	Élevée	Administrateur systèmes et réseaux	Sous 30 jours	Communauté par défaut refusée ; supervision SNMPv3 fonctionnelle.

DR 2 complété : plan d’actions priorisé

V1 VPN	Restreindre accès admin, activer MFA	Critique	Admin systèmes/réseaux	Immédiat, sous 7 j	MFA testée
V2 fichiers	Copie immuable hors site; retirer SMBv1	Critique	Admin systèmes/réseaux	Immédiat, sous 7 j	Restauration testée
V3 invité	Isoler le Wi-Fi invité	Élevée	Admin systèmes/réseaux	Sous 30 j	Accès interne bloqué
V4 commutateur	SNMPv3 + accès restreint	Élevée	Admin systèmes/réseaux	Sous 30 j	Défaut refusé ; test OK

✓ RÉPONSE À RETENIR

V1 et V2 : mesure immédiate, correction sous 7 jours. V3 et V4 : correction sous 30 jours. Tester la restauration d’une copie immuable hors site.

4. Communiquer et respecter les obligations de sécurité

La direction attend des recommandations directement applicables, qui distinguent les faits établis des hypothèses et évitent de divulguer inutilement des détails sensibles. Les questions concernent la sensibilisation aux accès distants, la conduite à tenir en cas de suspicion d'atteinte aux données RH et le suivi mesurable de l'amélioration de la sécurité.

Sensibilisation des salariés

Question 4.1. Rédigez à destination des salariés un message de sensibilisation de deux ou trois phrases concernant les accès distants et les demandes inhabituelles de validation de connexion. Indiquez le comportement attendu et un canal de signalement.

Le message doit donner une consigne claire face à une demande imprévue : ne pas l'approuver, même si elle semble provenir d'un service connu. Il faut aussi indiquer un canal que les salariés peuvent utiliser immédiatement, sans leur demander d'évaluer eux-mêmes si la connexion est malveillante. Le support informatique, par le canal habituel de l'entreprise, convient et permet de vérifier la demande.

> **✓ RÉPONSE À RETENIR**
>
> Ne validez que les connexions que vous avez vous-même initiées. Signalez toute demande inhabituelle au support informatique, par le canal habituel.

Données personnelles et RGPD

Question 4.2. L'application RH traite des données personnelles. Indiquez deux actions immédiates à mener si une atteinte à ces données est suspectée. Précisez dans quelles conditions l'obligation de notification à l'autorité de contrôle prévue par le RGPD peut s'appliquer et indiquez le délai prévu.

1. Limiter l'atteinte : alerter immédiatement le responsable informatique et le responsable de la protection des données, puis sécuriser les accès concernés sans détruire les traces utiles.
2. Préserver les journaux et éléments de preuve afin d'évaluer les données, les personnes et la période concernées. Ne pas présenter une fuite comme avérée avant vérification.

Selon l'article 33 du RGPD, l'autorité de contrôle doit être notifiée si la violation est susceptible d'engendrer un risque pour les droits et libertés des personnes, sauf si ce risque est improbable. La notification doit être faite, si possible, dans les 72 heures après en avoir pris connaissance. En cas de risque élevé, les personnes concernées doivent aussi être informées sans délai injustifié.

> **✓ RÉPONSE À RETENIR**
>
> Contenir l'atteinte et préserver les journaux; alerter le responsable de la protection des données. Si un risque pour les personnes est probable, notifier l'autorité si possible sous 72 heures.

Indicateur de sécurité

Question 4.3. Donnez un indicateur mesurable permettant à la direction de suivre l'amélioration de la sécurité après la mise en œuvre des remédiations, puis définissez ce que cet indicateur mesure.

Suivre mensuellement le taux de vulnérabilités prioritaires corrigées et vérifiées dans le délai fixé. Cet indicateur mesure la part des vulnérabilités prioritaires recensées pendant la période qui ont été corrigées puis contrôlées à temps. Calcul : nombre de vulnérabilités prioritaires corrigées et vérifiées dans le délai, divisé par le nombre total de vulnérabilités prioritaires recensées sur la période, puis multiplié par 100. Une hausse durable indique une meilleure maîtrise du traitement, sans prouver à elle seule l'absence de risque.

> **✓ RÉPONSE À RETENIR**
>
> Taux de corrections prioritaires vérifiées dans les délais : vulnérabilités corrigées et contrôlées à temps / vulnérabilités prioritaires recensées, en pourcentage.

Ce qu'il faut retenir de ce sujet (Session 2026)

Bilan de l'épreuve : Épreuve du BUT Réseaux et télécommunications, parcours cybersécurité, compétence C8, session 2026, code 26-BUT-RT-C8, durée de 2 heures et coefficient indicatif 3. À partir du système d'information d'une PME, elle évalue l'identification des actifs, l'analyse et la cotation des vulnérabilités, la hiérarchisation des risques, les remédiations, la sensibilisation et les obligations liées aux données personnelles.

Notions-clés, formules & règles à maîtriser

- La criticité se calcule avec la formule C = V × I, où V représente la vraisemblance et I l'impact.
- Les classes du DT 2 sont : 1 à 3 faible, 4 à 7 modérée, 8 à 11 élevée et 12 à 16 critique.
- Une vulnérabilité est une faiblesse exploitable ; une menace est une cause potentielle susceptible de l'exploiter.
- Une sauvegarde ne garantit pas la reprise : la capacité de restauration doit être vérifiée par des tests.

Points de vigilance & attentes du jury

- Justifier les valeurs de vraisemblance et d'impact par les faits du dossier et l'échelle du DT 2.
- Présenter les événements des journaux comme des indices à vérifier, et non comme la preuve d'une compromission.
- En cas d'égalité de criticité, départager d'abord selon l'impact, puis selon l'exposition de l'actif à Internet.
- Pour chaque action du plan, préciser un responsable autorisé, une échéance cohérente et un indicateur vérifiable.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment calculer et classer la criticité d'un risque dans ce sujet ?

Multipliez la vraisemblance par l'impact selon les échelles du DT 2 : C = V × I. Classez ensuite le résultat de 1 à 3 comme faible, de 4 à 7 comme modéré, de 8 à 11 comme élevé, et de 12 à 16 comme critique.

Q : Les échecs de connexion suivis d'une authentification réussie prouvent-ils une compromission ?

Non. Ils constituent un signal d'alerte, mais le dossier ne confirme ni extraction de données, ni modification de fichiers, ni interruption de service. Il faut vérifier la légitimité de la connexion et examiner les journaux et autres indices pertinents.

Q : Que faut-il inclure dans le plan d'action et comment organiser son temps ?

L'épreuve vaut 20 points, répartis entre quatre parties de 4, 6, 6 et 4 points. Complétez les DR 1 et DR 2, prévoyez au moins trois actions et faites figurer une action de sauvegarde et de restauration.

Q : Quelle méthode de cotation et quelles règles de notification sont attendues ?

Utilisez exclusivement l'échelle interne du DT 2, qui n'est pas un score normalisé, et justifiez les valeurs choisies. Pour une violation de données personnelles, le RGPD prévoit une notification à l'autorité dans les 72 heures, sauf si la violation est peu susceptible d'engendrer un risque pour les personnes.

Sujet officiel associé (PDF) : https://butrt.fr/assets/annales/but-rt/C8 - Sensibiliser aux vulnérabilités d'un système d'information et aux remédiations possibles/2026/BUT Réseaux et Télécommunications - C8 - Sensibiliser aux vulnérabilités d'un système d'information et aux remédiations possibles - Session 2026 - 1-Sujet.pdf

Ressources BUT Réseaux et Télécommunications : Toutes les annales & corrigés • Fiches de révision complètes • Simulateur de notes d'examen

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.